

Essentials to creating your own Security Posture using Splunk Enterprise

Using Splunk to maximize the efficiency and effectiveness of the SOC / IR

Richard W. McKee, MS-ISA, CISSP | Principal Cyber Security Analyst Nevada National Security Site September 28, 2017 | Washington, DC

spiunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

.screen?product_id=FL-DSH-01&JSE

" It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle."

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

Sun Tzu, The Art of War



Richard W. McKee

Background – Experience and Education

Principal Cyber Security Analyst – Nevada National Security Site

- ▶ 25 years in law enforcement
 - Last 11 years in computer forensics and cyber investigations (criminal and national security)
- Master of Science Information Security and Assurance
- Bachelor of Business Administration Management Information Systems
- Certifications CISSP, Splunk Certified Power User, EnCE, GPEN, GCIH, GREM, GMON, GNFA, GISP



Background

How the NNSS Splunk experience relates to your enterprise



What is the NNSS?



Creen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP /product.screen?product_id=FL-DSH-01&JSESSIONID=SD12L4FF10ADFF10 T /01d1into1

?6&JSESSIONID=SD5SL9FF1ADFF3 HTTP



National Nuclear Security Administration



SECURITY SITE

NEVADA NATIONAL



Prevention is Ideal... But Detection is a Must

- Splunk is the primary SIEM for the NNSS
- All hosts and devices capable of sending logs to Splunk do so
- Cyber has made logging a policy requirement and all in-house developers or hired consultants must write software capable of logging and sending events to Splunk

Data Sources

"...know yourself..."

- Windows Hosts
- Linux Hosts
- Mac Hosts
- Routers and Switches
- Firewalls
- Endpoint Protection
- Syslog
- Internal Splunk servers
- Databases

- VPN
- RSA
- Active Directory
- VoIP Phones and Servers
- Email Security Appliance
- Malware Sandbox
- FortiMail
- DLP
- Mobile Device Management



Configuration

► A physical syslog server is the primary feed for Splunk

- For security, only the syslog server can communicate directly with the Splunk indexers
- All forwarders and devices feed the syslog box directly*
- ► A 10Gbps tap is also feeding the syslog server
- ► If Splunk fails, logs are also temporarily stored on Syslog







Host Logs

- Enterprise Snare is used to grab logs from sources. NNSS brought the Snare developer in from Australia to custom create agents for Windows, Mac, Linux, SQL, and Epilog
- The Snare Agents are highly customizable and act as the first filter prior to Splunk, allowing the reduction of unnecessary data

| | Token Elevation Type indicates This event is generated when |
|----------------------|--|
| uncate List | |
| | |
| -tenning.com/cart.do | splunk> .conf2 |

Snare Configuration

| Action Required | Criticality | Event ID Include/Exclude | Event ID Match | User Match | General Match | Source Match | Return | Event Src |
|--------------------|-------------|-----------------------------|----------------------------|------------|---------------|-----------------|---|-----------|
| Delete Modify | Information | Exclude | | Include: * | Include: * | | Success Failure Error Information | Security |
| Delete Modify | Information | Include | Logon_Logoff | Exclude: | Include: * | | Success Failure | Security |
| Delete Modify | Information | Include | 520,4616,1102,517,4697,601 | Include: * | Include: * | Include: * | Success Failure Error Information Warning Critical | Security |
| Delete Modify | Information | Include | User_Right_Events | Include: * | Exclude: | Include: * | Success Failure Error Information Warning | Security |
| Delete Modify | Information | Include | Process_Events | Include: * | Include: * | Include: * | Success Failure Error Information Warning | Security |

404 3322

200 1318

Creen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP /product.screen?product_id=FL-DSH-01&JSESSIONID=SDISL4FF10ADFF10 HITP 1. 7 /oldinezate // // /oldinezate //

