

MAGAZINE

# BSD

FOR NOVICE AND ADVANCED USERS

## FreeNAS

A COMPLETE GUIDE TO FREENAS HARDWARE DESIGN

**DOES YOUR INFORMATION  
BELONG TO THE CIA TRIAD?**

**SECURITY MONITORING  
OF INDUSTRIAL CONTROL SYSTEMS**

**INTERVIEW WITH SOLÈNE RAPENNE**  
WHAT MAKES THE SPECIAL CONNECTION  
BETWEEN DRAGONFLY BSD AND OWNCLOUD?

VOL.9 NO.03  
ISSUE 68  
1898-9144



855-GREP-4-IX  
[www.iXsystems.com](http://www.iXsystems.com)  
Enterprise Servers and Storage  
for Open Source



- ✓ Rock-Solid Performance
- ✓ Professional In-House Support

# FREENAS MINI STORAGE APPLIANCE

IT SAVES YOUR LIFE.



## HOW IMPORTANT IS YOUR DATA?

Years of family photos. Your entire music and movie collection. Office documents you've put hours of work into. Backups for every computer you own. We ask again, *how important is your data?*

## NOW IMAGINE LOSING IT ALL

Losing one bit - that's all it takes. One single bit, and your file is gone.

The worst part? **You won't know until you absolutely need that file again.**



*Example of one-bit corruption*

## THE SOLUTION

The FreeNAS Mini has emerged as the clear choice to save your digital life. **No other NAS in its class offers ECC (error correcting code) memory and ZFS bitrot protection to ensure data always reaches disk without corruption and never degrades over time.**

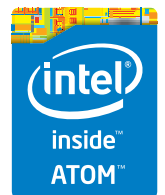
No other NAS combines the inherent data integrity and security of the ZFS filesystem with fast on-disk encryption. No other NAS provides comparable power and flexibility. The FreeNAS Mini is, hands-down, the best home and small office storage appliance you can buy on the market. **When it comes to saving your important data, there simply is no other solution.**

### The Mini boasts these state-of-the-art features:

- 8-core 2.4GHz Intel® Atom™ processor
- Up to 16TB of storage capacity
- 16GB of ECC memory (with the option to upgrade to 32GB)
- 2 x 1 Gigabit network controllers
- Remote management port (IPMI)
- Tool-less design; hot swappable drive trays
- FreeNAS installed and configured



<http://www.ixsystems.com/mini>



# FREENAS CERTIFIED STORAGE



With over six million downloads, FreeNAS is undisputedly *the* most popular storage operating system in the world.

Sure, you could build your own FreeNAS system: research every hardware option, order all the parts, wait for everything to ship and arrive, vent at customer service because it *hasn't*, and finally build it yourself while hoping everything fits - only to install the software and discover that the system you spent *days* agonizing over **isn't even compatible**. Or...

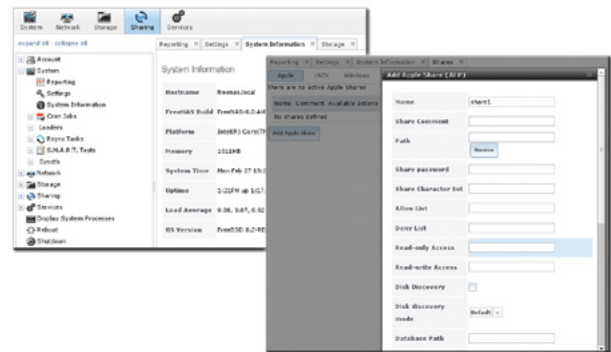
## MAKE IT EASY ON YOURSELF

As the sponsors and lead developers of the FreeNAS project, iXsystems has combined over 20 years of hardware experience with our FreeNAS expertise to bring you FreeNAS Certified Storage. **We make it easy to enjoy all the benefits of FreeNAS without the headache of building, setting up, configuring, and supporting it yourself.** As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS.

## Every FreeNAS server we ship is...

- » Custom built and optimized for your use case
- » Installed, configured, tested, and guaranteed to work out of the box
- » Supported by the Silicon Valley team that designed and built it
- » Backed by a 3 years parts and labor limited warranty

As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS. **Contact us today for a FREE Risk Elimination Consultation with one of our FreeNAS experts.** Remember, every purchase directly supports the FreeNAS project so we can continue adding features and improvements to the software for years to come. **And really - why would you buy a FreeNAS server from *anyone* else?**



### FreeNAS 1U

- Intel® Xeon® Processor E3-1200v2 Family
- Up to 16TB of storage capacity
- 16GB ECC memory (upgradable to 32GB)
- 2 x 10/100/1000 Gigabit Ethernet controllers
- Redundant power supply

### FreeNAS 2U

- 2x Intel® Xeon® Processors E5-2600v2 Family
- Up to 48TB of storage capacity
- 32GB ECC memory (upgradable to 128GB)
- 4 x 1GbE Network interface (Onboard) - (Upgradable to 2 x 10 Gigabit Interface)
- Redundant Power Supply



<http://www.iXsystems.com/storage/freenas-certified-storage/>

Dear Readers,

*As spring is here, it is high time to wish you that Easter will bring you a lot of joy, happiness, hope and light.*

*Our wishes for this Easter.  
Good health,  
Good fortune,  
Fulfilling life.*

*I hope that this issue of BSD magazine will be a good lecture for the holidays. I know that all of you are waiting for holidays so I do not bother you more. Please go to the Table of Contents page to see what we prepared and what you will find inside this BSD issue. Just start reading now.*

*Finally, I would like to thank you Authors, Reviewers, Proofreaders, BSD fans, Friends, and Readers for your invaluable support and contribution.*

*Happy Easter!  
Ewa & BSD Team*

# MAGAZINE BSD

**Editor in Chief:**

Ewa Dudzic  
ewa.dudzic@software.com.pl

**Contributing:**

Michael Shirk, Andrey Vedikhin, Petr Topiarz,  
Charles Rapenne, Anton Borisov, Jeroen van Nieuwenhuizen,  
José B. Alós, Luke Marsden, Salih Khan,  
Arkadiusz Majewski, BEng, Toki Winter, Wesley Mouedine  
Assaby, Rob Somerville

**Top Betatesters & Proofreaders:**

Annie Zhang, Denise Ebery, Eric Geissinger, Luca  
Ferrari, Imad Soltani, Olaoluwa Omokanwaye, Radjis  
Mahangoe, Mani Kanth, Ben Milman, Mark VonFange

**Special Thanks:**

Annie Zhang  
Denise Ebery

**Art Director:**

Ireneusz Pogroszewski

**DTP:**

Ireneusz Pogroszewski  
ireneusz.pogroszewski@software.com.pl

**Senior Consultant/Publisher:**

Paweł Marciniak  
pawel@software.com.pl

**CEO:**

Ewa Dudzic  
ewa.dudzic@software.com.pl

**Publisher:**

Hakin9 Media SK  
02-676 Warsaw, Poland  
Postepu 17D  
Poland  
worldwide publishing  
editors@bsdmag.org  
www.bsdmag.org

Hakin9 Media SK is looking for partners from all over the world. If you are interested in cooperation with us, please contact us via e-mail: editors@bsdmag.org.

All trademarks presented in the magazine were used only for informative purposes. All rights to trademarks presented in the magazine are reserved by the companies which own them.

# FreeNAS

## in an Enterprise Environment

**NEW RELEASE**

By the time you're reading this, FreeNAS has been downloaded more than 5.5 million times. For home users, it's become an indispensable part of their daily lives, akin to the DVR. Meanwhile, all over the world, thousands of businesses, universities, and government departments use FreeNAS to build effective storage solutions in myriad applications.



### What you will learn...

- How TrueNAS builds off the strong points of the FreeBSD and FreeNAS operating systems
- How TrueNAS meets modern storage challenges for enterprise

**WE INTERRUPT THIS MAGAZINE TO BRING YOU THIS IMPORTANT ANNOUNCEMENT:**

THE PEOPLE WHO DEVELOP FREENAS, THE WORLD'S MOST POPULAR STORAGE OS, HAVE JUST REVAMPED TRUENAS.

The FreeNAS operating system is free, open source, and available to the public and offers thorough documentation, a large and active community, and a feature-rich storage environment. Based on FreeBSD, FreeNAS can share over a host of protocols (SMB, NFS, FTP, iSCSI, etc) and features an intuitive web interface, the ZFS file system, a plug-in system for backup, and much more.

Despite the massive popularity of FreeNAS, many aren't aware of its big brother, TrueNAS. TrueNAS is the data in some of the most demanding and complex enterprise environments: the proven, enterprise-grade, professionally-supported line of TrueNAS storage systems.

But what makes TrueNAS different from FreeNAS? Well, I'm glad you asked...



### Commercial Grade Support

When a mission critical storage system goes down, an organization's whole operation can come to a halt. Whole community-based (and free), it can't always get an expert to help and running in a timely manner. TrueNAS offers the responsiveness and expertise of a dedicated support team to provide that safety.

Created by the same team that developed FreeNAS.

**POWER WITHOUT CONTROL MEANS NOTHING. TRUENAS STORAGE GIVES YOU BOTH.**

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Simple Management   | <input checked="" type="checkbox"/> Self-Healing Filesystem            |
| <input checked="" type="checkbox"/> Hybrid Flash Acceleration                                 | <input checked="" type="checkbox"/> High Availability                  |
| <input checked="" type="checkbox"/> Intelligent Compression                                   | <input checked="" type="checkbox"/> Qualified for VMware and HyperV    |
| <input checked="" type="checkbox"/> All Features Provided Up Front (no hidden licensing fees) | <input checked="" type="checkbox"/> Works Great With Citrix XenServer® |

To learn more, visit: [www.ixsystems.com/truenas](http://www.ixsystems.com/truenas)



### POWERED BY INTEL® XEON® PROCESSORS

Intel, the Intel logo, Intel Xeon and Intel Xeon Inside are trademarks of Intel Corporation in the U.S. and/or other countries. VMware and VMware Ready are registered trademarks or trademarks of VMware, Inc. in the United States and other jurisdictions.

Citrix makes and you receive no representations or warranties of any kind with respect to the third party products, its functionality, the test(s) or the results there from, whether expressed, implied, statutory or otherwise, including without limitation those of fitness for a particular purpose, merchantability, non-infringement or title. To the extent permitted by applicable law. In no event shall Citrix be liable for any damages of any kind whatsoever arising out of your use of the third party product, whether direct, indirect, special, consequential, incidental, multiple, punitive or other damages.

## FreeBSD World

### C Developer in a FreeBSD World. Part 2 **8**

**David Carlier**

In the “The Journey of a C developer in a FreeBSD World”, David described the changes that occur when you land in a BSD system coming from Linux. Now, you get ready to get your C/C++ code working in both platforms; this time we will look into the debugging side.

## Expert says ...

### A Complete Guide to FreeNAS Hardware Design, Part II: Hardware Specifics **12**

**Josh Paetzel**

A guide to selecting and building FreeNAS hardware, written by the FreeNAS Team, is long past overdue by now. For that, we apologize. The issue was the depth and complexity of the subject, as you’ll see by the extensive nature of this four part guide, due to the variety of ways FreeNAS can be utilized.

## Security

### Does your information belong to the CIA triad? **14**

**Rob Somerville**

Confidentiality, Integrity and Availability are the three pillars of Information Security. In this article, we pose a number of scenarios to you the IT professional and ask What would you do? Every environment is different, so we will not provide any answers. Instead we want to stimulate thought and debate around the ethics that Donn Parker says are missing from the computer center.

### Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems **18**

**Eric D. Knapp & Joel Thomas Langill**

The first step of information analysis requires a certain degree of data collection so that there is a healthy body of data to assess. Collecting evidence relevant to cyber security requires knowing what to monitor and how to monitor it. You will learn about determining what to monitor, successfully monitoring security zones, information management and, log storage and retention.

## Column

### With a former intelligence operative confirming that the NSA has developed the prized technique of concealing spyware in the firmware of hard drives, what are the implications and is there any point in shutting the door now that the horse has bolted? **42**

**Rob Somerville**

## Interview

### Interview with with Solène Rapenne Luca Ferrari **44**

# Among clouds Performance and Reliability is **critical**

Download syslog-ng Premium Edition  
product evaluation [here](#)

Attend to a free logging tech webinar [here](#)



**BalaBit**  
IT Security

[www.balabit.com](http://www.balabit.com)

## syslog-ng log server

The world's first High-Speed Reliable Logging™ technology

### HIGH-SPEED RELIABLE LOGGING

- above 500 000 messages per second
- zero message loss due to the Reliable Log Transfer Protocol™
- trusted log transfer and storage

# C Developer in a FreeBSD World. Part 2

DAVID CARLIER

In the “The Journey of a C developer in a FreeBSD World”, I described the changes that occur when you land in a BSD system coming from Linux. Now you, dear readers, get ready to get your C/C++ code working in both platforms; this time we will look into the debugging side. Indeed, FreeBSD’s libc has jemalloc builtin. OpenBSD contains its specific implementation, called ottomalloc.

**A**s a C/C++ developer, you have concerns about memory leakage, corrupted memory. In the previous issue, the article “GDB debugger” perfectly described its proper usage. Its reading is greatly recommended. We’ll focus on the memory allocators.

In OpenBSD, several options are available via the MALLOC\_OPTIONS environment variable or the global malloc\_options variable changeable from within your C/C++ code. To enable a specific option, it is the uppercase letter. To disable it, it is the lowercase counterpart.

The malloc statistics are disabled by default, for performance matters. In order to enable these, the OpenBSD source code is needed and we just need to uncomment this line in lib/libc/stdlib/malloc.c:

```
/* #define MALLOC_STATS */
```

Then we can just recompile the libc:

```
> cd lib/libc
> make obj && make depend && make install
```

Now, malloc\_dump symbol is available!

```
> nm /usr/lib/libc.a | grep malloc_dump
00000790 T malloc_dump
```

One I find quite useful is the junk option (enabled by default since 5.6 release).

Indeed, after an allocation, the memory area is filled with 0xd0. When it is freed, it is filled with 0xdf. What you can spot easily is when you try to use a previously freed memory pointer.

```
int
main(int argc, char *argv[])
{
    char *p = new char[4];
    strcpy(p, "foo", 4);
    std::cout << p << std::endl;
    delete p;
    std::cout << p << std::endl;
    return (0);
}
```

...



You ought to see this kind of output:

```
> ./test
foo
XXXXXXXXXXXX
=> we have our filled free pointer ...
...
...
> env MALLOC_OPTIONS=j ./test => let's disable the junk
option
foo
foo
=> not good at all, we can believe the p pointer is still
valid at this point ...
...
```

As you can see above, the junk option is really useful and the performance hit is quite acceptable so it is quite advised to keep this option on, even in production.

The Freeguard option, F, is useful for detecting double free.

```
int
main(int argc, char *argv[])
{
    ...
    char *p = malloc(sizeof(char) * count);
    ...
    free(p);
    ...
    <i.e no realloc meanwhile ...>
    ...
    free(p);
    return (0);
}

> ./test
=> The double free not caught ...

> env MALLOC_OPTIONS=F ./test
test(7086) in free(): error: bogus pointer (double free?)
0x7820972ff40
Abort trap (core dumped)
=> The double free is caught
```

Another flag useful for debugging, A (for abort, enabled by default) which simply coredumps the current process.

Previously, we compiled the libc to enable the malloc statistics, hence to enable D (for Dump) statistics. So compiled with debug symbols:

```
...
int
main(int argc, char *argv[])
{
    char *p = malloc(4096);
    malloc_dump(2);
    return (0);
}

> ./test
=> from within the code, malloc_dump prints on the given
file descriptor those statistics ...
Malloc dir of test at 0x11d6c987f3d0
Region slots free 511/512
Finds 0/0
Inserts 1/0
Deletes 0/0
Cheap reallocs 0/0
Free chunk structs:
Free pages cached: 0
slot) hash d type page f
size [free/n]
65) # 65 0 pages 0x11d6a9f84000 0x11d6aa3ed86d 4096
In use 16384
Guarded 0
Leak report
f sum # avg
0x11d6aa3ed86d 4096 1 4096
```

Here we got the faulty address, 0x11d6aa3ed86d, when the pointer was allocated but never freed.

Or we can call malloc\_dump from within gdb

```
...
> gdb ./test
After putting a breakpoint to exit, we call call malloc_
dump to print on stderr

malloc_dump(2)
...
0xfa0110012704096 1 4096
...
list *0xfa011001270
```

We retrieve our faulty code here:

```
int
main(int argc, char *argv[])
{
    char *p = malloc(4096);
```

```

malloc_dump(2);
return (0);
}

```

Apart of `MALLOC_OPTIONS`, OpenBSD protects well against stack overflow's issues. The stack protector flag is implied; there's no need to add it for the compilation.

```

int
main(int argc, char *argv[])
{
    char buf[4];
    strcpy(buf, "foobar");
    printf("%s\n", buf);
}
...
> cc -g -O2 -o test test.c
/tmp/ccPGztFB.o(.text+0x1db): In function 'main':
: warning: strcpy() is almost misused, please use
    strcpy()
...
> ./test
foobar
Abort trap (core dumped)

```

When possible, it is advised to use `strncpy` (the compiler is nice enough to warn you about that), except if you're 100% confident about the source you attempt to copy.

```

int
main(int argc, char *argv[])
{
    char buf[4];
    strncpy(buf, "foobar", 7);
    printf("%s\n", buf);
}
...
> cc -g -O2 -o test test.c
test.c: In function 'int main()':
test.c:9 warning: array size (4) smaller than bound length (7)
=> you have been warned that your buffer is really too
    small ...

```

For FreeBSD, it is slightly different but we can retrieve similar options with `jemalloc`, like `junk`.