?6&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1



Snare Custom Config

| Identify the high level event | Logon or Logoff Access a file or directory Start or stop a process Use of user rights USB Event Any event(s) Account Administration Account Administration Change the security policy Restart, shutdown and system Filtering platform events |
|---|--|
| Event ID Search Term Optional, Comma separated: only used by the 'Any Event' setting above | Include Exclude |
| General Search Term Wildcards accepted | Include Exclude Regular Expression |
| User Search Term User Names, comma separated. Wildcards accepted | Include Exclude |
| Source Search Term Source Names, comma separated. Wildcards accepted | Include Exclude Microsoft-Windows-TaskScheduler |
| Identify the event types to be captured | Success Audit Failure Audit Information Warning Error Critical Verbose ActivityTracing |
| Identify the event logs (ignored if any objective other than 'Any event(s)' is selected): | Security System Application Directory Service DNS Server DFS-Replication Legacy FRS Custom Event Log |
| Select the Alert Level | 🔾 🖨 Critical 🔍 😁 Priority 🔍 😁 Warning 💿 😁 Information 🔍 🔵 Clear |



Category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category.screen?category.screen?category_id=GIFTS&:screen?category_id=GIF

Epilog Agent

Possible uses:

- AV Logs from Linux hosts
- DNS Logs from Domain Controllers
- DHCP Logs from Domain Controllers

Can be used to monitor any flat text files from any directory or UNC path



Epilog Agent

| SNARE Log Configuration The following parameters of the SNARE log inputs may be set: | | | | | | | |
|---|--|--|--|--|--|--|--|
| Select the Log Type | Custom Event Log DNS_Log | | | | | | |
| Multi-Line Format | • Single line only • Fixed number of lines • • • • • • • • • • • • • • • • • • • | | | | | | |
| Send Comments: By default, lines starting with '≠' will be ignored. Enable this option if you wish to collect these lines | | | | | | | |
| Log File or Directory | E:\DNSLog\ | | | | | | |
| Log Name Format: (optional) <u>Help</u> | DNS | | | | | | |
| | Change Configuration Reset Form | | | | | | |



Splunk Searching & Reporting Highly Customized for IR

| & Views 🗸 Searches & Repo | rts 🗸 | & Views 🗸 Searches & Reports 🗸 | r | & Views 🗸 Searches & Reports 🗸 | | |
|---------------------------|----------|--------------------------------|-----|---|---|--|
| Active Directory | <u>م</u> | IOC Scan | • | Elevated Account Browser Execution by | Q | |
| DHCP | • | Lookup Tables | • | | | |
| DNS | • | Mac Activity | • | Elevated Account Browser Execution with Host | q | |
| Email | • | RSA | • | Elevated Account Deleted | Q | |
| Errors | • | SEP | • | FireEye Alerts | Q | |
| File Activity | • | Snort | , | FortiSandbox Alerts | ٩ | |
| Firewall | • | VMware | • | License Usage Data Cube | Q | |
| GET Requests | • | VPN | • | Logons by Elevated AD USer | Q | |
| Internet Activity | | Windows Activity | • | Slideshow Views Supportability | Q | |
| Investigative | • - | Avecto - Command Execution | Q 📮 | Snare - Agent Heartbeat | Q | |



ET /category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category.sc

Quick Investigative Searches

These searches are complete except for areas for the incident responder to put a username, IP, hostname, etc.

| < Back | | | | | | |
|--|---|--|--|--|--|--|
| [Investigative] - Browsing Activity Search (Avecto) | | | | | | |
| [Investigative] - Computer Lookup | Q | | | | | |
| [Investigative] - FW Activity for Specific IP Address | ٩ | | | | | |
| [Investigative] - Search for a Domain Name | Q | | | | | |
| [Investigative] - Search for MAC Address | Q | | | | | |
| [Investigative] - SID Search | Q | | | | | |
| [Investigative] - User Activity (| Q | | | | | |
| [Investigative] - User Lookup | Q | | | | | |

splunk'> .conf20

Search Examples - DNS

| DATE/TIME (UTC) ^ | REQUESTER CLIE | NT IP 🗘 | DOMAIN 0 |
|---------------------|----------------|---------|-------------------------------------|
| 03-13-2016 04:53:59 | | | clients4.google.com |
| 03-13-2016 04:53:59 | | | csc3-2010-crl.verisign.com |
| 03-13-2016 04:53:59 | | | prod.nexusrules.live.com.akadns.net |
| 03-13-2016 04:53:59 | | | ocsp.globalsign.com |
| 03-13-2016 04:53:59 | | | www.microsoft.com |
| 03-13-2016 04:53:59 | | | ent-shasta-rrs.symantec.com |
| 03-13-2016 04:53:59 | | | streamerapi.finance.yahoo.com |
| 03-13-2016 04:53:59 | | | csc3-2009-2-crl.verisign.com |
| 03-13-2016 04:53:59 | | | pki.energy.gov |
| 03-13-2016 04:53:59 | | | ent-shasta-rrs.symantec.com |
| 03-13-2016 04:53:59 | | | www.google.com |
| 03-13-2016 04:53:59 | | | chk.l2.nessus.org |
| 03-13-2016 04:53:59 | | | ent-shasta-rrs.symantec.com |
| 03-13-2016 04:53:59 | | | nexusrules.officeapps.live.com |

buttercut

404 3322

SE8 ISESSI

netp:

404

SCreen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1 Oduct school 255ADFF0 H

//screen?category_id=GIFTs&lstSSIONID=SDISL4FF10ADtF10 HTTP 1.1" 400.1" /products ET /oldfink?tem_forduct_id=EL_DSH=04&JSESSIONID=SDSL7FF6ADtF50 HTTP 1.1" 200 31d=SU 1 1 dink?tem_id=EST-26&JSESSIONID=SDSL9FF1ADtF30 HTTP 1.1" 200 31d=SU 1 1 dink?tem_id=EST-26&JSESSIONID=SDSL9FF1ADtF30 HTTP 1.1" 200 31d=SU

"GET

"GET /oldlink?item

splunk'> .conf2017

Search Examples – Files Written to USB

| DATE/TIME FILE WRITTEN (LOCAL) 0 | USER 0 | HOSTNAME 0 | DOMAIN 0 | USB DEVICE ID 0 | FILES WRITTEN 0 |
|---|--------|------------|----------|--|-------------------------------------|
| 2016-03-12 20:53:35 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/~Archive3.pst.tmp |
| 2016-03-12 20:53:35 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/Archive3.pst |
| 2016-03-12 20:49:27 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/July 9 2013.pst |
| 2016-03-12 20:49:27 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/~July 9 2013.pst.tmp |
| 2016-03-12 20:49:20 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/~Archive3.pst.tmp |
| 2016-03-12 20:49:20 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/Archive3.pst |
| 2016-03-12 20:49:07 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/~Archive 4.pst.tmp |
| 2016-03-12 20:49:07 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DTimev_0217\AA0000022A1F&0 | F:/Exchange/Archive 4.pst |
| 2016-03-12 20:38:26 | | | NTSOPS | USBSTOR\Disk&Ven_Apricorn&Prod_tegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/~Archive3.pst.tmp |
| 2016-03-12 20:38:26 | | | NTSOPS | USBSTOR\Disk&Ven Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0 | F:/Exchange/Archive3.pst |

Serial number of the USB device is captured, allowing CIRT to do serial number lookups and correlation



splunk

Search Examples – Possible Compromised Hosts



Firewall logs are examined daily and hosts that meet two or three of the following are highlighted:

1 – Hosts with the most data flowing out

Product id=FL-DSH-01&JS

- 2 Hosts with the highest number of connections
- 3 Hosts with the longest duration of connections