As a developer, you might need to make sure that `MALLOC_PRODUCTION` is not defined in either `/etc/src.conf` and `/etc/make.conf`. Although it brings significant performance improvements, the debugging capabilities are lost.

```

...

int
main(int argc, char *argv[])
{
    char *p = new char[4];
    strcpy(p, "foo", 4);
    std::cout << p << std::endl;
    delete p;
    std::cout << p << std::endl;
    return (0);
}

> ./test
foo
ZZZZZZZZZZ
...
> setenv MALLOC_CONF "junk:false"
> ./test
foo
foo

```

It is possible to dump statistics via `stats_print` options:

```

> setenv MALLOC_CONF "stats_print:true"
> ./test
...
___ Begin jemalloc statistics ___
Version: 3.6.0-0-g46c0af68bd248b04df75e4f92d5fb804c3d75340
Assertions enabled
Run-time option settings:
  opt.abort: true
  opt.lg_chunk: 22
  opt.dss: "secondary"
  opt.narenas: 32
  opt.lg_dirty_mult: 3
  opt.stats_print: true
  opt.junk: true
  opt.quarantine: 0
  opt.redzone: false
  opt.zero: false
  opt.utrace: false
  opt.xmalloc: false
  opt.tcache: true
  opt.lg_tcache_max: 15
CPUs: 8
Arenas: 32
Pointer size: 8
Quantum size: 16
Page size: 4096

```

```

Min active:dirty page ratio per arena: 8:1
Maximum thread-cached size class: 32768
Chunk size: 4194304 (2^22)
Allocated: 4096, active: 4096, mapped: 8388608
Current active ceiling: 4194304
chunks: nchunks   highchunks   curchunks
         2         2         2
huge:  nmalloc    ndalloc    allocated
       0         0         0

arenas[0]:
assigned threads: 1
dss allocation precedence: secondary
dirty pages: 1:0 active:dirty, 0 sweeps, 0 madvises, 0
  purged
          allocated    nmalloc    ndalloc    nrequests
small:    0            0            0            0
large:   4096         1            0            1
total:   4096         1            0            1
active:   4096
mapped:  4194304
bins:    bin  size regs pgs   allocated    nmalloc
          ndalloc  nrequests    nfills    nflushes
          newruns  reruns      curruns
[0..27]
large:  size pages  nmalloc  ndalloc  nrequests  curruns
       4096  1      1         0        1          1
[1017]
--- End jemalloc statistics ---

```

or from within the code:

```

#include <malloc_np.h>

...
void
m_stats(void *args __unused, const char *data)
{
    if (data != NULL)

```

```

        printf("%s\n");
    }
    ...
    int
    main(int argc, char *argv[])
    {
        char *p = malloc(4096);
        /* could simply make the first argument as NULL */
        malloc_stats_print(m_stats, NULL, NULL);
        return (0);
    }

```

With the utrace option, it adds an entry for ktrace...

```

> setenv MALLOC_CONF "utrace:true"
> ktrace ./test
> kdump
...
1245 test      CALL  utrace(0x7fffffff0000,0x18)
1245 test      USER  0x801006000 = malloc(4096)
1245 test      RET   utrace 0
1245 test      CALL  utrace(0x7fffffff0008,0x18)
1245 test      USER  free(0x801006000)
...

```

As you can see without any third party tool, in FreeBSD / OpenBSD we have those features which greatly help with debugging. Even if the price to pay is having lower performance results, it is worth it during the development at least.

## ABOUT THE AUTHOR

*David Carlier has been a developer since 2001, has been using BSD since 2004 and has worked for a mobile based position as a C/C++ developer in Ireland since 2012. During his spare time, he contributes to various BSD projects, especially FreeBSD, and writes some articles for BSDMag.*



# A Complete Guide to FreeNAS Hardware Design,

## Part II: Hardware Specifics

JOSH PAETZEL

### General Hardware Recommendations

I've built a lot of ZFS storage hardware and have two decades of experience with FreeBSD. The following are some thoughts on hardware.



### Intel Versus AMD

FreeNAS is based on FreeBSD. FreeBSD has a long history of working better on Intel than AMD. Things like (but not limited to) the watchdog controllers, USB controllers, and temperature monitoring all have a better chance of being well supported when they are on an Intel platform. This is not to say that AMD platforms won't work, that there aren't AMD platforms that work flawlessly with FreeNAS, or even that there aren't Intel platforms that are poor choices for FreeNAS, but all things being equal, you'll have better luck with Intel than AMD.

The Intel Avoton platforms are spendy but attractive: ECC support, low power, AES-NI support (a huge boon for encrypted pools). On the desktop side of things, there are Core i3 platforms with ECC support, and of course there are many options in the server arena. The single socket E3


 The logo for iXsystems, featuring a stylized red figure climbing a tree on the left, and the word "systems" in white lowercase letters inside a blue oval with a registered trademark symbol.
 **systems**®

Xeons are popular in the community, and of course for higher end systems, the dual package Xeon platforms are well supported.

### Storage Controllers

LSI is the best game in town for add-on storage controllers. Avoid their MegaRAID solutions and stick with their HBAs. You'll see three generations of HBAs commonly available today. The oldest (and slowest) are the SAS 2008 based I/O controllers such as the 9211 or the very popular IBM M1015. The next generation of these controllers was based on the 2308 which added PCI 3.0 support and increased CPU horsepower on the controller itself. An example here is the 9207. Both the 2008 and 2308 based solutions are 6Gbps SAS parts. The newest generation of controllers are 12Gbps parts such as the 9300. The FreeNAS driver for the 6 Gbps parts is based on version 16 of the stock LSI driver with many enhancements that LSI never incorporated into their driver. In addition, many of the changes after version 16 were specifically targeted at the Integrated RAID functionality that can be flashed onto these cards. As a result, "upgrading" the driver manually to the newer versions found on the LSI website can actually result in downgrading its reliability or performance. I highly recommend running version 16 firmware on these cards. It's the configuration tested by LSI, and it's the configuration tested by the FreeNAS developers. Running newer firmware *should* work, however running older firmware is not recommended or supported as there are known flaws that can occur by running the FreeNAS driver against a controller with an older firmware. FreeNAS will warn you if the firmware on an HBA is incompatible with the driver. Heed this warning or data loss can occur. The newer 12Gbps parts use version 5 of the LSI driver. Cards using this driver should use version 5 of the firmware.

Most motherboards have some number of SATA ports built in. There are certain models of Marvell and J-Micron controllers that are used on motherboards that have large numbers of SATA ports. Some of these controllers have various compatibility issues with FreeNAS, and some of these controllers also have forms of RAID on them. As a general rule, the integrated chipset AHCI SATA ports have no issues when used with FreeNAS, they just tend to be limited to 10 ports (and often far fewer) on most motherboards.

### Hard Drives

Desktop drives should be avoided whenever possible. In a desktop, if an I/O fails, all is lost. For this reason, desktop drives will retry I/Os endlessly. In a storage device, you want redundancy at the storage level. If an individual drive fails an I/O, ZFS will retry the I/O on a different drive. The faster that happens, the faster the array will be able to cope with hardware faults. For larger arrays, desktop drives (yes, I've seen attempts to build 1PB arrays with ZFS and desktop drives) are simply not usable in many cases. For small to medium size arrays, a number of manufacturers produce a "NAS" hard drive that is rated for arrays of modest size (typically 6-8 drives or so). These drives are worth the additional cost.

At the high end, if you are building an array with SAS controllers and expanders, consider getting the nearline 7200 RPM SAS drives. These drives are a very small premium over Enterprise SATA drives. However, running SATA drives in SAS expanders –while supported– is a less desirable configuration than using SAS end to end due to the difficulty of translating SATA errors across the SAS bus.


 A solid red circle graphic.
 **JOSH PAETZEL**

*iXsystems Director of IT*

# Does your information belong to the CIA triad?

ROB SOMERVILLE

Confidentiality, Integrity and Availability are the three pillars of Information Security. In this article, we pose a number of scenarios to you the IT professional and ask What would you do? Every environment is different, so we will not provide any answers. Instead we want to stimulate thought and debate around the ethics that Donn Parker says are missing from the computer center.

## 01

### Question 1.

A senior manager has a vital deadline for early Monday morning. As part of this deadline, they must compose a very dense presentation of images, video and music from media legally stored and appropriately

licensed on the corporate server over the weekend at home. This request arrives late on a Friday evening, and due to the size of the media, the only available hard-drive is an external USB drive that contains data confidential to the organisation. Transfer of the data via other means is impossible due to the total file sizes. The manager in question is renown for losing or breaking items. As there is not sufficient time to securely wipe the drive, a standard disk format is applied, in the knowledge that the confidential information could be recovered fairly easily by a competent professional. Should IT inform the manager of this fact and ask them to be extra vigilant?

## 02

### Question 2.

In addition to the scenario in Question 1, the venue where the public presentation will take place does not have a Performing Rights Society licence (or global equivalent) to play the background music to the presentation. IT are aware of this issue, but past experience has shown that advising managers about these facts are inevitably met with resistance, censure and in some cases verbal abuse. Whose duty is it to inform the manager?

presentation. IT are aware of this issue, but past experience has shown that advising managers about these facts are inevitably met with resistance, censure and in some cases verbal abuse. Whose duty is it to inform the manager?

## 03

### Question 3.

A laptop is returned by a member of staff for a major upgrade. Should an audit be performed on the data downloaded from the Internet and websites visited as a matter of course? Internet provision is supplied free of charge

by the organisation to staff members working from home. Where are the lines drawn between corporate and personal use? If illegal content was found (e.g. pirated music or videos) who would hold legal liability if a) Access was via a corporate VPN / Firewall or b) Access was direct to the Internet?

04

**Question 4.**

With the discovery of spyware now being embedded in the firmware of hard drives<sup>1</sup>, what action can IT take to remedy this attack vector? Is there a policy in place to inform senior management of the risks?

If the response of management

to this risk is non-committal or worse still, derisory, how can IT protect itself from the buck being passed down the line in the case of an incident?

05

**Question 5.**

Manager (A) demands administrator rights to a system and you refuse, offering an adequate alternative. You have verbal evidence from Manager (A) that they wanted this access for unethical reasons. Your manager

(B) is the best friend of Manager (A). How would you

address this scenario without compromising Manager (B) or yourself?

06

**Question 6.**

As a result, sometime later in your annual review you are marked down by Manager (B) for being uncooperative. You also discover that Manager (B) is quite at ease with Manager (A)'s behaviour, despite the risks

to the organisation. With hindsight, how would this affect your response to Question 5?

07

**Question 7.**

You discover a major security flaw in a public facing Internet system and alert your manager. Both you and your manager agree that this system is not fit for purpose and should be recommissioned. Senior management

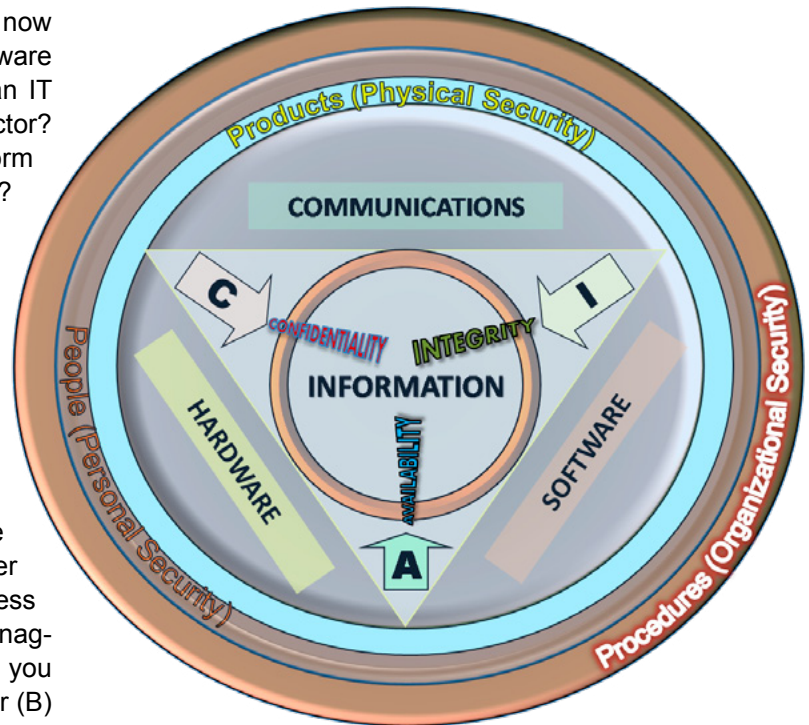
overrides both you and your manager and the flaw remains un-patched, due to cost. What do you do?

08

**Question 8.**

Consequently, the flaw is exploited and a customer reports the breach. The system is decommissioned, but you are warned by your employer not to discuss this with anyone.

The system is widely used; do you



inform the IT departments in other organisations as the vendor is attempting to cover up the issue and will not fix it in a speedy manner?

09

**Question 9.**

A member of staff (A) has gone on sick leave and another member of staff in the same department (B) wants access to their data and email for business purposes. Approval for this should come from their respective

manager (C), but he cannot be contacted to give approval, and you deny the request. The member of staff (B) reports this to senior management and you are told to give (B) access by senior manager (D). Consequently, (A) and manager (C) make an official complaint against you as (B) has accidentally sent confidential information to a third party using (A)'s email account. (D) washes their hands of the whole affair and has support of senior management who would prefer to lay blame at the door of IT. How do you proceed?

<sup>1</sup> <http://www.reuters.com/article/2015/02/16/us-usa-cyberspying-idUSKBN0LK1QV20150216>

10

**Question 10.**

Your manager (A) refuses to give (B) access to an external VPN of a partner organisation as it is a known security risk. You witness the exchange, and while your manager's response could be considered brusque, it is not aggressive or threatening. Shortly after, you find (B) in tears and report this to your manager (A). (B) attempts to make a formal complaint against (A). If the complaint is investigated (A)'s manager, (C) will lead the process. You are approached by an influential senior member of staff (D) and are effectively told if you are approached as a witness to lie about the incident. You cannot tell (A) and (D) is frequently seen with (C) who is reportedly 'on-side' with (D). How do you proceed if a) you are asked to be a witness and b) you have no faith in the formal whistle-blowing policy? All the others you know who have followed this path have been dismissed or have resigned under duress.

11

**Question 11.**

Consequently, no formal complaint is raised. Do you make a formal complaint against (D) to your manager (A) knowing full well that (A) has an axe to grind with (D) and that (C) will probably take the side of (D)?

12

**Question 12.**

All Internet and Email traffic is monitored and logged in your organisation. A personal witch-hunt is being performed against a popular, professional and effective member of staff. Do you provide the logs 'as is' knowing that any minor infringements of company policy (e.g. Facebook use, sending personal emails etc.) – which are normally ignored – will be used against them?

13

**Question 13.**

The company responsible for facilities management has access to all areas of the building, but you suspect that they are tampering with equipment in the datacenter. Furthermore, they have allowed 3rd parties unsupervised into the datacenter without notifying IT on numerous occasions. Access is via key-card, but senior management refuse to allow you to install an additional key-lock as the FM company is responsible for the infrastructure and they

demand access. Apart from generating a bureaucratic "Told you so" audit trail, what can you do to remedy matters?

14

**Question 14.**

The CEO of the organisation has asked you to securely delete certain key original documents. You know that the media and national press are anxious to obtain the originals. Multiple historical backups exist, but the individual file cannot be removed from these without destroying the backups. How rigorously do you carry out your instructions, if at all? Would it be ethical to release the document to the press in direct defiance of instructions?

15

**Question 15.**

Manager (A) who was instrumental in head-hunting you for your senior role is being investigated for stealing intellectual property from a company you both worked for some years ago. While you were not party to this event, you always believed manager (A)'s account that there was a major disagreement and everything was settled so when you are questioned you defend the manager as you have no evidence to the contrary. Some months later, a customer demands a brand-new PC for his daughter otherwise he will withhold substantial payment. You raise your concerns with (A), but are told to deliver a new computer despite your protests. Some months later, manager (A) (along with others) resign due to major conflicts with senior management. You then discover major financial improprieties have been taking place throughout the organisation and you are being pressurised to fraudulently sign compliance certification which are legally binding documents. You refuse, and are ostracised by the senior partners. Do you resign on principle?

**ABOUT THE AUTHOR**

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*



# Great Specials

On FreeBSD® & PC-BSD® Merchandise

Give us a call & ask about our  
**SOFTWARE BUNDLES**

**1.925.240.6652**

**\$39.95**

FreeBSD 9.1 Jewel Case CD Set  
or FreeBSD 9.1 DVD

**\$29.95**

PC-BSD 9.1 DVD

**\$49.95**

The PC-BSD 9.0 Users Handbook  
PC-BSD 9.1 DVD



**\$99.95**

The FreeBSD CD or DVD Bundle

Inside each CD/DVD Bundle, you'll find:  
FreeBSD Handbook, 3rd Edition  
Users Guide FreeBSD Handbook, 3rd Edition, Admin Guide  
FreeBSD 9.1 CD or DVD set  
FreeBSD Toolkit DVD

*Stylish Dress Attire*  
Look Your Professional Best



*Comfy Apparel*  
Stay Warm in Zip Ups & Pullovers

*T-Shirts*  
Lots of Styles to Choose From

**FreeBSD 9.1 Jewel Case CD/DVD**.....\$39.95

CD Set Contains:

- Disc 1** Installation Boot LiveCD (i386)
- Disc 2** Essential Packages Xorg (i386)
- Disc 3** Essential Packages, GNOME2 (i386)
- Disc 4** Essential Packages (i386)

FreeBSD 9.0 CD.....\$39.95

FreeBSD 9.0 DVD.....\$39.95

## FreeBSD Subscriptions

Save time and \$\$\$ by subscribing to regular updates of FreeBSD

FreeBSD Subscription, start with CD 9.1.....\$29.95

FreeBSD Subscription, start with DVD 9.1.....\$29.95

FreeBSD Subscription, start with CD 9.0.....\$29.95

FreeBSD Subscription, start with DVD 9.0.....\$29.95

## PC-BSD 9.1 DVD (Isotope Edition)

PC-BSD 9.1 DVD.....\$29.95

PC-BSD Subscription.....\$19.95

## The FreeBSD Handbook

The FreeBSD Handbook, Volume 1 (User Guide).....\$39.95

The FreeBSD Handbook, Volume 2 (Admin Guide).....\$39.95

## The FreeBSD Handbook Specials

The FreeBSD Handbook, Volume 2 (Both Volumes).....\$59.95

The FreeBSD Handbook, Both Volumes & FreeBSD 9.1.....\$79.95

**PC-BSD 9.0 Users Handbook**.....\$24.95

**BSD Magazine**.....\$11.99

**The FreeBSD Toolkit DVD**.....\$39.95

**FreeBSD Mousepad**.....\$10.00

**FreeBSD & PCBSD Caps**.....\$20.00

**BSD Daemon Horns**.....\$2.00



*Bundle Specials!*  
Save \$\$\$

*Just Plain Fun*  
Mousepads & Novelty Horns



BSD Magazine  
Available Monthly



For even MORE items  
visit our website today!

[www.FreeBSDMall.com](http://www.FreeBSDMall.com)

# Industrial Network Security

## Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

### Security Monitoring of Industrial Control Systems

ERIC D. KNAPP JOEL THOMAS LANGILL

The first step of information analysis requires a certain degree of data collection so that there is a healthy body of data to assess. Collecting evidence relevant to cyber security requires knowing what to monitor and how to monitor it.

Unfortunately, there is a lot of information that could be relevant to cyber security, and because there are many unknown threats and exploitations, even information that may not seem relevant today may be relevant tomorrow as new threats are discovered. Even more unfortunate is that the amount of seemingly relevant data is already overwhelming – sometimes consisting of millions or even billions of events in a single day, with even higher rates of events occurring during a period of actual cyber-attack.<sup>1</sup> It is therefore necessary to assess which events, assets, applications, users, and behaviors should be monitored – as well as any additional relevant systems that can be used to add context to the information collected, such as threat databases, user information, and vulnerability assessment results.

An additional challenge arises from the segregated nature of a properly secured industrial network. Deploying a single monitoring and information management sys-

tem across multiple otherwise-separated zones violates the security goals of those zones and introduces potential risk. The methods used to monitor established zones must be considerate of the separation of those zones, and the data generated from this monitoring need to be managed accordingly as well. While there are benefits to fully centralized information management, the information being generated may be sensitive and may require “need to know” exposure to security analysts. Therefore, centralized monitoring and management needs to be overlaid with appropriate security controls and countermeasures, up to and including full separation – forgoing the efficiencies of central management so that the analysis, information management, and reporting of sensitive information remains local in order to maintain absolute separation of duties between, for example, a highly critical safety system and a less secure supervisory system.

In order to deal with massive volumes of log and event data that can result from monitoring established network zones, and the challenges of highly distributed and seg-

<sup>1</sup> J.M. Butler. Benchmarking Security Information Event Management (SIEM). The SANS Institute Analytics Program, February, 2009.

regated zones, best practices in information management – including short and long-term information storage – must be followed. This is necessary in order to facilitate the threat detection process, and also as a mandate for relevant compliance requirements, such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), NRC Title 10 CFR 73.54, Chemical Facility Anti-Terrorism Standards (CFATS), and others (see Chapter 13, “Standards and Regulations”).

## DETERMINING WHAT TO MONITOR

The trite answer to “what to monitor” is “everything and more!” Everything that we monitor, however, results in information that must be managed. Every data point results in a log record, or perhaps a security or safety alert. Assets, users, applications, and the communication channels that interconnect them all require monitoring. Because there are so many assets, users, applications, and networks that need to be monitored, the total amount of information generated every second in even a moderately sized enterprise can be staggering.<sup>2</sup> While products exist to automate security event and information management, the total amount of information available can quickly overwhelm the information analysis and storage capacity of these tools. Therefore, security monitoring requires some planning and preparation in order to ensure that all necessary information is obtained, without overloading and potentially crippling the tools the information is intended to feed.

One approach is to segregate monitoring by zone. Just as the separation of functional groups into zones helps minimize risk, it also helps to minimize the total information load that is generated by that zone. In other words, there are limited assets and activities within a zone, and therefore there are less total logs and events.

To further complicate matters, operational technology (OT) activities and metrics must also be considered when securing industrial networks – representing new data types from yet another potentially overwhelming source of new assets such as remote terminal units (RTUs), programmable logic controllers (PLCs), intelligent electronic devices (IEDs), and other industrial assets; applications such as human-machine interfaces (HMIs), and Historians; and networks such as fieldbus and smart grid networks.

### TIP

When considering network monitoring and information management, it is helpful to benchmark the information load currently being produced in both IT and OT networks. IT networks require identifying which devices need

to be monitored. This means understanding what servers, workstations, firewalls, routers, proxies, and so on (almost every IT device is capable of producing logs of some sort) are important – the process of determining critical assets described in Chapter 2, “About Industrial Networks,” and Chapter 9, “Establishing Zones and Conduits,” is helpful here. Once it has been determined which devices need to be monitored, the event load generated by these devices needs to be calculated. One method is to measure the event load of a period of time that contains both normal and peak activity, and divide the total number of events by the time period (in seconds) to determine the average event per second (EPS) load of the network. Alternately, a worst-case calculation can be based entirely on peak event rates, which will result in a higher EPS target.<sup>3</sup>

Most assets in OT networks, mainly the embedded device types, like PLCs, RTUs, and IEDs, which make up the majority of network-attacked assets, do not produce events or logs at all, and therefore they cannot be measured. However, they do produce information. This can be easily derived by looking at historized data from the control plants, and/or through the use of specialized industrial protocol monitors. Determine which assets you wish to monitor, and use the Data Historian system to determine the amount of information collected from these assets over time. This information will need to be normalized and centralized – either automatically via an SIEM or similar product, or manually via human time and effort – so it may be prudent to limit the amount of historized data that need to be exposed for security assessment. Some Historian tags – especially system tags concerning authentication, critical alarm tags concerning point or operational changes, stopped or failed processes, and so on – are obvious choices, while others may have little relevance to security. This step is effectively a form of security event “rationalization,” similar to the process performed on the process event systems of ICS to improve operational effectiveness.

Once the initial benchmark is obtained, add room for growth, and room for headroom – perhaps 10% (this will vary by situation). When sizing the IT network, it is also prudent to plan for “peak averages” where peak traffic rates occur for extended periods of time (i.e. the peak becomes the average), as this condition can occur during an extended attack, or as a result of a successful breach and subsequent infection with malware.<sup>4</sup> Unusual peak averages may also occur on OT systems during abnormal events, such as plant startups and shutdowns, or during system patching or on-process migrations and upgrades. OT systems may re-

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.

<sup>4</sup> Ibid.

port different conditions but are less likely to report higher numbers of conditions unless the control process being historized has been significantly altered.

So what really needs to be monitored? The following guidelines help to identify what systems should be monitored.

## SECURITY EVENTS

Security events are those events generated by security and infrastructure products: network or host-based firewalls, network routers and switches, malware prevention systems, intrusion detection and prevention systems, application monitors, and so on. Ideally, any event generated by a security device should be relevant, and therefore, these devices should be used for promiscuous monitoring. Realistically, false positives can dilute the relevance of valid security events.

### NOTE

The term “false positive” is often misused. False positives are often associated with what are seemingly irrelevant security data because security logs and events originate from many sources and are often generated quickly and in large quantities. When an alert is generated because a benign activity matches a detection signature of an intrusion detection system (IDS), the result is a false positive. Similarly, if an anti-virus system falsely indicates that a file is infected, the result is a false positive. False positives make security analysis more difficult by generating extra data points that need to be assessed, potentially clouding real incidents from detection.

*False positives* can be minimized through tuning of the faulty detection signatures – a process that should be performed regularly to ensure that detection devices are operating as efficiently as possible. While false positives often result in large amounts of unnecessary or irrelevant data, not all irrelevant data are false positives. Many security analysts and even security vendors are tempted to overly tune devices to eliminate any alert that occurs in large numbers because of this common misconception. The issue with overly aggressive tuning is that while it will make incidents easier to manage in day-to-day operations, it can introduce *false negatives* – that is, when a real threat fails to create an alert, or when a correlation rule fails to trigger because a necessary condition was suppressed by over-tuning (see Chapter 11, “Exception, Anomaly, and Threat Detection”). Remembering that event correlation signatures are signature-matching rules that detect known threat patterns, the elimination of smaller seemingly irrelevant events can prevent detection of the larger pattern. Similarly, as security researchers discover new patterns, event data that seem irrelevant today

may become relevant in the future (see Figure 1). To ensure accurate threat detection and correlation, all legitimately produced events should be retained short-term for live analysis (i.e. kept on-line) and long-term for forensic and compliance purposes (i.e. kept off-line) regardless of how irrelevant they may seem at the time of collection. Only true false positives – the events generated due to a false signature match – should be eliminated via tuning or filtering.

When considering the relevance of security events in industrial networks, consider the source of the event and its relevance to the specific zone being monitored. For example, all zones should have at least one perimeter security device, such as a firewall or IPS, but there may also be multiple host-based security devices capable of generating events, such as anti-virus, application whitelisting, intrusion detection and prevention systems (HIDS/HIPS), firewalls, or other security devices (see Chapter 9, “Establishing Zones and Conduits”). One example is industrial security appliances

|                       |          | Predicted classification                                     |  |
|-----------------------|----------|--|--|
|                       |          | Negative   | Positive   |
| Actual classification | Negative | <b>True negative</b><br><i>Correctly - Not identified</i>    | <b>False positive</b><br><i>Incorrectly - identified</i> |
|                       | Positive | <b>False negative</b><br><i>Incorrectly - Not identified</i> | <b>True positive</b><br><i>Correctly - identified</i>    |

Figure 1. Image278417.JPG

That use industrial protocol and application monitoring to enforce how industrial protocols are used.

These logs might provide much more specific data to a zone than do general security events, as seen in the example below from a Tofino industrial security appliance that provides detailed information pertaining to the unauthorized use of an industrial protocol (Modbus/TCP) function code (6 = “write single register”):

```
May20 09:25:50 169.254.2.2Apr 14 19:47:32
00:50:C2:B3:23:56
CEF:1|TofinoSecurity Inc|TofinoSA|02.0.00|300008|TofinoModbus/
TCPEnforcer:Function Code List Check|6.0|msg =
Functioncode 6 isnot in permitted function code list
TofinoMode = OPERATIONAL smac = 9c:eb:02:a6:22 src =
192.168.1.126 spt = 32500
```

```
dmac= 00:00:bc:cf:6b:08 dst = 192.168.1.17 dpt = 502 proto
= TCP TofinoEthType = 800 TofinoTTL= 64 TofinoPhysIn = eth0
```

In contrast, a generic Snort IDS might produce a syslog event string identifying a perimeter policy violation, such as the attempted Windows update shown below, but cannot provide the context of application function codes within the industrial network (see Chapter 6, “Industrial Network Protocols”).

```
Jan 01 00:00:00 [69.20.59.59] snort:[1:2002948:6] ETPOLICY
External Windows Updatein Progress [**] [Classification:
Potential Corporate Privacy Violation][Priority:1]
{TCP} 10.1.10.33:1665
->192.168.25.35:80
```

An often-overlooked step prior to commissioning any device that will generate security events is to “tune” or validate that normal traffic does not trigger events. Figure 2 illustrates how a complete rule set for a Tofino Security Appliance might look once commissioned. Note that only the last rule (as indicated by the arrow) is actually enforcing segregation on the conduit by performing deep-packet inspection on Modbus/TCP (502/tcp) traffic originating in the ICS Host zone and destined for the ICS Controllers zone. There are many other types of valid traffic that is generated to support functionality like the Network Neighborhood used in Windows operating systems and Neighboring Switches/Routers typical in both IT and OT network devices that is commonly sent to broadcast and multicast addresses. This valid traffic, if not properly handled with “drop-no log” entries in the rule

set would generate “false positives” in terms of the security events within an industrial network. Some of the traffic that must be considered include

- Windows NetBIOS Traffic – Name Resolution Service (137/udp) and Datagram Server (138/udp)
- Multicast DNS (5353/udp)
- Link-Layer Multicast Name Resolution (5355/udp)
- Universal Plug ‘n Play (1900/udp and 2869/tcp)
- Web Services Discovery Protocol (3702/udp)
- Cisco Discovery Protocol
- Link Layer Discovery Protocol
- Internet Control Message Protocol (IP Protocol 1)
- Internet Group Management Protocol (IP Protocol 2)
- Internet Protocol Version 6 (IPv6).

**ASSETS**

Assets – the physical devices connected to the network – also provide security data, typically in the form of logs. Assets can produce logs that track activity on a variety of levels. The operating system itself produces many logs, including system logs, application logs, and file system logs.

System logs are useful for tracking the status of devices and the services that are (or are not) running, as well as when patches are (or are not) applied. Logs are useful for determining the general health of an asset, as well as validating that approved ports and services are running. These logs are valuable in tracking which users (or applications) have authenticated to the asset, satisfying several compliance requirements. The following represents individual records from a Redhat Linux system log showing a successful user login, and a Windows failed authentication:

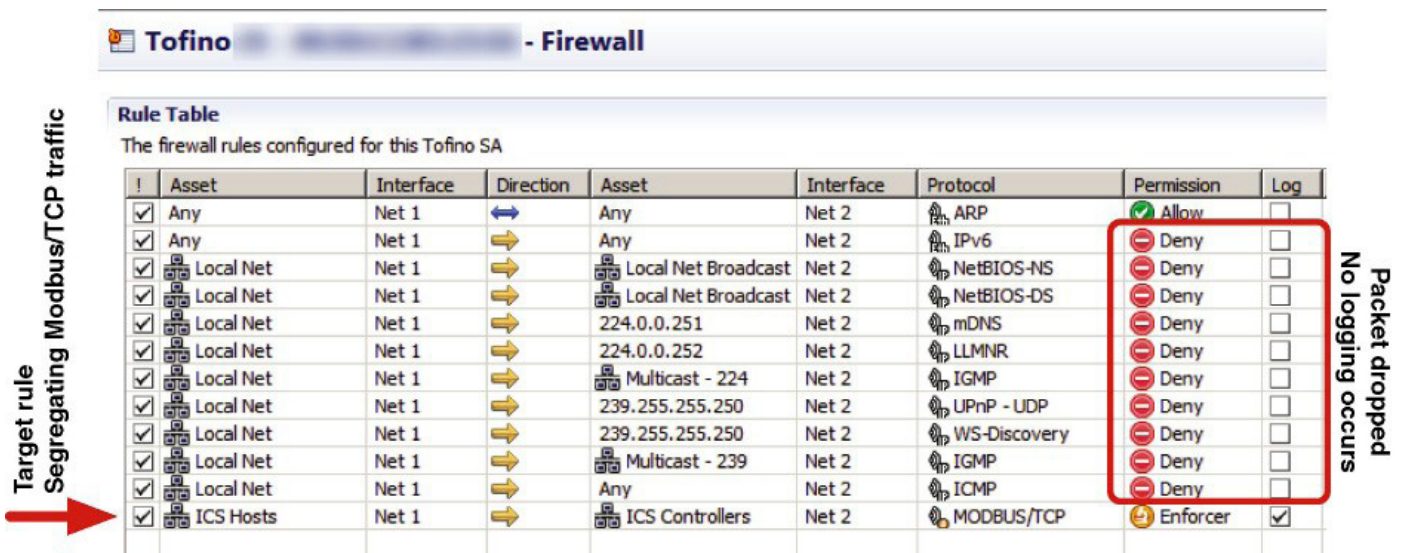


Figure 2. Tuning an industrial network security appliance

```
<345>Mar17 11:23:15 localhostsshd[27577]:Accepted password
forknapp from ::ffff:10.1.1.1port 2895 ssh2
<345>Fri Mar17 11:23:152011 680 Security SYSTEM User
Failure
Audit ENTERPRISEAccountLogon attempt by: MICROSOFT_
AUTHENTICATION_PACKAGE_V1_0Logonaccount: KNAPP Source
Workstation: ENTERPRISEError Code:0xC000006A 4574
```

Although syslog is ubiquitously used across a variety of systems, other event logging systems are used as well – the most notable of which is the Windows Management Instrumentation (WMI) framework. WMI produces auditable events in a structured data format that can be used against scripts (for automation) as well as by other Windows operating system functions.<sup>5</sup> Because syslog is so widely supported, WMI events are often logged using a Windows syslog agent, such as Snare for Windows to stream WMI events over syslog. It is also possible to configure log forwarding between Windows hosts when restrictions prohibit the installation of agents on critical assets using the Windows Event Collector functionality.

The following WMI event example indicates the creation of a new process on a Windows server:

```
Computer Name:WIN-0Z6H21NLQ05
EventCode:4688
Type: Audit Success(4) UserName:
Category: Process Creation Log File Name:Security
String[%1]:S-1-5-19
String[%2]: LOCAL SERVICE String[%3]: NT AUTHORITY
String[%4]:0x3e5
String[%5]:0xc008
String[%6]:C:\Windows\System32\RacAgent.exe
String[%7]: %%1936
String[%8]:0xc5e4
Message: Anewprocess has been created.Subject: Security
ID:
S-1-5-19Account Name: LOCAL SERVICEAccountDomain:
NT AUTHORITY LogonID: 0x3e5 Process
Information:NewProcessID: 0xc008 New ProcessName: C:\
Windows\System32\RacAgent.exe Token Elevation Type:
TokenElevationTypeDefault (1)CreatorProcessID: 0xc5e4
Token ElevationType indicatethe type of token thatwas
assigned to the newprocessinaccordance with User
Account Control policy. Type1isa fulltoken with no
privileges removed orgroups disabled.Afull token
isonly used if User Account Controlis disabled or
ifthe user is the built-in Administrator account
or a serviceaccount. Type2isan elevated token with
no privileges removed or groups disabled.Anelevated
```

token isused when User Account Controlisenabled and the user chooses to startthe program usingRunas administrator.Anelevated token isalso used when an application isconfigured toalways require administrative privilegeor to always require maximumprivilege, and theuseris a member of theAdministratorsgroup. Type 3is a limited token withadministrative privileges removed andadministrativegroups disabled. The limited token isused when User Account Controlis enabled, the applicationdoes not requireadministrativeprivilege, and theuserdoes not choose to start theprogram using Runas administrator.

The same event, when collected via syslog using a WMI agent, such as Snare, might look like this:

```
<12345> Fri Mar17 11:23:15 2011||WIN-
0Z6H21NLQ05||4688||Audit
Success (4)|||ProcessCreation||Security||S-1-5-19||LOCAL
SERVICE||NT AUTHORITY||0x3e5||0xc008||C:\Windows\System32\
RacAgent.exe||%%1936||0xc5e4
```

Application logs (covered in more detail under the section “Applications”) provide a record of application-specific details, such as logon activities to an HMI, configuration changes, and other details that indicate how an application is being used. These Application Logs are an important component in the security associated with many ICS applications since these applications commonly utilize a single Windows logon authentication account and manage individual user actions via local application accounts and security settings.

File system logs typically track when files are created, changed, or deleted, when access privileges or group ownerships are changed, and similar details. File system logging is included in Windows using the Windows File Protection (WFP) within WMI, which is an “infrastructure for management data and operations on Windows-based operating systems.”<sup>6</sup> File monitoring in Unix and Linux systems is performed using auditd, as well as with other commercial file integrity monitoring (FIM) products, such as Tripwire ([www.tripwire.com](http://www.tripwire.com)) and nCircle ([www.ncircle.com](http://www.ncircle.com)). These logs are extremely valuable for assuring the integrity of important files stored on an asset – such as configuration files (ensuring that the asset’s configurations remain within policy), and the asset’s log files themselves (ensuring that logged activities are valid and have not been tampered with to cover up indications of illicit behavior).

<sup>5</sup> Microsoft. Windows Management Instrumentation. [http://msdn.microsoft.com/en-us/library/aa394582\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa394582(v=VS.85).aspx), January 6, 2011 (cited: March 3, 2011).

<sup>6</sup> Ibid.

## CONFIGURATIONS

Configuration monitoring refers to the process of monitoring baseline configurations for any indications of change,<sup>7</sup> and is only a small part of Configuration Management (CM). Basic configuration monitoring can be done at a rudimentary level through a combination of host configuration file monitoring (to establish the baseline), system and application log monitoring (to look for change actions), and FIM (to ensure that configurations are not altered). While this does not provide true CM, it does provide an indication as to when established configurations are altered, providing a valuable security resource.

Full CM systems provide additional key functions, typically mapping at least partially to the security controls outlined in NIST SP 800-53 under the section “Configuration Management,” which provides a total of nine configuration management controls:<sup>8</sup>

- Configuration management policy and procedures – establishes a formal, documented configuration management policy.
- Baseline configurations – identifying and documenting all aspects of an asset’s configurations to create a secure template against which all subsequent configurations are measured.
- Change control – monitoring for changes and comparing changes against the established baseline.
- Security impact analysis – the assessment of changes to determine and test how they might impact the security of the asset.
- Access restrictions for change – limiting configuration changes to a strict subset of administrative users.
- Configuration settings – identification, monitoring, and control of security configuration settings and changes thereto.
- Least functionality – the limitation of any baseline configuration to provide the least possible functionality to eliminate unnecessary ports and services.
- Information service (IS) component (asset) inventory – establishing an asset inventory to identify all assets that are subject to CM controls, as well as to detect rogue or unknown devices that may not meet baseline configuration guidelines.
- Establishment of a configuration management plan – assigning roles and responsibilities around an established CM policy to ensure that CM requirements are upheld.