Search Examples – GET Requests

| DATE/TIME (UTC) ≎ | SOURCE IP 0 | DESTINATION | DESTINATION CITY 0 | DESTINATION REGION 0 | DESTINATION COUNTRY 0 | GET REQUEST 0 |
|------------------------|-------------|----------------|-----------------------|-------------------------|--------------------------|---|
| 03-13-2016 04:22:51 | | 74.113.233.187 | White Plains | NY | United States | anx.apnanalytics.com/tr.gif?anxa=TBNotifier&tbnguid=931F74FE-43F 08&anxr=w6oxRvGb&ie_hpr=-5&osDetail=6.3.1.sp0.x64&wx_tboff=0&c |
| 03-13-2016 04:22:51 | | 199.36.100.106 | New York | NY | United States | tbapi.search.ask.com/v6/apnu/update?tb=0V02-SP&cbid=*BA0&v=33 |
| 03-13-2016 03:14:05 | | 65.52.108.27 | Redmond | WA | United States | g.bing.com/GWX/GWX? ts=1457838808370&SQM=4195fb5ad069431a99d94a37c22905c7&GV FA5D-42c9-9DF0-014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/ |
| 03-13-2016 03:14:05 | | 65.52.108.27 | Redmond | WA | United States | g.bing.com/GWX/GWX? ts=1457838807980&SQM=4195fb5ad069431a99d94a37c22905c7&GV 014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/1.1 |
| 03-13-2016 00:54:55 | | 93.184.215.59 | Washington | DC | United States | cdn.pokki.com/pokki/platforms/version56e3af4771eed.exe HTTP/1.1 |
| 03-13-2016 00:48:19 | | 74.113.233.187 | White Plains | NY | United States | anx.apnanalytics.com/tr.gif?anxa=TBNotifier&tbnguid=829444A8-CF4 27&anxr=A8PsHV4W&ie_hpr=0&osDetail=10.0.1.sp0.x64&cr_ds=0&an |
| 03-13-2016 00:44:37 | | 65.52.108.27 | Redmond | WA | United States | g.bing.com/GWX/GWX? ts=1457829892004&SQM=4e694025c3564ead844a9b51f4cace12&GV FA5D-42c9-9DF0-014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/ |
| 03-13-2016 00:44:36 | | 65.52.108.27 | Redmond | WA | United States | g.bing.com/GWX/GWX? ts=1457829891598&SQM=4e694025c3564ead844a9b51f4cace12&GV 014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/1.1 |



/Category.screen?category_id=GFTS&JSESSIONID=SDISL4FF19ADFF10 HTTP 1.1" 404 720 "http://buttercuP-shopping.com/cat.do/cat

Search Examples – IOCs

| < Back | | | | |
|--|-----|--|--|--|
| IOC Scan - Domain Names (FW) | ۹ 1 | | | |
| IOC Scan - Domain Names (Requests) | Q | | | |
| IOC Scan - Domain Names (Windows) | Q | | | |
| IOC Scan - Filename (| Q | | | |
| IOC Scan - Filename (Macs) | Q | | | |
| IOC Scan - Filename (USB) | Q | | | |
| IOC Scan - Filename (Windows Printing) | Q | | | |
| IOC Scan - Hash Values (| Q | | | |
| IOC Scan - Hash Values (| Q | | | |
| IOC Scan - IP Addresses (FW) | Q - | | | |

0:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category.screen?category.screen?category.id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 332 "http://buttercup-shopping.com/category.screen?



Search Examples – RSA Activity

| DATE/TIME (UTC) 0 | USER 0 | ACTION 0 | RESULT 0 |
|---------------------|--------|----------|----------------------|
| 03-13-2016 07:18:02 | | success | AUTHN_METHOD_SUCCESS |
| 03-13-2016 07:12:36 | | SUCCESS | AUTHN_METHOD_SUCCESS |
| 03-13-2016 07:12:18 | | failure | AUTHN_METHOD_FAILED |
| 03-13-2016 07:12:18 | | failure | AUTHN_METHOD_FAILED |
| 03-13-2016 06:51:01 | | success | AUTHN_METHOD_SUCCESS |
| 03-13-2016 06:36:43 | | success | AUTHN_METHOD_SUCCESS |

RSA Activity includes PIN resets, token failures, and emergency backup PIN access