Configuration management tools may also offer automated controls to allow batch configurations of assets across

<sup>7</sup> National Institute of Standards and Technology, Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August, 2009.

<sup>8</sup> Ibid.

large networks, which is useful for ensuring that proper baselines are used in addition to improving desktop management efficiencies. For the purposes of security monitoring, it is the monitoring and assessment of the configuration files themselves that is a concern. This is because an attacker will often attempt to either escalate user privileges in order to obtain higher levels of access, or alter the configurations of security devices in order to penetrate deeper into secured zones – both of which are detectable with appropriate CM controls in place.

The logs produced by the CM are therefore a useful component of overall threat detection by using change events in combination with other activities, such as an event correlation system. For example, a port scan, followed by an injection attempt on a database, followed by a configuration change on the database server is indicative of a directed penetration attempt. Change logs are also highly beneficial (and in some cases mandatory) for compliance and regulatory purposes, with configuration and change management being a common requirement of most industrial security regulations (see Chapter 13, “Standards and Regulations”).

### TIP

The problem with Configuration Management within ICS is that a large portion of the critical configuration information is retained in embedded devices often running proprietary or closed operating systems using nonstandard communication protocols. These devices (PLCs, RTUs, IEDs, SIS, etc.) represent the true endpoint with a connection to the physical process under control, making their configuration details (control logic, hardware configuration, firmware, etc.) one of the most critical components pertaining to the operational integrity of the ICS. While several available IT products, such as Tripwire, Solarwinds, and What’sUpGold, can provide configuration and change management for servers, workstations, and network devices, specialized products, such as Cyber Integrity™ by PAS and the Industrial Defender Automation Systems Manager from Lockheed Martin, provide not only the necessary database components to identify and track configuration changes, but an extensive library of system and device connectors necessary to extract configuration data from ICS components.

## APPLICATIONS

Applications run on top of the operating system and perform specific functions. While monitoring application logs can provide a record of the activities relevant to those functions, direct monitoring of applications using a dedicated application monitoring product or application con-

tent firewall will likely provide a greater granularity of all application activities. Application logs can indicate when an application is executed or terminated, who logs into the application (when application-level security is implemented), and specific actions performed by users once logged in. The information contained in application logs is a summary, as it is in all log records. A sample application log record generated by an Apache web server is provided here:

```
Jan 01 00:00:00 [69.20.32.12]93.80.237.221 - -
[24/ Feb/2011:01:56:33 -0000] "GET/spambot/
spambotmostseendownload.
php HTTP/1.0" 500 71224 "http://yandex.ru/yandsearch?text
= video.
krymtel.net" "Mozilla/4.0 (compatible; MSIE6.0; WindowsNT
5.1; MRA 4.6 (build01425))"
```

A corresponding application log entry from an ICS illustrating a local access level change is shown here:

```
Jan 01 00:00:00 ICSSERVER1HMI1LEVEL SecurityLevel Admin
Jan 01 00:00:00 ICSSERVER1HMI1LEVEL SecurityLevel Oper
```

For a more detailed accounting of application activity, an application monitoring system can be used. For example, while it is possible that malware might be downloaded over HTTP, and be indicated in a log file, such as the first example shown earlier, monitoring an application's contents across a session could indicate malware that is

embedded in a file being downloaded from an otherwise normal-seeming website, as shown in Figure 3.

## NETWORKS

Network flows are records of network communications, from a source to one or more destinations. Network infrastructure devices, such as switches and routers, usually track flows. Flow collection is typically proprietary to the network device manufacturer (e.g. Cisco supports Net-Flow, and Juniper supports J-Flow), although many vendors also support the sFlow standard (see Table 1).

Monitoring flows provides an overview of network usage over time (for trending analysis, capacity planning, etc.) as well as at any given time (for impact analysis, security assessment, etc.), and can be useful for a variety of functions, including<sup>9</sup>

- Network diagnosis and fault management.
- Network traffic management or congestion management.
- Application management, including performance management, and application usage assessments.
- Application and/or network usage accounting for billing purposes.
- Network security management, including the detection of unauthorized devices, traffic, and so on.

Network flow analysis is extremely useful for security analysis because it provides the information needed to trace the communications surrounding a security incident back to its source. For example, if an application

<sup>9</sup> Flow.org, Traffic Monitoring using sFlow. <http://www.sflow.org/sFlowOverview.pdf>, 2003 (cited: March 3, 2011).

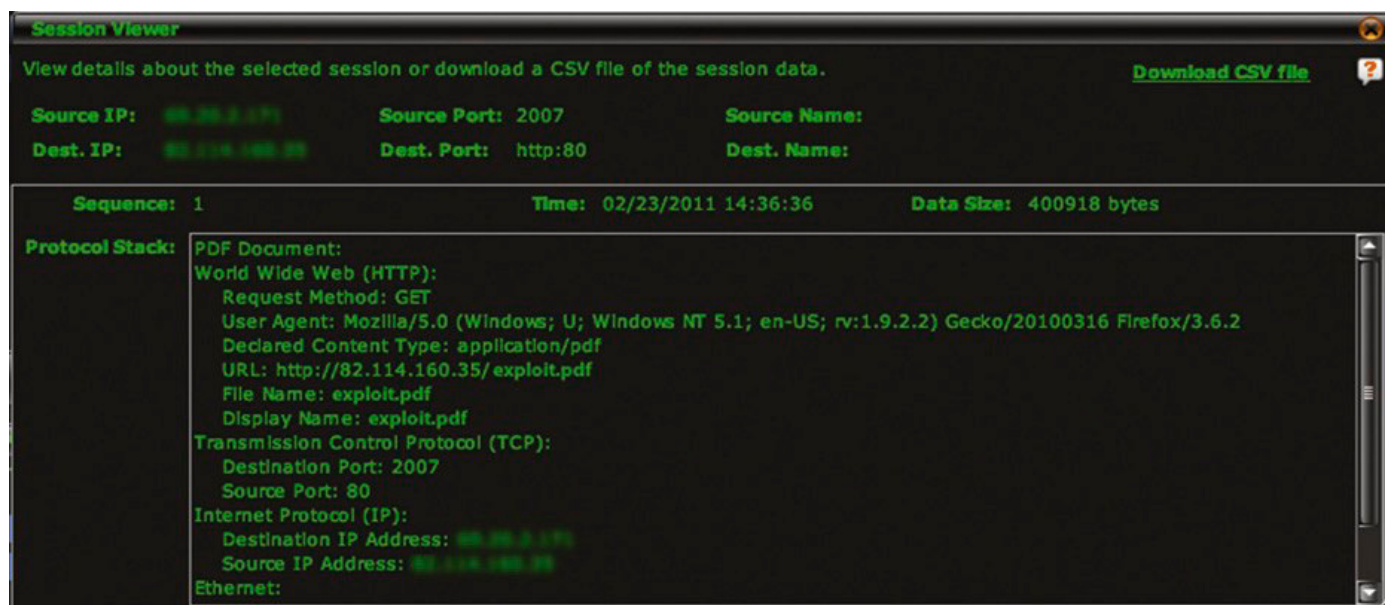


Figure 3. Application session details from an application monitor



**Table 1.** Network Flow Details

| Flow Detail                                | What It Indicates   | Security Ramifications  |
|--|---|---|
| SNMP interface indices (ifIndex in IF-MIB) | The size of the flow in terms of traffic volume (bytes, packets, etc.), as well as errors, latency, discards, physical addresses (MAC addresses), etc.                                  | SNMP details can provide indications of abnormal protocol operation that might indicate a threat<br>More germane to industrial networks, the presence of interface errors, latency, etc. can be directly harmful to the correct operation of many industrial protocols (see Chapter 6, "Industrial Network Protocols")<br>Essential for the correlation of communications against security events |
| Flow start time                            | When a network communication was initiated and when it ended  |   |
| Flow end time                              | Collectively, the start and stop timestamps also indicate the duration of a network communications  |   |
| Number of bytes/ packets                   | Indicates the "size" of the network flow, indicative of how much data is being transmitted  | Useful for the detection of abnormal network access, large file transfers, as might occur during information theft (e.g. retrieving a large database query result, downloading sensitive files, etc.)<br>Essential for the correlation of related logs and security events (which often track IP address details)   |
| Source and destination IP addresses        | Indicates where a network communication began and where it was terminated   | IP addresses may also be used to determine the physical switch or router interface of the asset, or   |
| Source and destination port                | Note that in non-IP industrial networks, the flow may terminate at the IP address of an MI or PLC even though communications may continue over specialized industrial network protocols | even the geographic location of the asset (through the use of a geolocation service)  |

whitelisting agent detects malware on an asset, it is extremely important to know where that malware came from, as it has already breached the perimeter defenses of the network and is now attempting to move laterally and infect adjacent machines. By correlating the malware attempt to network flows, it may be possible to trace the source of the malware and may also provide a path of propagation (i.e. where else did the virus propagate).

Network flow analysis also provides an indication of network performance for industrial network security. This is important because of the negative impact that network performance can have on process quality and efficiency, as shown in Table 1. An increase in latency can cause certain industrial protocols to fail, halting industrial processes.<sup>10</sup>

**CAUTION**

It is important to verify with the ICS supplier that network flow functionality can be enabled on the industrial network without negatively impacting the performance and integ-

ity of the network and its connected devices. Many industrial protocols include real-time extensions (see Chapter 6, "Industrial Network Protocols") that see switch performance issues when available forwarding capacity has been altered. Network vendors like Cisco have addressed this with special "lite" capabilities for netflow reporting. Always consult the ICS supplier before making modifications to recommended or qualified network topologies and operating parameters.

**USER IDENTITIES AND AUTHENTICATION**

Monitoring users and their activities is an ideal method for obtaining a clear picture of what is happening on the network, and who is responsible. User monitoring is also an important component of compliance management, as most compliance regulations require specific controls around user privileges, access credentials, roles, and behaviors. This requirement is enforced more so on systems that must comply with requirements, such as 21 CFR Part 11 and similar standards common in "FDA-regulated industries," such as pharmaceutical, food, and beverage.

10 B. Singer, Kenexis Security Corporation, in: D. Peterson (Ed.), Proceedings of the SCADA Security Scientific Symposium, 2: Correlating Risk Events and Process Trends to Improve Reliability, Digital Bond Press, 2010.

Unfortunately, the term “user” is vague – there are user account names, computer account names, domain names, host names, and of course the human user’s identity. While the latter is what is most often required for compliance management (see Chapter 13, “Standards and Regulations”), the former are what are typically provided within digital systems. Authentication to a system typically requires credentials in the form of a username and password, from a machine that has a host name, which might be one of several hosts in a named domain. The application itself might then authenticate to another backend system (such as a database), which has its own name and to which the application authenticates using yet another set of credentials. To further complicate things, the same human operator might need to authenticate to several systems, from several different machines, and may use a unique username on each. As mentioned earlier, ICS users may utilize a “common” Windows account shared by many, while each possesses a unique “application” account used for authentication and authorization within the ICS applications.

It is therefore necessary to normalize users to a common identity, just as it is necessary to normalize events to a common taxonomy. This can be done by monitoring activities from a variety of sources (network, host, and application logs), extracting whatever user identities might be present, and correlating them against whatever clues might be preset within those logs. For example, if a user authenticates to a Windows machine, launches an application and authenticates to it, and then the application authenticates to a backend system, it is possible to track that activity back to the original username by looking at the source of the authentications and the time at which they occurred. It can be assumed that all three authentications were by the same user because they occurred from the same physical console in clear succession.

As the systems become more complex and distributed, and as the number of users increases, each with specific roles and privileges, this can become cumbersome, and an automated identity management mechanism may be required.

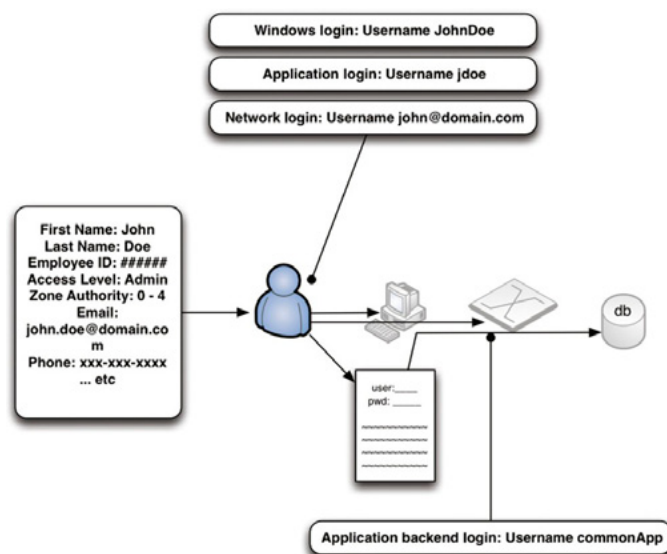
This process is made simpler through the use of common directories, such as Microsoft Active Directory and/or the Lightweight Directory Access Protocol (LDAP), which act as identity directories and repositories. However, there may still be several unique sets of credentials per human operator that are managed locally within the applications versus centrally via a directory service. The difficulty lies in the lack of common log formats, and the corresponding lack of universal identities between diverse systems. User monitoring therefore requires the extraction of user information from a variety of network and application

logs, followed by the normalization of that identity information. John Doe might log into a Windows domain using the username j.doe, have an e-mail address of jdoe@company.com, and log into a corporate intranet or Content Management System (CMS) as johnnyd, and so on. To truly monitor user behavior, it is necessary to recognize j.doe, jdoe, and johnnyd as a single identity.

Several commercial identity and access management (IAM) systems (also sometimes referred to as identity and authentication management systems) are available to facilitate this process. Some commercially available IAM systems include: NetIQ (formerly Novell and spun off as part of the merger with Attachmate), Oracle Identity Management (also encompassing legacy Sun Identity Management prior to Oracle’s acquisition of Sun Microsystems), and IBM’s Tivoli Identity. Other third-party identity solutions, such as Securonix Identity Matcher, offer features of both a centralized directory and IAM by mining identity information from other IAMs and normalizing everything back to a common identity.<sup>11</sup> More sophisticated SIEM and Log Management systems might also incorporate identity correlation features to provide user normalization. An authoritative source of identity is provided by managing and controlling authentications to multiple systems via a centralized IAM irrespective of the method used, as shown in Figure 4.

Once the necessary identity context has been obtained, it can be utilized in the information and event management process to cross-reference logs and events back to users. A SIEM dashboard shows both network and event details associated with their source users in Figure 5.

<sup>11</sup> Securonix, Inc., Securonix Identity Matcher: Overview. <http://www.securonix.com/identity.htm>, 2003 (cited: March 3, 2011).



**Figure 4.** Normalization of user identity

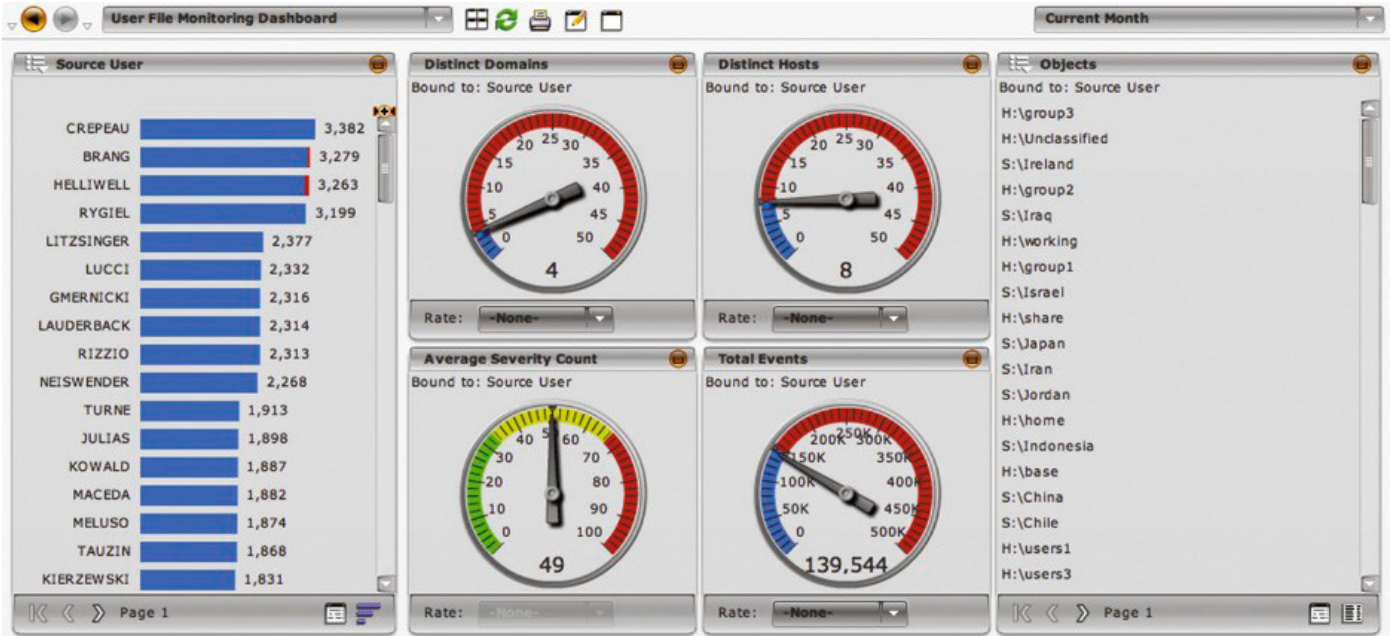


Figure 5. User activity related to file access as displayed by an SIEM

Table 2. Contextual Information Sources and Their Relevance

| Information Source                             | Provided Context  | Security Implications  |
|--|---|--|
| Directory services (e.g. active directory)     | User identity information, asset identity information, and access privileges  | Provides a repository of known users, assets, and roles that can be leveraged for security threat analysis and detection, as well as for compliance  |
| Identity and authentication management systems | Detailed user identity information, usernames and account aliases, access privileges, and an audit trail of authentication activity   | Enables the correlation of users to access and activities based upon privilege and policy. When used to enrich security events, provides a clear audit trail of activity versus authority that is necessary for compliance auditing  |
| Vulnerability scanner                          | Asset details including the operating system, applications in use (ports and services), patch levels, identified vulnerabilities, and related known exploits  | Enables security events to be weighted based upon the vulnerability of their target (i.e. a Windows virus is less concerning if it is targeting a Linux workstation)<br>Also provides valuable asset details for use in exception reporting, event correlation, and other functions                |
| Penetration tester                             | Exploitation success/failure, method of exploitation, evasion techniques, etc.  | Like with a vulnerability scanner, pen test tools provide the context of an attack vector. Unlike VA scan results, which show what could be exploited, a pen test indicates what has been exploited – which is especially useful for determining evasion techniques, detecting mutating code, etc. |
| Threat database/ CERT                          | Details, origins and recommendations for the remediation of exploits, malware, evasion techniques, etc.<br>Threat intelligence may also be used as “watchlists,” providing a cross-reference against which threats can be compared in order to highlight or otherwise call out threats of a specific category, severity, etc. | Threat intelligence can be used in a purely advisory capacity (e.g. providing educational data associated with a detected threat), or in an analytical capacity (e.g. in association with vulnerability scan data to weight the severity calculation of a detected threat)                         |

## ADDITIONAL CONTEXT

While user identity is one example of contextual information, there is a wealth of additional information available that can provide context. This information – such as vulnerability references, IP reputation lists, and threat directories – supplements the monitored logs and events with additional valuable context. Examples of contextual information are provided in Table 2.

Contextual information is always beneficial, as the more context is available for any specific event or group of events, the easier it will be to assess relevance to specific security and business policies. This is especially true because the logs and events being monitored often lack the details that are most relevant, such as usernames (see Figure 6).<sup>12</sup>

It is important to know that contextual information adds to the total volume of information already being assessed. It is therefore most beneficial when used to enrich other security information in an automated manner (see section “Information Management”).

## BEHAVIOR

Behavior is not something that is directly monitored, rather it is the analysis of any monitored metric (obtained from a log, network flow, or other source) over time. The result is an indication of expected versus unexpected activity, which is extremely useful for a wide range of security functions, including anomaly-based threat detection, as well as capacity or threshold-based alarming. Behavior is

<sup>12</sup> A. Chuvakin, Content Aware SIEM. <http://www.sans.org/security-resources/idxfaq/vlan.php> February, 2000 (cited: January 19, 2011).

also a useful condition in security event correlation (see Chapter 11, “Exception, Anomaly, and Threat Detection”).

Behavior analysis is often provided by security log and event monitoring tools, such as log management systems, SIEMs, and network behavior anomaly detection (NBAD) systems. If the system used for the collection and monitoring of security information does not provide behavioral analysis, an external tool, such as a spreadsheet or statistics program, may be required.

## SUCCESSFULLY MONITORING SECURITY ZONES

Understanding what to monitor is only the first step – actually monitoring all of the users, networks, applications, assets, and other activities still needs to happen. The discussion of what to monitor focused heavily on logs, because log files are designed to describe activities that have occurred, are fairly ubiquitous, and are well understood. Log files are not always available however, and may not provide sufficient detail in some instances. Therefore, monitoring is typically performed using a combination of methods, including the following:

- Log collection and analysis
- Direct monitoring or network inspection
- Inferred monitoring via tangential systems.

Except in pure log-collection environments, where logs are produced by the assets and network devices that are already in place, specialized tools are required to monitor the various network systems. The results of moni-

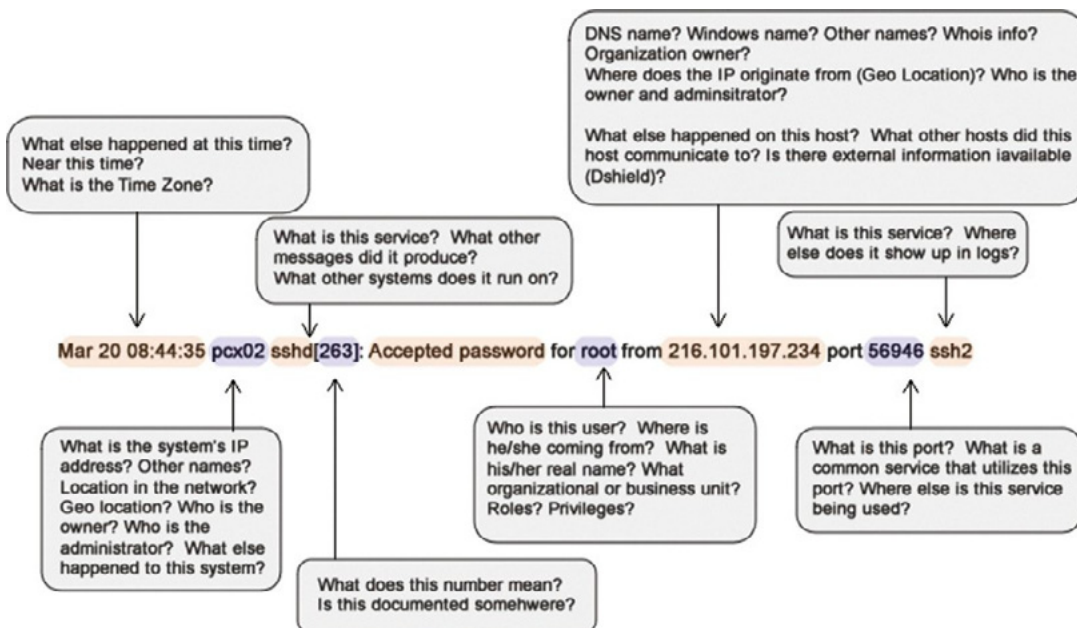


Figure 6. A log file, illustrating the lack of context image

toring (by whatever means) needs to be dealt with, because while manual logs and event reviews are possible (and allowed by most compliance regulations), automated tools are available and are recommended.

The central analysis of monitored systems is contrary to a security model built upon functional isolation. This is true because industrial networks should be separated into functional security zones, and centralized monitoring requires that log and event data either remain within a functional group (limiting the value for overall situation awareness of the complete system) or be shared between zones (potentially putting the security of the zone at risk). In the first scenario, logs and events are not allowed across the zone perimeter where they may be collected, retained, and analyzed only by local systems within that zone. In the second scenario, special considerations must be made for the transportation of log and event data across zone perimeters to prevent the introduction of a new inbound attack vector. A common method is to implement special security controls (such as a data diode, unidirectional gateway, or firewall configured to explicitly deny all inbound communications) to ensure that the security data are only allowed to flow toward the centralized management system. A hybrid approach may be used in industrial networks where critical systems in remote areas need to operate reliably. This provides local security event and log collection and management so that the zone can operate in total isolation, while also pushing security data to a central location to allow for more complete situational awareness across multiple zones.

## LOG COLLECTION

Log collection is simply the collection of logs from whatever sources produce them. This is often a matter of directing the log output to a log aggregation point, such as a network storage facility and/or a dedicated Log Management system. Directing a log is often as simple as directing the syslog event data service to the IP address of the aggregator. In some cases, such as WMI, events are stored locally within a database rather than as log files. These events must be retrieved, either directly (by authenticating to Windows and querying the event database via the Windows Event Collector functionality) or indirectly (via a software agent, such as Snare, which retrieves the events locally and then transmits them via standard syslog transports).

## DIRECT MONITORING

Direct monitoring refers to the use of a “probe” or other device to passively examine network traffic or hosts by placing the device in-line with the network. Direct monitoring is

especially useful when the system being monitored does not produce logs natively (as is the case with many industrial network assets, such as RTUs, PLCs, and IEDs). It is also useful as a verification of activity reported by logs, as log files can be altered deliberately in order to hide evidence of malicious activities. Common monitoring devices include firewalls, intrusion detection systems (IDSs), database activity monitors (DAMs), application monitors, and network probes. These are often available commercially as software or appliances, or via open-source distributions, such as Snort (IDS/ IPS), Wireshark (network sniffer and traffic analyzer), and Kismet (wireless sniffer).

Often, network monitoring devices produce logs of their own, which are then collected for analysis with other logs. Network monitoring devices are sometimes referred to as “passive logging” devices because the logs are produced without any direct interaction with the system being monitored. Database activity monitors, for example, monitor database activity on the network – often on a span port or network tap. The DAM decodes network packets and then extracts relevant SQL transactions in order to produce logs. There is no need to enable logging on the database itself resulting in no performance impact to the database servers.

In industrial networks, it is similarly possible to monitor industrial protocol use on the network by providing “passive logging” to those industrial control assets that do not support logging. Passive monitoring is especially important in these networks, as many industrial protocols operate in real time and are highly susceptible to network latency and jitter. This is one reason why it is difficult to deploy logging agents on the devices themselves (which would also complicate asset testing policies), making passive network logging an ideal solution in these cases. Special consideration to any industrial network redundancy should also be considered when deploying network-based monitoring solutions.

In some instances, the device may use a proprietary log format or event streaming protocol that must be handled specially. Cisco’s Security Device Event Exchange protocol (SDEE) (used by most Cisco IPS products) requires a username and password in order to authenticate with the security device so that events can be retrieved on demand, and/or “pushed” via a subscription model. While the end result is the same, it is important to understand that syslog is not absolutely ubiquitous.

## INFERRED MONITORING

Inferred monitoring refers to situations where one system is monitored in order to infer information about another system. Many applications connect to a database. So as

an example, monitoring the database in lieu of the application itself will provide valuable information about how the application is being used, even if the application itself is not producing logs or being directly monitored by an Application Monitor.

**NOTE**

Network-based monitoring inevitably leads to the question, “Is it possible to monitor encrypted network traffic?” Many industrial network regulations and guidelines recommend the encryption of control data when these data are transferred between trusted security zones via untrusted conduits ... so how can these data be monitored via a network probe? There are a few options, each with benefits and weaknesses. The first is to monitor the sensitive network connection between the traffic source and the point of encryption. That is, encrypt network traffic externally using a network-based encryption appliance, such as the Certes Networks Enforcement Point (CEP) variable speed encryption appliances, and place the network probe immediately between the asset and the encryption. The second option is to utilize a dedicated network-based decryption device, such as the Netronome SSL Inspector. These devices perform deliberate, hardware-based man-in-the-middle attacks in order to break encryption and analyze the network contents for security purposes. A third option is not to monitor the encrypted traffic at all, but rather to monitor for instances of data that should be encrypted (such as industrial protocol function codes) but are not producing exception alerts indicating that sensitive traffic is not being encrypted.

To determine which tools are needed, start with your zone’s perimeter and interior security controls (see Chapter 9, “Establishing Zones and Conduits”) and determine which controls can produce adequate monitoring and which cannot. If they can, start by aggregating logs from the absolute perimeter (the demarcation between the least critical zone and any untrusted networks – typically the business enterprise LAN) to a central log aggregation tool (see the section “Information Collection and Management Tools”). Begin aggregating logs from those devices protecting the most critical zones, and work outward until all available monitoring has been enabled, or until the capacity of your log aggregation has become saturated. At this point, if there are remaining critical assets that are not being effectively monitored, it may be necessary to increase the capacity of the log aggregation system.

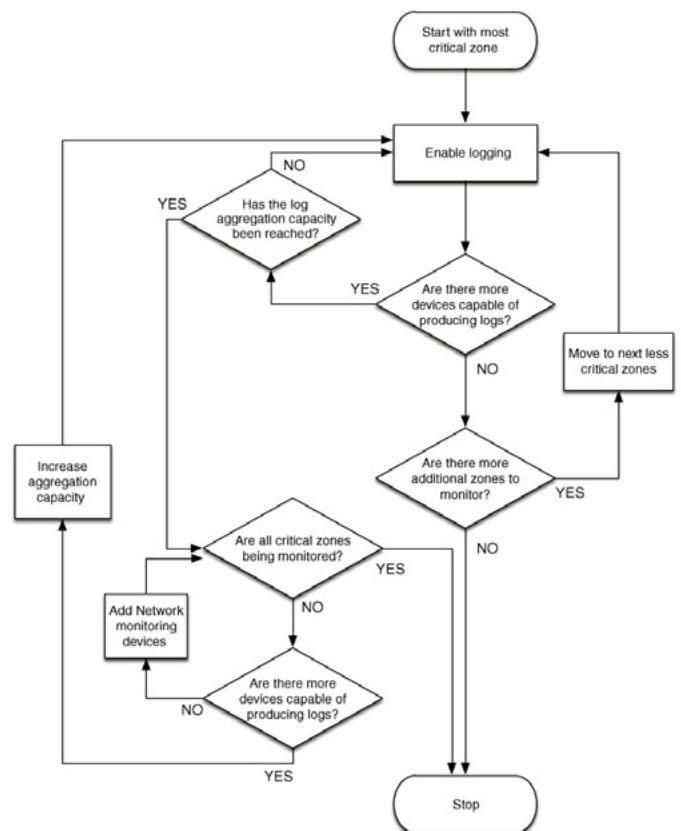
**TIP**

Adding capacity does not always mean buying larger, more expensive aggregation devices. Distribution is al-

so an option – keep all log aggregation local within each zone (or within groups of similar zones), and then aggregate subsets of each zone to a central aggregation facility for centralized log analysis and reporting. While this type of event reduction will reduce the effectiveness of threat detection and will produce less comprehensive reports from the centralized system, all the necessary monitoring and log collection will remain intact within the zones themselves, where they can be accessed as needed.

This concept is particularly well-suited for industrial networks in that it allows the creation of a local “dashboard” where relevant events for nearby assets can be displayed and responded to quickly by a “first responder” that may reside in the operational or plant environment, while offering the ability to export these events to upper-level aggregators that have a much broader view of more assets, and can focus more on event correlation and threat analysis typically performed in a security operations center.

If all logs are being collected and there are still critical assets that are not adequately monitored, it may be necessary to add additional network monitoring tools to compensate for these deficiencies. This process is illustrated in Figure 7.



**Figure 7.** Process for enabling zone monitoring

**CAUTION**

Remember that when aggregating logs it is still necessary to respect the boundaries of all established security zones. If logs need to be aggregated across zones (which is helpful for the detection of threats as they move between zones), make sure that the zone perimeter is configured to only allow the movement of logs in one direction; otherwise, the perimeter could potentially be compromised. In most instances, simply creating a policy that explicitly states the source (the device producing logs) and the destination (the log aggregation facility) for the specified service (e.g. syslog, port 514) is sufficient in order to enforce a restricted one-way transmission of the log files. For critical zones, physical separation using a data diode or unidirectional gateway may be required to assure that all log transmissions occur in one direction, and that there is no ability for malicious traffic to enter the secure zone from the logging facility.

Additional monitoring tools might include any asset or network monitoring device, including host-based security agents, or external systems, such as an intrusion detection system, an application monitor, or an industrial protocol filter. Network-based monitoring tools are often easier to deploy, because they are by nature nonobtrusive and, if configured to monitor a spanned or mirrored interface, typically do not introduce latency.

**INFORMATION COLLECTION AND MANAGEMENT TOOLS**

The “log collection facility” is typically a log management system or a security information and event management (SIEM) system. These tools range from very simple to very complex and include free, open-source, and com-

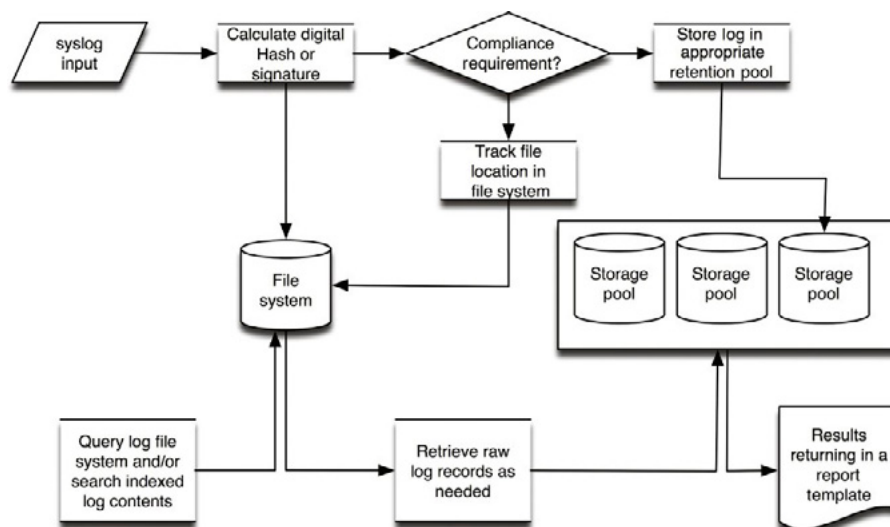
mercial options. Some options include syslog aggregation and log search, commercial log management systems, the open source security information management (OS-SIM) system, and commercial security information and event management systems.

**Syslog Aggregation and Log Search**

Syslog allows log files to be communicated over a network. By directing all syslog outputs from supported assets to a common network file system, a very simple and free log aggregation system can be established. While inexpensive (essentially free), this option provides little added value in terms of utilizing the collected logs for analysis, requiring the use of additional tools, such as open source log search or IT search tools, or through the use of a commercial log management system or SIEM. If logs are being collected for compliance purposes as well as for security monitoring, additional measures will need to be taken to comply with log retention requirements. These requirements include nonrepudiation and chain of custody, as well as ensuring that files have not been altered, or accessed by unauthorized users. This can be obtained without the help of commercial systems, although it does require additional effort by IT managers.

**Log Management Systems**

Log management systems provide a commercial solution for log collection, analysis, and reporting. Log management systems provide a configuration interface to manage log collection, as well as options for the storage of logs – often allowing the administrator to configure log retention parameters by individual log source. At the time of collection, log management systems also provide the necessary non-



**Figure 8.** Typical log management operations

repudiation features to ensure the integrity of the log files, such as “signing” logs with a calculated hash that can be later compared to the files as a checksum. Once collected, the logs can then also be analyzed and searched, with the ability to produce prefiltered reports in order to present log data relevant to a specific purpose or function, such as compliance reports, which produce log details specific to one or more regulatory compliance controls, as shown in Figure 8.

## Security Information and Event Management Systems

Security information and event management systems, or SIEMs, extend the capabilities of log management systems with the addition of specific analytical and contextual functions. According to security analysts from Gartner, the differentiating quality of a SIEM is that it combines the log management and compliance reporting qualities of a log management or legacy security information management (SIM) system with the real-time monitoring and incident management capabilities of a security event manager (SEM).<sup>13</sup> A SIEM must also support “data capture from heterogeneous data sources, including network devices, security devices, security programs, and servers,”<sup>14</sup> making the qualifying SIEM an ideal platform for providing situational awareness across security zone perimeters and interiors.

Many SIEM products are available, including the open-source variants (OSSIM by AlienVault), as well as several commercial SIEMs (ArcSight by Hewlett-Packard, QRadar by IBM, LogRhythm, Enterprise Security Manager by McAfee, and Splunk Enterprise), competing across a variety of markets, and offering a variety of value-added features and specializations.

Because a SIEM is designed to support real-time monitoring and analytical functions, it will parse the contents of a log file at the time of collection, storing the parsed information in some sort of structured data store, typically a database or a specialized flat-file storage system. By parsing out common values, they are more readily available for analytics, helping to support the real-time goals of the SIEM, as shown in Figure 9. The parsed data are used for analytics, while a more traditional log management framework that will hash the logs and retain them for forensic analysis, a logical connection between the log file and the parsed event data is typically maintained within the data store.

SIEM platforms are often used in security operations centers (SOCs), providing intelligence to security opera-

tors that can be used to detect and respond to security concerns. Typically, the SIEM will provide visual dashboards to simplify the large amounts of disparate data into a more human-readable form. Figure 10 illustrates how a custom dashboard is created within Splunk to visual ICS-related security events. Figure 11 shows how this dashboard can be expanded to provide more application-layer event information pertaining to industrial protocol security events (e.g. use of invalid function codes).