splunk

Search Examples – Process Execution

| DATE/TIME (UTC) 0 | HOSTNAM | EO | DOMAIN 0 | Avecto_description 0 | SOFTWARE VERSION 0 | PROCESS | PARENT PROCESS ID 0 | HASH 0 | COMMAND EXECUTED 0 |
|----------------------------|---------|----|----------|-------------------------------------|-----------------------|---------|---------------------------|--|---|
| Mar 13 07:53:22 2016 | | | | Task Scheduler Engine | 6.1.7600.16385 | 4252 | 332 | 2D5A9FFAE8898BA67963290FC4E1DDF99DED5E2E | taskeng.exe {68819784-53C7-4 941922548-1860439328-29390 |
| Mar 13 07:53:22 2016 | | | | Adobe Reader and Acrobat Manager | 1.824.16.6751 | 7848 | 4252 | 7224E3586E6576C071A6141F3073A831734B08D4 | *C:\Program Files (x86)\Comm |
| Mar 13 07:53:20 2016 | | | | Windows host process (Rundll32) | 6.1.7600.16385 | 5464 | 5500 | 963B55ACC8C566876364716D5AAFA353995812A8 | rundll32 C:\WINDOWS\system32\spool /pjob=29993 /pname"\\nts-ps2 |
| Mar 13 07:53:19 2016 | | | | COM Surrogate | 6.1.7600.16385 | 7128 | 848 | E977B87698C3E595D55827665E22FBF788DD3F9F | C:\WINDOWS\system32\DIHos FF9B966D75B0} |

This search identifies software, versions, PID, PPID, Hash values of executable, path, etc. This is used with a lookup table to identify new software and find malware based on path and hash

Splunk Alert Example

| To 1 | Splunk Splunk Review: [Real Time Alert] - Windows Executable Launched To If there are problems with how this message is displayed, click here to view it in a web browser. | | | | | | | | | | | |
|---|--|-----|--|--|--|--|--|--|--|--|--|--|
| The alert condition for '[Real Time Alert] - Windows Executable Launched' was triggered. DATE/TIME ACCOUNT INSTALLER HOSTNAME HOST IP INSTALLING EXECUTABLE LAUNCHED(UTC) SOFTWARE | | | | | | | | | | | | |
| | Feb 16 18:49:36 2016 | | | | C:\Users\ AppData\LocalLow\Oracle\Java\AU\au.msi. | | | | | | | |
| | Feb 16 18:48:34 2016 | | | | C:\Users AppData\LocalLow\Oracle\Java\jre1.8.0_74\jre1.8.0_74.msi. | | | | | | | |
| | Feb 16 18:32:35 2016 | | | | C:\Users \AppData\Local\dell\drivers\APP_WIN_R312259\dellsysmgr.msi. | | | | | | | |
| | National Nuclear Security Administrat US Department of Energy Nevada National Security Site | ion | | | | | | | | | | |

404 3322

200 1318

Y_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP

SIONID=SD5SL9FF1ADFF3 HTTP

/product.screen?product_id=FL-DSH-01&JSESSIONID=SD15L4FF10ADFF10 / oldistatesproduct_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9