### NOTE

Log management and SIEM platforms are converging as information security needs become more closely tied to regulatory compliance mandates. Many traditional log management vendors now offer SIEM features, while traditional SIEM vendors are offering log management features.

### Data Historians

Data Historians are not security monitoring products, but they do monitor activity (see Chapter 4, “Introduction to Industrial Control Systems and Operations”) and can be a useful supplement to security monitoring solutions in several ways, including

- Providing visibility into control system assets that may not be visible to typical network monitoring tools.
- Providing process efficiency and reliability data that can be useful for security analysis.

Because most security monitoring tools are designed for enterprise network use, they are typically restricted to TCP and UDP-based IP networks and therefore have no

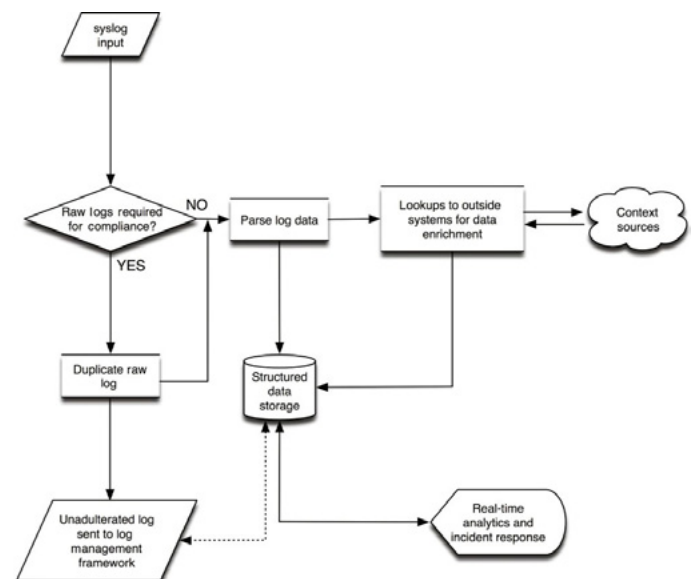


Figure 9. Typical SIEM operations

<sup>13</sup> K.M. Kavanagh, M. Nicolett, O. Rochford, “Magic quadrant for security information and event management,” Gartner Document ID Number: G00261641, June 25, 2014.

<sup>14</sup> Ibid.



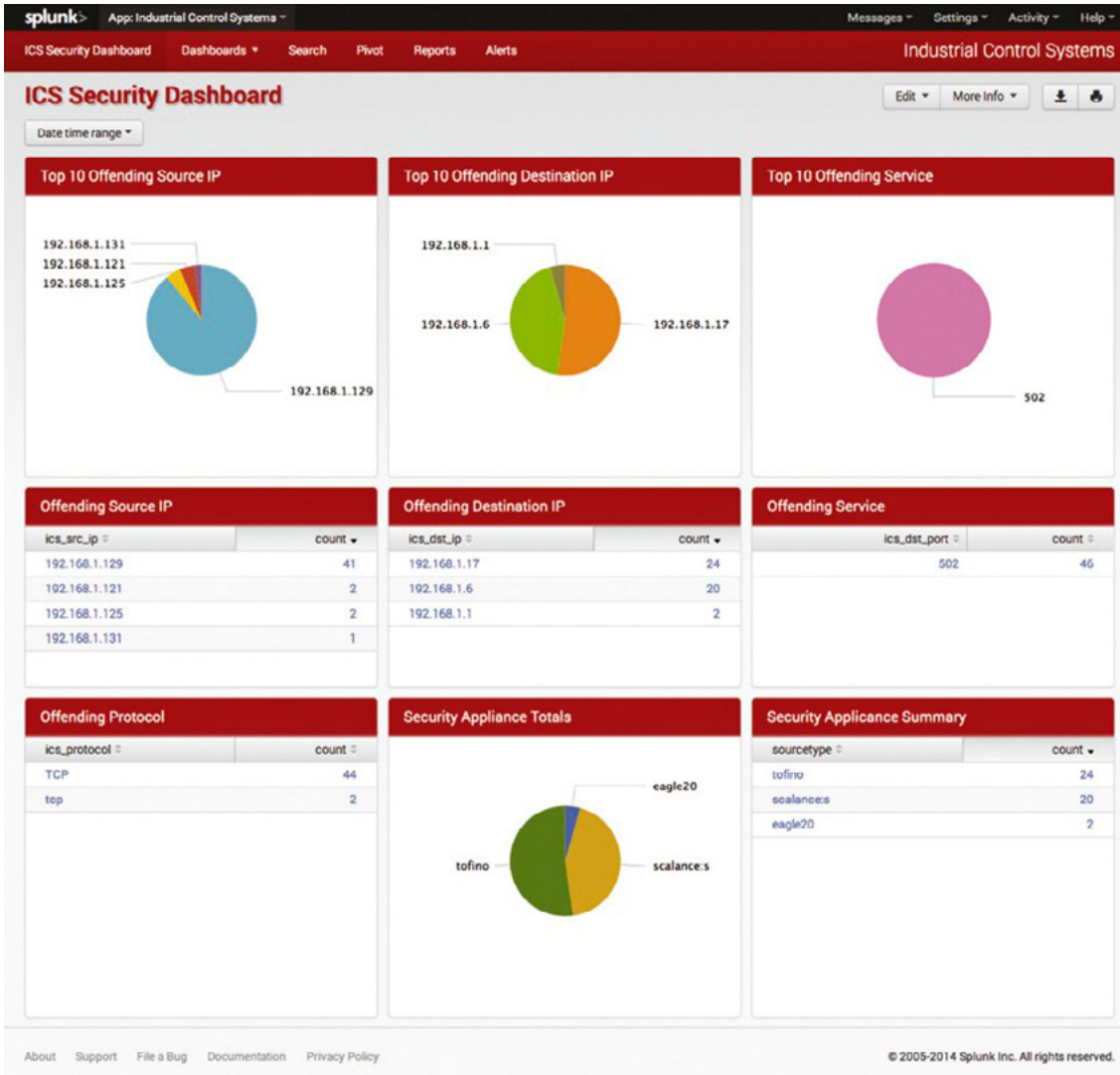


Figure 10. ICS security dashboard for Splunk

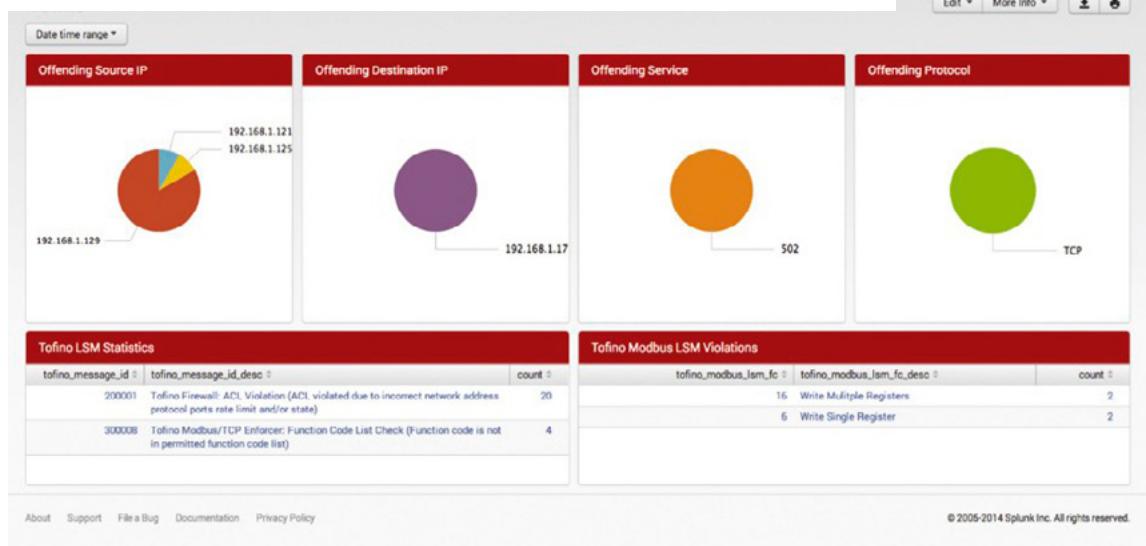


Figure 11. ICS security dashboard – application layer event analysis

visibility into large portions of most industrial plants that may utilize serial connectivity or other nonroutable protocols. Many industrial protocols are evolving to operate over Ethernet using TCP and UDP transports over IP, meaning these processes can be impacted by enterprise network activities. The security analysis capabilities of SIEM are made available to operational data by using the operational data provided by a Historian, allowing threats that originate in IT environments but target OT systems (i.e. Stuxnet and Dragonfly) to be more easily detected and tracked by security analysts. Those activities that could impact the performance and reliability of industrial automations systems can be detected as well by exposing IT network metrics to operational processes, including network flow activity, heightened latency, or other metrics that could impact the proper operation of industrial network protocols (see Chapter 6, “Industrial Network Protocols”).

## MONITORING ACROSS SECURE BOUNDARIES

As mentioned in the section “Successfully Monitoring Security Zones,” it is sometimes necessary to monitor systems across secure zone boundaries via defined conduits. This requires zone perimeter security policies that will allow the security logs and events generated by the monitoring device(s) to be transferred to a central man-

agement console. Data diodes are ideal for this application as they force the information flow in one direction – away from the zones possessing higher security levels and toward the central management system. If a firewall is used, any “hole” provided for logs and events represents a potential attack vector. The configuration must therefore explicitly limit the communication from the originating source(s) to the destination management system, by IP (Layer 3), Port (Layer 4), and preferably application content (Layer 7), with no allowed return communication path. Ideally, this communication would be encrypted as well, as the information transmitted could potentially be sensitive in nature.

## INFORMATION MANAGEMENT

The next step in security monitoring is to utilize the relevant security information that has been collected. Proper analysis of this information can provide the situational awareness necessary to detect incidents that could impact the safety and reliability of the industrial network.

Ideally, the SIEM or Log Manager will perform many underlying detection functions automatically – including normalization, data enrichment, and correlation (see Chapter 11, “Exception, Anomaly, and Threat Detection”) – providing the security analyst with the following types of information at their disposal:

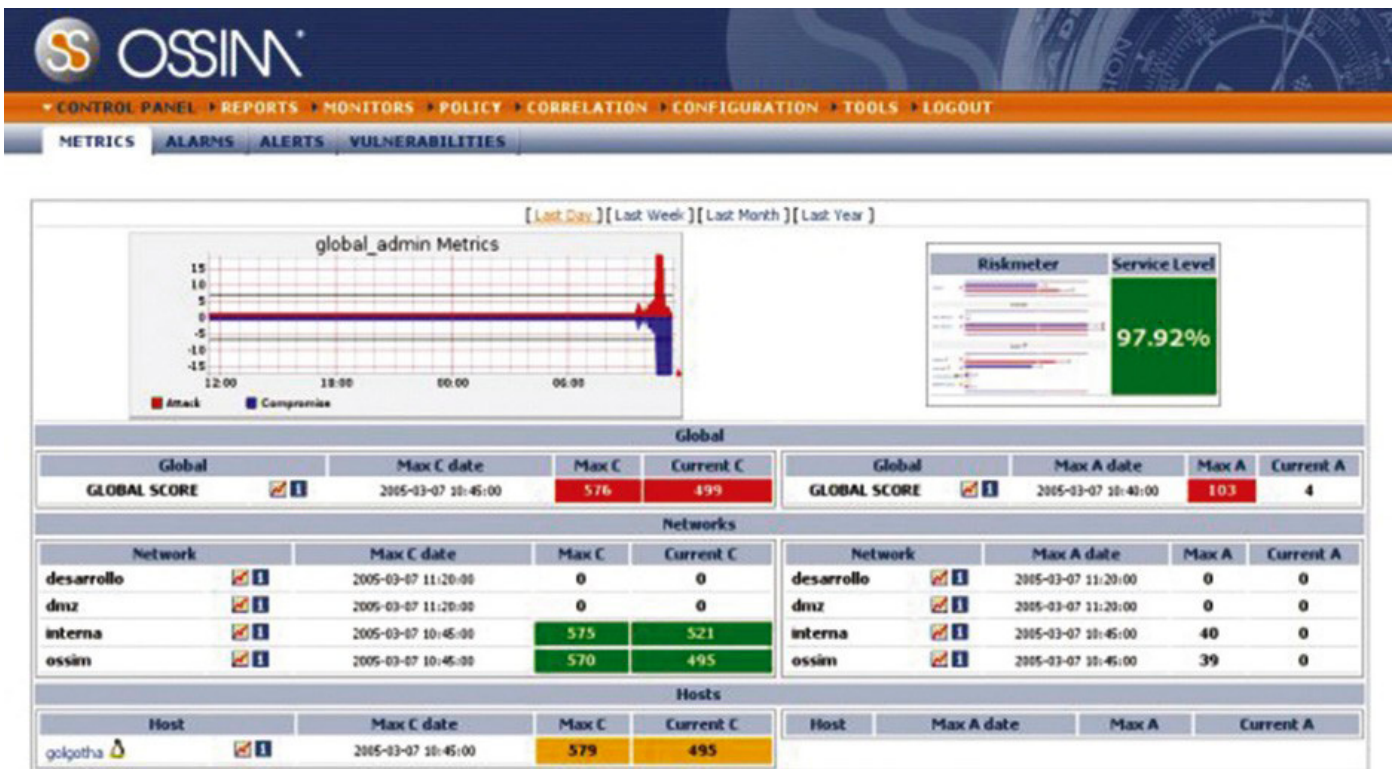


Figure 12. The Open SourceSecurityInformation Management project

- The raw log and event details obtained by monitoring relevant systems and services, normalized to a common taxonomy.
- The larger “incidents” or more sophisticated threats derived from those raw events that may include correlation with external global threat intelligence sources.
- The associated necessary context to what has been observed (raw events) and derived (correlated events).

Typically, an SIEM will represent a high-level view of the available information on a dashboard or console, as illustrated in Figure 12, which shows the dashboard of the Open Source Security Information Management (OS-SIM) platform. With this information in hand, automated and manual interaction with the information can occur. This information can be queried directly to achieve direct answers to explicit questions. It can also be formulated into a report to satisfy specific business, policy, or compliance goals, or it can be used to proactively or reactively notify a security or operations officer of an incident. The information is available to further investigate incidents that have already occurred.

## QUERIES

The term “query” refers to a request for information from the centralized data store. This can sometimes be an actual database query, using structured query language (SQL), or it may be a plain-text request to make the information more accessible by users without database ad-

ministration skills (although these requests may use SQL queries internally, hidden from the user). Common examples of initial queries include the following:

- Top 10 talkers (by total network bandwidth used)
- Top talkers (by unique connections or flows)
- Top events (by frequency)
- Top events (by severity)
- Top events over time
- Top applications in use
- Open ports.

These requests can be made against any or all data that are available in the data store (see the section “Data Availability”). By providing additional conditions or filters, queries can be focused yielding results more relevant to a specific situation. For example

- Top 10 talkers during non-business hours
- Top talkers using specific industrial network protocols
- All events of a common type (e.g. user account changes)
- All events targeting a specific asset or assets (e.g. critical assets within a specific zone)
- All ports and services used by a specific asset or assets
- Top applications in use within more than one zone.

Query results can be returned in a number of ways: via delimited text files, a graphical user interface or dash-

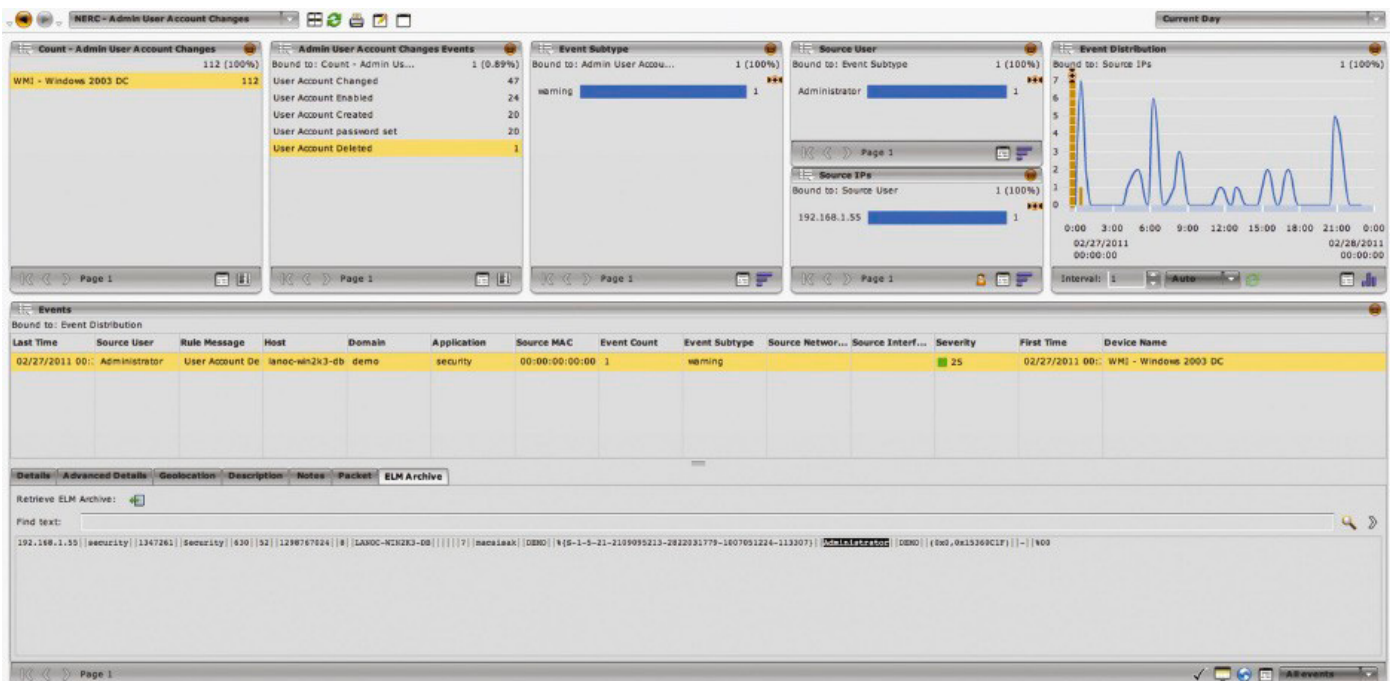


Figure 13. An SIEM dashboard showing administrative account changes



Figure 14. An example of a graphical interface for creating event correlation rules

board, preformatted executive reports, an alert that is delivered by SMS or e-mail, and so on. Figure 13 shows user activity filtered by a specific event type – in this example, administrative account change activities that correspond with NERC compliance requirements.

A defining function of an SIEM is to correlate events to find larger incidents (see Chapter 11, “Exception, Anomaly, and Threat Detection”). This includes the ability to define correlation rules, as well as present the results via a dashboard. Figure 14 shows a graphical event correlation editor that allows the logical conditions (such as “if A and B then C”), while Figure 15 shows the result of an incident query – in this case the selected incident (an HTTP Command and Control Spambot) being derived from four discrete events.

REPORTS

Reports select, organize, and format all relevant data from the enriched logs and events into a single document. Reports provide a useful means to present almost any data set. Reports can summarize high-level incidents for executives, or include precise and comprehensive documentation that provides minute details for internal auditing or for compliance. An example of a report generated by an SIEM is shown in Figure 16 showing a quick summary of the OSIsoft PI Historian authentication failures and point change activity.

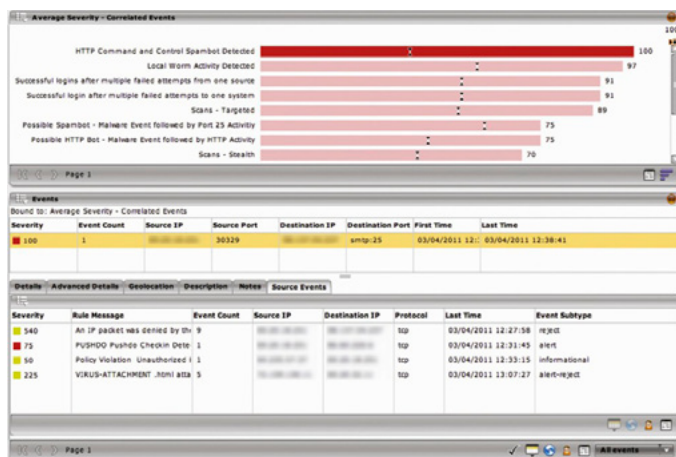


Figure 15. An SIEM dashboard a correlated event and its source events

ALERTS

Alerts are active responses to observed conditions within the SIEM. An alert can be a visual notification in a console or dashboard, a direct communications (e-mail, page, SMS, etc.) to a security administrator, or even the execution of a custom script. Common alert mechanisms used by commercial SIEMs include the following:

- Visual indicators (e.g. red, orange, yellow, green)
- Direct notification to a user or group of users
- Generation and delivery of a specific report(s) to a user or group of users
- Internal logging of alert activity for audit control
- Execution of a custom script or other external control
- Generation of a ticket in a compatible help desk or incident management system.

Several compliance regulations, including NERC CIP, CFATS, and NRC RG 5.71, require that incidents be appropriately communicated to proper authorities inside and/or outside of the organization. The alerting mechanism of an SIEM can facilitate this process by creating a useable variable or data dictionary with appropriate contacts within the SIEM and automatically generating appropriate reports and delivering them to key personnel.

INCIDENT INVESTIGATION AND RESPONSE

SIEM and log management systems are useful for incident response, because the structure and normalization of the data allow an incident response team to drill into a specific event to find additional details (often down to the source log file contents and/or captured network packets), and to pivot on specific data fields to find other related activities. For example, if there is an incident that requires investigation and response, it can be examined quickly providing relevant details, such as the username and IP address. The SIEM can then be queried to determine what other events are associated with the user, IP, and so on. In some cases the SIEM may support active response capabilities, including

- Allowing direct control over switch or router interfaces via SNMP, to disable network interfaces.
- Executing scripts to interact with devices within the network infrastructure, to reroute traffic, isolate users, and so on.
- Execute scripts to interact with perimeter security devices (e.g. firewalls) to block subsequent traffic that has been discovered to be malicious.
- Execute scripts to interact with directory or IAM systems to alter or disable a user account in response to observed malicious behavior.

Industrial Incidents

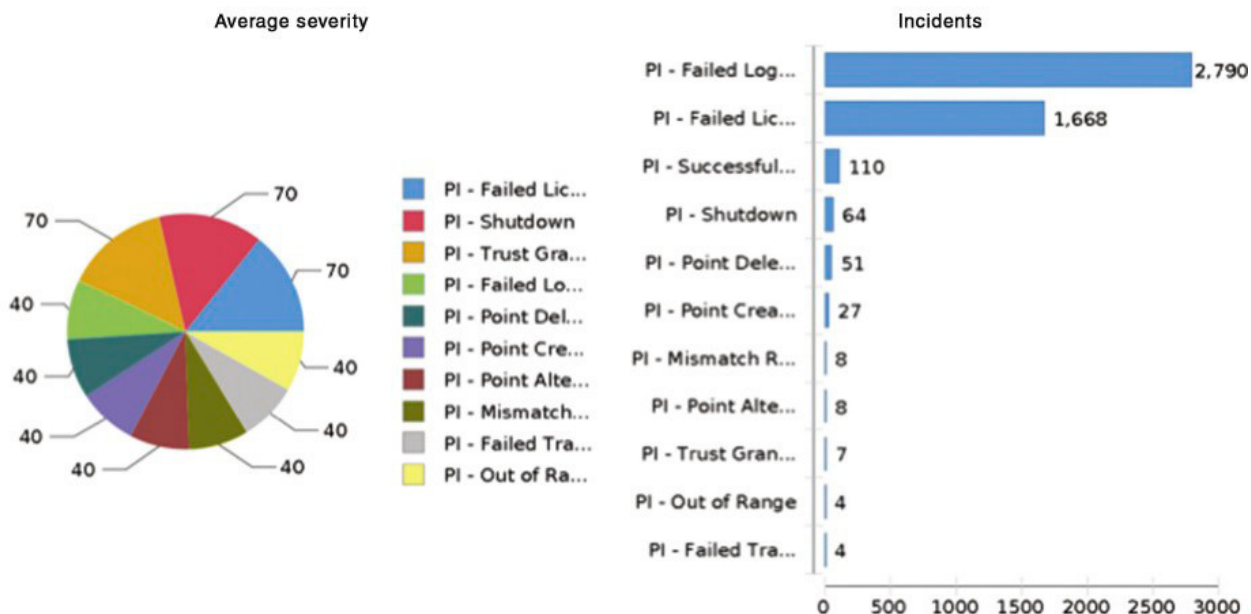
Report Generated: Mar 4, 2011 1:58 PM

Time Zone: Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London GMT+00:00

Report Period: 2011/01/01 00:00:00 to 2011/04/01 00:00:00

Device Count: 49

Incident overview



User and asset details

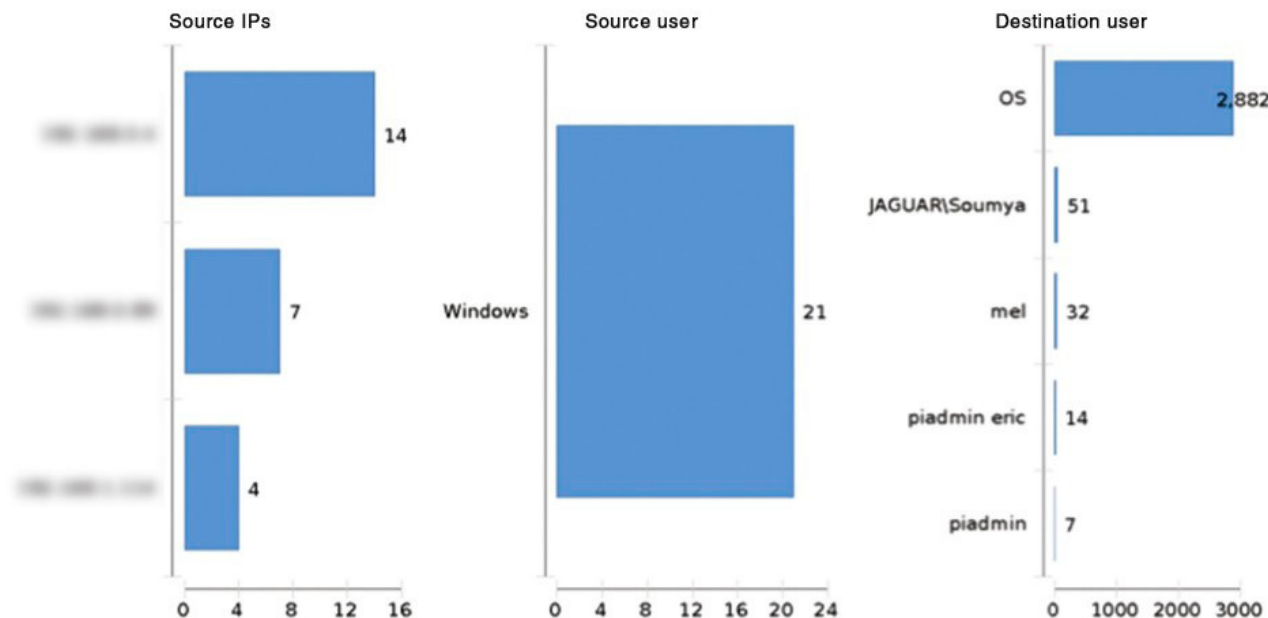


Figure 16. An SIEM report showing industrial activities

These responses may be supported manually or automatically, or both.

### CAUTION

While automated response capabilities can improve efficiencies, they should be limited to non-critical security zones and/or to zone perimeters. As with any control deployed within industrial networks, all automated responses should be carefully considered and tested prior to implementation. A false positive could trigger such a response and cause the failure of an industrial operation, with potentially serious consequences.

### LOG STORAGE AND RETENTION

The end result of security monitoring, log collection, and enrichment is a large quantity of data in the form of log files, which must be stored for audit and compliance purposes (in the cases where direct monitoring is used in lieu of log collection, the monitoring device will still produce logs, which must also be retained). This represents a few challenges, including how to ensure the integrity of the stored files (a common requirement for compliance), how and where to store these files, and how they can be kept readily available for analysis.

### NONREPUDIATION

Nonrepudiation refers to the process of ensuring that a log file has not been tampered with, so that the original raw log file can be presented as evidence, without question of authenticity, within a court of law. This can be achieved in several ways, including digitally signing log files upon collection as a checksum, utilizing protected storage media, or the use of third-party FIM systems.

A digital signature is typically provided in the form of a hash algorithm that is calculated against the log file at the time of collection. The result of this calculation provides a checksum against which the files can be verified to ensure they have not been tampered with. If the file is altered in any way, the hash will calculate a different value and the log file will fail the integrity check. If the checksum matches, the log is known to be in its original form.

The use of appropriate storage facilities can ensure nonrepudiation as well. For example, by using write once read many (WORM) drives, raw log records can be accessed but not altered, as the write capability of the drive prevents additional saves. Many managed storage area network (SAN) systems also provide varying levels of authentication, encryption, and other safeguards.

A FIM may already be in use as part of the overall security monitoring infrastructure, as described in the section “Assets.” The FIM observes the log storage facility for any

sign of changes or alterations, providing an added level of integrity validation.

### DATA RETENTION/STORAGE

The security monitoring tools just mentioned all require the collection and storage of security-related information. The amount of information that is typically required could easily surpass 170 GB over an 8-h period for a medium-sized enterprise collecting information at approximately 20,000 events per second.<sup>15</sup> It is worth mentioning that event generation within an industrial network is typically a small fraction of this number, and when properly tuned, presents a manageable amount of information storage.

Data retention refers to the amount of information that is stored long-term, and can be measured in volume (the size of the total collected logs in bytes) and time (the number of months or years that logs are stored for). The length of time a log is retained is important, as this metric is often defined by compliance regulations – NERC CIP requires that logs are retained for anywhere from 90 days to up to 3 years, depending upon the nature of the log.<sup>16</sup> The amount of physical storage space that is required can be calculated by determining which logs are needed for compliance and for how long they must be kept. Some of the factors that should be considered include the following:

- Identifying the quantity of inbound logs
- Determining the average log file size
- Determining the period of retention required for logs
- Determining the supported file compression ratios of the log management or SIEM platform being used.

Table 3 illustrates how sustained log collection rates map to total log storage requirements over a retention period of 7 years, resulting in a few terabytes ( $10^{12}$ ) of storage up to hundreds of terabytes or even petabytes ( $10^{15}$ ) of storage.

There may be a requirement to retain an audit trail for more than one standard or regulation depending upon the nature of the organization, often with each regulation mandating different retention requirements. As with NERC CIP, there may also be a change in the retention requirements depending upon the nature of the log, and whether an incident has occurred. All of this adds up to even greater, long-term storage requirements.

### TIP

Make sure that the amount of available storage has sufficient headroom to accommodate spikes in event activity,

<sup>15</sup> J.M. Butler, Benchmarking Security Information Event Management (SIEM). The SANS Institute Analytics Program, February, 2009.

<sup>16</sup> North American Electric Reliability Corporation. NERC CIP Reliability Standards, version 4. <http://www.nerc.com/page.php?cid=2> February 3, 2011 (cited: March 3, 2011).

because event rates can vary (especially during a security incident).

**DATA AVAILABILITY**

Data availability differs from retention, referring to the amount of data that is accessible for analysis. Also called “live” or “online” data, the total data availability determines how much information can be analyzed concurrently – again, in either volume (bytes and/or total number of events) or time. Data retention affects the ability of an SIEM to detect “low and slow” attacks (attacks that purposefully occur over a long period of time in order to evade detection), as well as to perform trend analysis and anomaly detection (which by definition requires a series of data over time – see Chapter 11, “Exception, Anomaly, and Threat Detection”).

**TIP**

In order to meet compliance standards, it may be necessary to produce a list of all network flows within a particular security zone that originated from outside of that zone, for the past 3 years. For this query to be successful, 3 years of network flow data need to be available to the SIEM at once. There is a work-around if the SIEM’s data availability is insufficient (for example, it can only keep 1 year of data active). The information can be stored in volumes consistent with the SIEM’s data availability by archiving older data sets. A partial result is obtained by querying the active data set. Two additional queries can be run by then restoring the next-previous backup or archive, producing multiple partial result sets of 1 year each. These results can then be combined to obtain the required 3-year report. Note that this requires extra effort on the part of the analyst. The archive/retrieval process on some legacy SIEMs may interfere with or interrupt the collection of new logs until the process is complete.

Unlike data retention, which is bound by the available volume of data storage (disk drive space), data availability is dependent upon the structured data that are used by the SIEM for analysis. Depending upon the nature of the data store, the total data availability of the system may be limited to a number of days, months, or years. Typically, one or more of the following limits databases:

- The total number of columns (indices or fields)
- The total number of rows (discreet records or events)
- The rate at which new information is inserted (i.e. collection rate)
- The rate at which query results are required (i.e. retrieval rates).

Depending upon the business and security drivers behind information security monitoring, it may be necessary to segment or distribute monitoring and analysis into zones to meet performance requirements. Some factors to consider when calculating the necessary data availability include

- The total length of time over which data analysis may be required by compliance standards.
- The estimated quantity of logs that may be collected in that time based on event estimates.
- The incident response requirements of the organization – certain governmental or other critical installations may require rapid-response initiatives that necessitate fast data retrieval.
- The desired granularity of the information that is kept available for analysis (i.e. are there many vs. few indices).

**SUMMARY**

A larger picture of security-related activity begins to form once zone security measures are in place. Exceptions from the established security policies can then be detect-

**Table 3. Log Storage Requirements Over Time**

| Logs per Second | Logs per Day (in Billions) | Logs per Year (in Billions) | Average Bytes per Event | Retention Period in Years | Raw Log Size (TB) | Compressed Bytes (TB) 5:1 | Compressed Bytes (TB) 10:1 |
|-----------------|----------------------------|-----------------------------|-------------------------|---------------------------|-------------------|---------------------------|----------------------------|
| 100,000         | 8.64                       | 3154                        | 508                     | 7                         | 10,199            | 2040                      | 1020                       |
| 50,000          | 4.32                       | 1577                        | 508                     | 7                         | 5,100             | 1020                      | 510                        |
| 25,000          | 2.16                       | 788                         | 508                     | 7                         | 2,550             | 510                       | 255                        |
| 10,000          | 0.86                       | 315                         | 508                     | 7                         | 1,020             | 204                       | 102                        |
| 5,000           | 0.43                       | 158                         | 508                     | 7                         | 510               | 102                       | 51                         |
| 1,000           | 0.09                       | 32                          | 508                     | 7                         | 102               | 21                        | 11                         |
| 500             | 0.04                       | 16                          | 508                     | 7                         | 51                | 11                        | 6                          |

ed by measuring these activities and further analyzing them. Anomalous activities can also be identified so that they may be further investigated.

This requires well-defined policies with those policies configured within an appropriate information analysis tool. Just as with perimeter defenses to the security zone, carefully built variables defining allowed assets, users, applications, and behaviors can be used to aid in detection of security risks and threats. If these lists can be determined dynamically, in response to observed activity within the network, the “whitelisting” of known-good policies, becomes “smart-listing.” This helps further strengthen perimeter defenses through dynamic firewall configuration or IPS rule creation.

The event information can be further analyzed as various threat detection techniques are used together by event correlation systems that find larger patterns more indicative of serious threats or incidents. Widely used in IT network security, event correlation is beginning to “cross the divide” into OT networks, at the heels of Stuxnet and other sophisticated threats that attempt to compromise industrial network systems via attached IT networks and services.

Everything (measured metrics, baseline analysis, and whitelists) rely on a rich base of relevant security information. Where does this security information come from? The networks, assets, hosts, applications, protocols, users, and everything else that is logged or monitored contributes to the necessary base of data required to achieve “situational awareness” and effectively secure an industrial network.

#### ABOUT THE AUTHOR

*Eric D. Knapp is a recognized expert in industrial control systems (ICS) cyber security. He is the original author of “Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (First Edition)” and the*

*coauthor of “Applied Cyber Security for Smart Grids.” Eric has held senior technology positions at NitroSecurity, McAfee, Wurdtech, and Honeywell, where he has consistently focused on the advancement of end-to-end ICS cyber security in order to promote safer and more reliable automation infrastructures. Eric has over 20 years of experience in Information Technology, specializing in cyber security analytics, threat, and risk management techniques and applied Ethernet protocols in both enterprise and industrial networks. In addition to his work in information security, Eric is an award-winning fiction author. He studied English and Writing at the University of New Hampshire and the University of London, and holds a degree in communications.*

#### ABOUT THE AUTHOR

*Joel Thomas Langill brings a unique perspective to operational security with decades of experience in industrial automation and control. He has deployed ICS solutions covering most major industry sectors globally encompassing most generations of automated control. He has been directly involved in automation solutions spanning feasibility, budgeting, front-end engineering design, detailed design, system integration, commissioning, support and legacy system migration. Joel is currently an independent consultant providing services to ICS suppliers, end-users, system integrators, and governmental agencies worldwide. Joel founded the popular ICS security website SCADAhacker.com offering visitors resources in understanding, evaluating, and securing control systems. He developed a specialized training curriculum that focuses on applied cyber security and defenses for industrial systems. His website and social networks extends to readers in over 100 countries globally.*

*Joel serves on the Board of Advisors for Scada Fence Ltd., and is an ICS research focal point to corporations and CERT organizations around the world. He is a voting member of the ISA99 committee, and has published numerous reports on ICS-related campaigns including Heartbleed, Dragonfly, and Black Energy. He is a graduate of the University of Illinois–Champaign with a BS (University Honors/Bronze Tablet) in Electrical Engineering.*

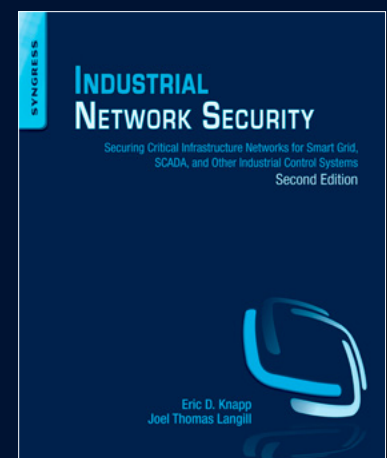
*He can be found on Twitter @SCADAhacker*

# Industrial Network Security Privacy, and Ethics

## Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

by Eric D. Knapp Joel Thomas Langill

<http://store.elsevier.com/>














**NET OPEN SERVICES** IS AN APPLICATION HOSTING COMPANY FOCUSED ON OPEN SOURCE APPLICATIONS MANAGEMENT IN HIGH AVAILABILITY ENVIRONMENT.