Account Activity Dashboard

| [Dashboard] Account A | ctivity | | | | | | | | Edit v | M | ore Info 🗸 | Ŧ | ð |
|--------------------------------------|-------------------------------|----------|------------------|-------------------|-----------------------|----------------------------|----------------------|-------------------------------|----------|--------------|------------------------|------------|-----|
| Accounts Enabled Past 7 Days | Accounts Disabled Past 7 Days | | | | | | | | | | | | |
| DATE/TIME ACCOUNT ENABLED (UTC) 0 | ACCOUNT ENABLED 0 | DOMAIN 0 | USER W ACCOUR | HO ENABLED | | DATE/TIME ACCOU (UTC) 0 | INT DISABLED | ACCOUNT DISABLED 0 | DOMAIN 0 | USER ACCO | WHO DISABI UNT ଁ | LED | |
| 1 03-11-2016 21:34:08 | | | | | 1 | 03-12-2016 14:59:4 | 5 | | | | | | |
| 2 03-11-2016 21:31:18 | | | | | | | | | - | - | | | |
| 3 03-11-2016 21:19:05 | | | | | 2 | 03-11-2016 21:02:0 | 5 | | | 1 | | | |
| 4 03-11-2016 21:12:37 | | | | | 3 | 03-11-2016 20:54:00 | 6 | | _ | - 11 | | | |
| 5 03-11-2016 21:10:56 | | | | | 4 03-10-2016 23:00:05 | | | | | | | | |
| 6 03-11-2016 21:01:56 | | | | | | 03-10-2016 22:56:11 | 1 | | | | | | |
| 7 03-11-2016 20:56:33 | | | | | 6 | 03-10-2016 22:49:2 | 7 | | | | | | |
| 8 03-11-2016 20:54:25 | | | | | 7 | 03-10-2016 22:48:2 | 7 | | | | | | |
| 9 03-11-2016 20:50:56 | | | | | 8 | 03-10-2016 21:57:19 | 9 | | | | | | |
| 10 03-11-2016 20:47:46 | | | | | 9 | 03-10-2016 19:01:5 | 5 | | | | | | |
| 9+10 | | | | 2m ago | 10 | 03-10-2016 18:39:39 | 9 | | | | | | |
| Accounts Created Past 7 Days | | | | | Ac | counts Deleted F | Past 7 Days | | | | | | |
| CREATED DATE/TIME (UTC) 0 NE | EW ACCOUNT NAME 0 C | REATOR 0 | HOST ACC | OUNT CREATED ON O | DEL (UT | LETED DATE/TIME | DELETED ACCOUNT 0 | USER WHO DELETED ACCOUNT © | DOM | AIN 0 | HOST ACCO DELETED 0 | UNT N 0 | |
| 1 Mar 10 22:08:10 2016 | | | | | 03-0 | 07-2016 16:57:37 | | | | | | | |
| 2 Mar 07 23:24:41 2016 | | - | | | | | | | | _ | | | |
| 3 Mar 07 18:15:05 2016 | | | | | | | | | | | | | |
| 4 Mar 07 16:59:32 2016 | | | | | | | | | | | | | |
| Top Successful Authentications | Past 1 Hour | | | | Us | er Account Logo | ons on Multiple | Systems Past 24 Hour | S | | | | |
| User Account 0 | | | | count 0 | | UserName 0 | | | | | | co | unt |
| 1 | | | | 490 | 1 | | | | | | | | 5 |
| 2 | | | | 300 | 2 | | | | | | | | 4 |
| 3 | | | | 288 | 3 | | | | | | | | 4 |
| 4 | | | | 277 | - 4 | | | | | | | | 3 |

Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cat.dovactegory.screen?category.screen?category.id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cat.dovactegory.screen?category.id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cat.dovact.dovactegory.screen?category.id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cat.dovact.dovactegory.id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.id=Est.l8BeF10Hz



Authentication Dashboard

| [Dashboard] Authentication | | | | Edit 🗸 🛛 More Info 🗸 🔮 |
|-------------------------------------|-------------------|--------|---|------------------------|
| Top 10 Login Failures Past 72 Hours | A | Top 10 | Privileged Account Failures Past 72 Hours | Δ |
| UserName 0 | # Failed Logins 0 | Use | Name 0 | # Failed Logins 🌣 |
| 1 | 2628 | 1 | | 74 |
| 2 | 1015 | 2 | | 44 |
| 3 | 927 | 3 | | 35 |
| 4 | 883 | 4 | | 31 |
| 5 | 754 | 5 | | 26 |
| 6 | 460 | 6 | | 20 |
| 7 | 417 | 7 | | 17 |
| 8 | 377 | 8 | | 17 |
| 9 | 332 | 9 | | 15 |
| 10 | 297 | 10 | | 13 |
| Top RSA Failures Past 72 Hours | A | Top RS | A Successful Logins past 72 Hours | A |
| user 0 | count 0 | user | 0 | count 0 |
| 1 | 13033 | 1 | | 85 |
| 2 | 10655 | 2 | | 83 |
| 3 | 5921 | 3 | | 62 |
| 4 | 5016 | 4 | | 59 |
| 5 | 2516 | 5 | | 49 |
| 6 | 2362 | 6 | | 43 |
| 7 | 1461 | 7 | | 40 |
| 8 | 1258 | 8 | | 34 |
| 9 | 1018 | 9 | | 33 |
| 10 | 977 | 10 | | 33 |

category_id=GIFT5&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen



Defense in Depth Dashboard

| [Dashboard] De | fense in D | epth | | | | | | | Edit 🗸 | More Int | fo 🗸 | Ŧ | • |
|--|---|-----------------------------------|---------------------------|---|--|------------|------------|-------------|-------------|--------------|------------|----------|-------|
| IDS/IPS Pa | ast 7 Days | | Malware Found Past 7 Days | | | | | | | | | | |
| TIME (LOCAL) 0 | DCAL) 0 HOSTNAME 0 ATTACK SIGNATURE 0 ATTACKER IP 0 | | | | DATE/TIME (LOCAL) 0 | HOSTNAME 0 | USERNAME 0 | RISK N | AME 0 | | | | |
| 2016-03-11 23:24:53 | | OS Attack: GNU Bash CVE-2014-6271 | 185.93.182.151 | 1 | 2016-03-08 13:03:43 | | SYSTEM | | | CI | eaned by | deletion | 1 |
| 2016-03-11 23:24:47 | | OS Attack: GNU Bash CVE-2014-6278 | 185.93.182.151 | | | | | | | | | | |
| 2016-03-11 23:24:42 | | OS Attack: GNU Bash CVE-2014-6271 | 185.93.182.151 | | | | | | | | | | |
| 2016-03-11 23:24:36 OS Attack: GNU Bash CVE-2014-6278 185.93.182.151 | | | | | | | | | | | | | |
| 2016-03-11 23:24:31 OS Attack: GNU Bash CVE-2014-6271 185.93.182.151 | | | | | | | | | | | | | |
| 2016-03-11 23:24:25 | | OS Attack: GNU Bash CVE-2014-6278 | 185.93.182.151 | | | | | | | | | | |
| 2016-03-11 23:24:20 | | OS Attack: GNU Bash CVE-2014-6271 | 185.93.182.151 | | | | | | | | | | |
| 2016-03-11 23:24:15 | | OS Attack: GNU Bash CVE-2014-6278 | 185.93.182.151 | | | | | | | | | | |
| 2016-03-11 23:24:09 | | OS Attack: GNU Bash CVE-2014-6271 | 185.93.182.151 | | | | | | | | | | |
| 2016-03-11 23:24:04 | | OS Attack: GNU Bash CVE-2014-6278 | 185.93.182.151 | | | | | | | | | | |
| Plost IDS/I | | | 8m ago | Snort Network IDS/IPS Past 72 Hours (Excluding Port Scans) | | | | | | | | | |
| Web Attack: Coldfusionownloan HTTP Hylafax Faxsurvey HTTP Hyp Web Attack: MS IIS ASPclosur Web Attack: ColdFusion I HTTP MS IIS Ne HTTP SCO Skunkware Audit: ' OS Attack: CNU Basi | d CVE-2013-3336 Remote PW Access rep CGI File Access e CVE-2000-0302 Remote Code Exec twdsn CGI Request t ViewSrc Traversal VNC Server Banner h CVE-2014-6278 | OS Attack: CNU | | "EXPLOIT ATTEMPTED - Dhole s Blackhole DNS response to "APP-DETECT DNS requesard to o "OS-OTHER Bash CGI envible inj "APP-DETECT DNS reque domain | ite attemptedi" 5 50main 360.cn" ection attempt" n 360safe.com | | | - INDICATOR | R-SCAN UPrP | ° s…ice disc | over atter | mpt" | |
| Potentially Comprom | Potentially Compromised Hosts Based on Firewall Activity | | | | | | | | | | | | |
| ID A | | | | | | | | | | | | 000 | int o |





File Activity Dashboard

| [Das | shboard |] File Act | ivity | | | | | Edit V More Info V | | | | | |
|------|------------------------|---|-----------------|------------|------------|------------|--|--------------------|--|--|--|--|--|
| | Sandbox A | lerts Past 72 | 2 Hours | | | 4 | Blocked USB Devices Past 72 Hours | | | | | | |
| 1 | DATE/TIME (UTC) ି | TIME RISK MALWARE SUBMISSION LEVEL 0 NAME 0 SOURCE IP 0 SOURCE 0 FILEN | | FILENAME 0 | | | | | | | | | |
| 1 0 | 03-10-2016 21:04:00 | Low Risk | N/A | | HTTP | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| File | s Written to | USB by Use | r Past 72 Hours | s | | ۵ | Users with Most Print Jobs Past 72 Hours | A | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | 0 | 1,000 2,0 | 000 3,000 | 4,000 5,00 | 10 6,000 7 | ,000 8,000 | 0 25 50 75 100 | 125 150 175 200 | | | | | |