NET OPEN SERVICES IS PROUD TO PROVIDE A HIGH QUALITY SERVICE TO OUR CUSTOMERS SINCE 10 YEARS.

OUR EXPERTISE INCLUDES:

-  CLOUD COMPUTING, PUBLIC, PRIVATE AND HYBRID CLOUD MANAGEMENT (OPENSTACK, CLOUDSTACK, RED HAT ENTERPRISE VIRTUALIZATION)
-  REMOTE MONITORING AND MANAGEMENT 24/7
-  NETWORKING AND SECURITY (OPEN BSD, IP TABLE, CHECKPOINT, CISCO,...)
-  OS AND APPLICATION MANAGEMENT (FREE BSD, OPEN BSD, SOLARIS, UNIX, LINUX, AIX, MS WINDOWS)
-  DATABASE MANAGEMENT (ORACLE, MYSQL, CASSANDRA, NOSQL, MS SQL, SYBASE...)
-  MANAGED HOSTING IN CARRIER CLASS DATA CENTERS
-  DISASTER RECOVERY



WE PROVIDE SERVICES IN EVERY STEP OF THE PROJECT LIFE, DESIGN, DEPLOYMENT, MANAGEMENT AND EVOLUTIONS. NETOPENSERVICES TEAM INCLUDES EXPERIENCED LEADERS AND ENGINEERS IN THE INTERNET SERVER INDUSTRY.

OUR TEAM HAS 15 YEARS OF EXPERIENCE IN DEVELOPING INTERNET INFRASTRUCTURE-GRADE SOLUTIONS AND PROVISIONING INTERNET DATACENTERS AND GLOBAL SERVICE NETWORKS TOGETHER.

WE OFFER EXCEPTIONAL HARDWARE SUPPORT AS SOFTWARE SUPPORT ON UNIX/LINUX AND OPEN SOURCE APPLICATION. NETOPENSERVICES DELIVERS THESE CUSTOM-BUILT LINUX AND UNIX SERVERS, AS WELL AS PRECONFIGURED SERVERS AND SCALABLE STORAGE SOLUTIONS, TO OUR CUSTOMERS. WE ALSO OFFER CUSTOM DEVELOPMENT AND ADVANCED-LEVEL UNIX/LINUX CONSULTING SOLUTIONS.

# With a former intelligence operative confirming that the NSA has developed the prized technique of concealing spyware in the firmware of hard drives, what are the implications and is there any point in shutting the door now that the horse has bolted?

ROB SOMERVILLE

**M**y wife, bless her, has to put up with a demanding home chef who in her own words, is “a good cook but a messy cook”. To further add insult to injury, on a trip to the supermarket I will religiously read the ingredients of every packet I purchase, unless of course I am confident of the brand, but even then I still have my suspicions. The age old traders’ trick of placing a thumb on the weighing scales or selling adulterated produce did not die out in the Victorian age, despite all the legislation and government control we live under in the 21st century. What concerns me most is provenance, where the product was produced and its roots. For instance, fake saffron is a lucrative business when the genuine article can sell upwards of \$7000 per kilogram, approximately tenfold that of raw Colombian cocaine prior to processing. As always, the Latin phrase *Caveat emptor* springs to mind – buyer beware.

For too long like the banking sector, the IT industry has based physical and electronic transactions on the basis of trust. Trust is the fundamental pillar backed by commercial law, and once that trust has eroded, only paranoia, panic and protectionism can seek to redress the balance. Maybe it is just me, but seasoned IT professionals tend to lean towards the paranoid, as technologists having grasped the hinterland of J. Robert Oppenheimer’s quote from the Bhagavad Gita – “Now I am become Death, the destroyer of worlds”. Realizing with great power comes responsibility, we lean towards the conservative, not wanting to take unnecessary risks, yet at the same time powerless in the face of a commercial and political juggernaut that

abandons value and is ignorant of the nuances of the dangers when technology becomes the master rather than the slave. We are all but cogs in the machine.

If the Reuters report<sup>1</sup> is accurate, and there is no reason technologically or conspiratorially to believe otherwise, we have crossed the Rubicon – reached a point of no return. Pandora’s box has been opened, and the IT industry needs to grasp the implications of this revelation. It is not so much that systems can be compromised. We know this as fact. What is so disturbing is that the manufacturing and commissioning process has been compromised, and unlike the defense or airline sectors, we do not have the skirts of an official secrets act or American equivalent to hide behind. You can wrap an incident in bureaucratic red tape and prevent physical access to an aircraft, but you cannot stop a horde of Open Source gurus examining kit with a hex editor or a decent oscilloscope and a voltmeter. Any Fifth Column will have a hard time remaining hidden, exponentially leading to the rapid erosion of trust.

What troubles me is that I have personal experience of this, and I can confirm that according to rumor, a major European airline in the early 1990’s replaced their flight control computers across the entire fleet when they discovered they were compromised by a foreign power, giving them the ability to remotely commandeer an aircraft. This was well known in the industry at the time, and I only came across this vertical knowledge as I was party to installing hardware and software for airlines worldwide

at the time. While I am not alone in blowing this particular whistle, to date the mainstream media and commercial culture would prefer that we dismiss this as fantasy or conspiracy and anyone subscribing to this as a false prophet or suffering from a Cassandra complex. The geopolitical and ethical implications are obvious post 9/11, yet the silence on this incident is deafening. All I can do is attest to what I heard and leave the reader to judge.

If we are to accept the fact that physical systems have been compromised at the manufacturing level, we must seriously consider that potentially even the Open Source movement itself has been compromised, either by accident or design. The Annus horribilis of the BASH scripting bug and SSL compromise will attest to this. While these security incidents have been confirmed as the result of human error, there are a raft of “Unknown Unknowns” lurking out there. To quote political rhetoric, the terrorists only need to be lucky once, the security services need to be vigilant continually. The rabbit hole extends very deep indeed and the implications are troubling. It all comes down to ethics, money and power, and no matter how innocent and pure our personal motives, there will always be those whose real intention is to pervert, corrupt and compromise while appearing as an angel of light. And this goes down through the chain, from hardware, firmware and software to design, commissioning and management. Statistically, there have to be some bad apples in the barrel.

We need to grow up as individuals, and as a community realize our value to the world. When the scandal of melamine in baby formula in China was exposed, there was the usual shock and horror but very little was done globally to improve food security and quality. In the Western world, we delegate this responsibility to our government, and the government points to the law and leaves the sector to police itself. *Plus ça change, plus c'est la même chose*. Technology is as critical as food for without it, our society – and indeed our civilization – would be in dire peril. The current Zeitgeist that looks to reform the established system, be it political, legal or financial is knocking at our door, and it would be a foolish man or woman that attempts to use the excuse of “We are different” as a rebuttal to the forces of change or self examination.

#### References:

1. <http://www.reuters.com/article/2015/02/16/us-usa-cyberspying-idUSKBN0LK1QV20150216>

#### ABOUT THE AUTHOR

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*



# Interview with Solène Rapenne

## Q: Could you please introduce yourself and your employer?

**A:** My name is Solène Rapenne, I'm a 25 year old IT girl. I work for a French company named Carte Blanche Conseil as the (only) IT administrator. Most of our servers run FreeBSD and they all use almost exclusively open source software.

Carte Blanche Conseil is a small company founded in 1989. The company is split into two activities: software development and consulting. Our business sector is mobility and traffic. We also develop the product MacMap which is a user-friendly GIS software for MacOS that we may release an open source version of in 2015.

## Q: How did you get started with the BSD generation of Operating Systems and when?

**A:** I think I tried BSD for the first time with FreeBSD version 6. I was very curious; at this time I was trying a few brands of Linux distributions and I wanted to try something a bit different, so I chose FreeBSD. I wasn't very familiar with Unix; even if I had used Linux before. I really had no idea of what I was doing sometimes. When trying to tweak the system, I often needed to reinstall from scratch because the system was broken and I didn't know how to repair it!

I learned a lot myself while I was at the university, and I have been using both FreeBSD and OpenBSD everyday, one on my workstation and the other on my laptop. In 2010, at the end of my studies, I successfully passed the BSD Associate certification.

## A: What is your favorite BSD OS and can you explain what makes it special to you compared to the others?

**A:** I can't say I have a favorite BSD. I really like FreeBSD, OpenBSD and DragonFly BSD. FreeBSD has great performance and it is stable, with nice features. Meanwhile, OpenBSD is stable, secure, very well documented and easy to use, but it lacks performance in my opinion. I like

playing with FreeBSD, everything in ports can be configured to use some specific options, system upgrades just works like a charm and the new package management is awesome. About DragonFly BSD, I like how it's always being improved. The system has gone far in a few years and tries to innovate while keeping the system pretty stable.

## Q: What is your approach with the Open Source culture and what do you think about it in the modern software life-cycle?

**A:** I really love Open Source. I'm not sure I would do the job I have actually if everything was closed-source. Open Source is a great thing where everyone can improve the tools for other people. I'm trying to use exclusively open-source software when it is possible. I would like to contribute more to software I like, but very often the projects need developers while I can only submit bug reports, ideas or some basic patches.

In France, there is more and more open source software paid for by the French Administration to suit their needs. They chose this model because once the contract is finished, the Administration can keep the sources, can receive contributions from volunteers and the project can evolve. If needed, they would pay developers to carry out further improvements. In the past, they were paying for software, and once the product was delivered, they couldn't improve it or fix anything without the seller's contribution. Then, when they really need the software to be improved, because of a new law for example, if the seller's company doesn't provide support for the product, they have to buy a new product and train people to use it.

## Q: Can you please introduce the ownCloud project?

**A:** ownCloud is a project that aims to provide to anyone the ability to have its own Cloud service and to sync files. Part of it is written in PHP for the web interface and backend, and another part for the syncing desktop client (Windows/Linux/Mac).

ownCloud comes by default with a few plugins to allow you to encrypt your files, manage users and set quotas, picture viewer, calendars, contacts, write documents (by using a LibreOffice headless server). You can install 3rd party applications to add video viewer support, roundcube mail integration and a lot more!

ownCloud is a great tool which allows you to share your files as you want. You can share a file or a folder with a link that can be set to expire at a given date and also set a password for accessing the files. Of course, files can be shared between users, and even between different ownCloud installations!

**Q: Are you actively involved in the development/management/promotion of the ownCloud project? If not, would you like to contribute and how?**

**A:** I am not actually involved in ownCloud. I am promoting it “passively” in communities I am in by telling them that I’m using it, that it is a nice product and by helping people to install and configure it.

**Q: What do you think makes ownCloud different from other cloud based storage?**

**A:** The most important thing with ownCloud is the word “own” in its name. It is open-source, you install it on YOUR server and do whatever you want with it. You can also write plugins for ownCloud or download “apps” made by the community. I have never used any other Cloud platform since I don’t want to share my data with companies.

**Q: Assuming a user has her own data on another cloud platform, how easy is it to migrate to ownCloud, sync the devices and start using this platform?**

ownCloud installation is easy, and it only requires little knowledge of UNIX. You can find a lot of tutorials about its installation process and on how to configure it. As far I as know, ownCloud doesn’t provide any migration tools to retrieve data from another cloud storage provider.

**Q: What makes the special connection between DragonFly BSD and ownCloud?**

**A:** DragonFly BSD is a very nice system, very lightweight, it has good performance and a really interesting filesystem. The filesystem HAMMER is really interesting when used with a storage utility like ownCloud. The snapshot system makes the software upgrade a lot easier when it comes to backup everything, because it allows to revert easily some files and it doesn’t take any time. It’s also possible to use the PFS streaming to replicate the ownCloud data in another

server for high availability. Deduplication can save some disk space depending on the kind of data stored. Compared to ZFS which provides most of these functionalities, HAMMER can run on more modest hardware.

**Q: Are there any specific ownCloud events such as conferences and meetings?**

**A:** Yes, ownCloud organizes events all around the world: <https://ownCloud.com/events/event/Personally> I never had the chance to be part of an event like this.

**Q: Do you believe that ownCloud is better suited for personal usage or even for enterprise adoption? Can you provide some notable examples of usage?**

**A:** For personal use, ownCloud can be more expensive than other well-known cloud storage services. Why? You need a server, or at least a company selling an ownCloud service, while the other cloud services offer you a bunch of free Gb. If your data amount fits into a free offer, ownCloud will be more expensive. However, if you have a huge amount of data, the ownCloud price will remain with a set price, while other services will cost more according to the amount stored. But with ownCloud, you can share the charges with other interested people, and even set quotas to be sure there will be space for everyone.

For enterprise adoption, it is different. Very often, companies already have a tool to share documents between employees like a NAS. ownCloud can be used to store, share and sync documents but it needs to change habits compared to a “traditional Windows share”. What ownCloud can really provide to an enterprise is the ability to share documents over the Internet. Since a few years, I see more and more people from other companies sending me links to a cloud storage to download some heavy files that can’t be sent by mail, but they use a 3rd party cloud service, certainly without agreement of their IT service but they don’t have any other choice if they want to share a file. ownCloud can bring the power to share files while keeping control over them.

**Q: Is there a training program to let the users start using the platform and/or ease the jump-in of enterprises?**

**A:** ownCloud has an online demo if you want to try the product: <https://demo.ownCloud.org/>.

There is no training on the product’s use, but sometimes there are events about (how to install, configure and maintain your ownCloud). The product is pretty easy to install anyway, and there is no need to train someone on its use.

# Big Data Gets Real in Boston!

People are talking about  
BigData TechCon!



**“Big Data TechCon is a great learning experience and very intensive.”**

—Huaxia Rui, Assistant Professor,  
University of Rochester



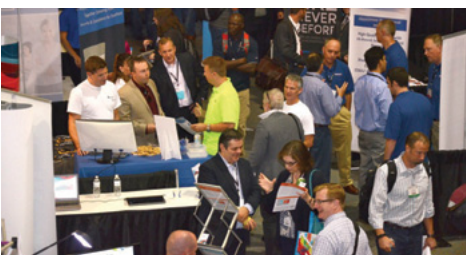
**“Get some sleep beforehand, and divide and conquer the packed schedule with colleagues.”**

—Paul Reed, Technology Strategy & Innovation, FIS



**“Worthwhile, technical, and a breath of fresh air.”**

—Julian Gottesman, CIO, DRA Imaging



**“Big Data TechCon is definitely worth the investment.”**

—Sunil Epari, Solutions Architect, Epari Inc.

## BigData TECHCON

April 26-28, 2015

Seaport World Trade Center Hotel



**Choose from 55+ classes and tutorials!**

**Big Data TechCon is the HOW-TO technical conference for professionals implementing Big Data solutions at their company**

**Come to Big Data TechCon to learn the best ways to:**

- Process and analyze the real-time data pouring into your organization
- Learn how to extract better data analytics and predictive analysis to produce the kind of actionable information and reports your organization needs.
- Come up to speed on the latest Big Data technologies like Yarn, Hadoop, Apache Spark and Cascading
- Understand HOW to leverage Big Data to help your organization today

[www.BigDataTechCon.com](http://www.BigDataTechCon.com)

 **Dr.WEB®**  
since 1992



# Dr.Web 9.0 for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search



© Doctor Web  
2003 — 2013

[www.drweb.com](http://www.drweb.com)

**Free 30-day trial:** <https://download.drweb.com>

**New features in Dr.Web 9.0 for Windows:** <http://products.drweb.com/9>

**FREE bonus — Dr.Web Mobile Security:**  
<https://download.drweb.com/android>





# Using FreeBSD as a File Server with ZFS

Ivan Voras

The ZFS storage workshop will teach you how to create a ZFS file system from scratch and build a file server on top of it, but it will also teach you how ZFS, file systems and storage servers work in general. You will learn what ZFS looks like, its many features and quirks, and how to use it in a FreeBSD server as a building block of a small file server.

ZFS is the ground-breaking file system originally developed at Sun Inc. for their Solaris operating system. It was open-sourced as a part of their OpenSolaris initiative and from there has spread to multiple other operating systems. FreeBSD was the first one to implement a working port, and though it has taken a fairly long time of tweaking and stabilization, it is now a robust and popular choice. There are products which successfully build upon the technologies of FreeBSD and ZFS, such as FreeNAS and its related enterprise-class products from iXsystems, which automate and simplify a lot of the tasks, but all of them use the same ZFS interface under the hood, which is not that complicated in itself.

The requirements for this workshop are decent knowledge of FreeBSD, a basic familiarity with command-line operations, and a system (possibly a virtual machine) on which the student will perform the required tasks, containing at least four hard drives (physical or virtual). Since the topic of this workshop is file servers, the participants must prepare a virtual or a physical machine with at least two disk drives (and preferably 4), which which to perform the exercises and the setup from the workshop.

<http://bsdmag.org/course/using-freebsd-as-a-file-server-with-zfs-2/>

**Ivan Voras is a FreeBSD developer and a long-time user, starting with FreeBSD 4.3 and throughout all the versions since. In real life he is a researcher, system administrator and a developer, as opportunity presents itself, with a wide range of experience from hardware hacking to cloud computing. He is currently employed at the University of Zagreb Faculty of Electrical Engineering and Computing and lives in Zagreb, Croatia. You can follow him on his blog in English at <http://ivoras.net/blog> or in Croatian at <http://hrblog.ivoras.net/>, as well as Google+ at <https://plus.google.com/+IvanVoras>.**



# Meet the Developer-Friendly Payment Solution



## 3 easy steps to optimized checkouts:

1

### Create the checkout page

With Gate2Shop, you can optimize your payment pages by using ready-made templates or by customizing payment pages to your site look and feel.

2

### Test and optimize

An effective payment page variant testing tool, A/B Testing helps you gain insight into user behaviour, increase payment conversion in the short and long term.

3

### Accept payments worldwide

With dozens of alternative and local payment methods offered in multiple currencies, the personalized checkout allows you to reach users from all around the world.

✓ Easy integration   ✓ Cross-platform   ✓ Secure



Call for a free consultation: +44 20 3051 0330

[www.g2s.com](http://www.g2s.com)