1 "GET /Category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_iscreen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 322 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category_id=CIMPRADFF7 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category_id=CIMPRADFF7 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category_id=CIMPRADFF7 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category_id=CIMPRADFF7" HTTP 1.1

Foreign Activity Dashboard



Network Access Dashboard

| [Da | Edit v More Info v | | | | | | | | | | |
|-----|----------------------|------------------|-----------------|---------------|---|-------------|------------|---------------|--|--|--|
| Pot | tential Unauthorized | Device on Networ | rk Past 30 Days | | Confirmed Unauthorized Device on Network Past 30 Days | | | | | | |
| | DATE/TIME (UTC) 0 | CLIENT IP 0 | HOSTNAME 0 | MAC ADDRESS 0 | | | | | | | |
| 1 | 03-07-2016 17:49:57 | | | | | | | | | | |
| 2 | 02-12-2016 17:29:00 | | | | | | | | | | |
| | | | | | | | | | | | |
| - | DHCP Activity | Past 15 Minutes | | | Internet Only Activity Past 15 Minutes | | | | | | |
| | DATE/TIME (UTC) 0 | CLIENT IP 0 | HOSTNAME 0 | MAC ADDRESS 0 | DATE/TIME (UTC) 0 | CLIENT IP 0 | HOSTNAME 0 | MAC ADDRESS 0 | | | |
| 1 | 03-13-2016 08:52:37 | | | | 1 03-13-2016 08:52:58 | | | | | | |
| 2 | 03-13-2016 08:52:08 | | | | 2 03-13-2016 08:50:45 | | | | | | |
| 3 | 03-13-2016 08:51:37 | | | | 3 03-13-2016 08:47:43 | | | | | | |
| 4 | 03-13-2016 08:51:16 | | | | 4 03-13-2016 08:47:20 | | | | | | |
| 5 | 03-13-2016 08:49:27 | | | | 5 03-13-2016 08:47:09 | | | | | | |
| 6 | 03-13-2016 08:49:18 | | | | 6 03-13-2016 08:46:46 | | | | | | |
| 7 | 03-13-2016 08:46:08 | | | | 7 03-13-2016 08:45:46 | | | | | | |
| 8 | 03-13-2016 08:45:05 | | | | 8 03-13-2016 08:40:32 | | | | | | |
| 9 | 03-13-2016 08:43:08 | | | | 9 03-13-2016 08:39:42 | | | | | | |

id=FL-DSH-01&JSE

sopping.com/cart.do?action=view&itemId=EST-G&product 1d=F1-SW-01tercup-shopping.com/category.screen7category_freeGifts" "PL-SW-01-Sping.com/cart.do?action=purchas&&itemId=EST-G&product_1Mov_SW-01-SLAFFAADSTIN_VENTURE 1d=ST-SW-01-SLAFFAADSTINWSITEMId=EST-S&product_Id=XV-CB-01-SW-01-SLAFFAADSTINWSITEMId=EST-S&product_Id=XV-CB-01-SLAFFAADSTINWSITEMId=EST-S&product_Id=XV-CB-01-SLAFFAADSTINWSITEMId=EST-S&product_Id=XV-CB-01-SLAFFAADSTINWSITEMId=EST-S&product_Id=XV-CB-01-SLAFFAADSTINWSITEMId=EST-S&product_Id=XV-CB-01-SLAFFAADSTINWSITEMID=S&



Network Traffic Dashboard





Outbound Data Dashboard



404 3322

netp:

404

"GET /product.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1 "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SDSSJ7FF6ADFF9 HTTP 1.1 2005 - 200 Y.Screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP 1.1



Key Takeaways

1. Identify all of your logging sources

- 2. Identify what information from those sources can indicate malicious behavior
- 3. Prepare alerts and dashboards based upon those indicators
- 4. Prepare and save searches for repetitive, common searches

5. ACT ON THE INFORMATION!!!!

