Pretty Good SOC

Effectively Enhancing our SOC with Sysmon & PowerShell Logging to detect and respond to today's real-world threats

Kent Farries | Sr. Systems Analyst, Security Intelligence & Analytics
Ikenna Nwafor | Sr Systems Analyst, Security Design
September 25-28, 2017 | Washington, DC
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.
Introduction & Background
TransAlta Information and Challenges
What was our problem?
Our Journey
New Log Configuration
Endpoint Detection and Forensics
What’s Next
References and Links
Q&A
Kent Farries Background and Role

- I have been with TransAlta for 17 Years in various roles over the years. Desktop, Server, Manager, Architect. Currently Focused on Security and Operational Intelligence

- We are dedicated to the protection of TransAlta’s computing infrastructure while enabling a safe computing landscape where the people of TransAlta can conduct business efficiently

- Favorite Splunk t-shirt
  - I like big data and I cannot lie

- Interesting fun fact about me
  - I was a video game champion in 1982 and you can find me listed in IMDB for the Chasing Ghosts Documentary as well as on the Twin Galaxies gaming site
Over 14 years in Information Security and Network Management; 3 years at TransAlta as a Senior Information Systems Security Analyst

Mostly focused on the Governance Risk and Compliance (GRC), Incident Response, Security Operations, User Education and Security Awareness

A member of TransAlta’s Information Security team responsible for ensuring the security of TransAlta’s network and Critical Infrastructure

Certifications – CISSP, CISM, CISA, GICSP

Favorite Splunk T-Shirt
  • Because You Can’t Always Blame Canada
TransAlta Overview

► Over one hundred years of power generation
  • Wind, hydro, solar, natural gas, coal
  • Clean Power Transition Underway
► Operations in Canada, U.S. and Australia
► Well respected power generator and wholesale marketer of electricity
► Critical Infrastructure for Utility Power Generation
► Regulatory Requirements – NERC CIP, SOX
► IT Security Team based in Calgary with SOC outsourced
What was our problem?

Advanced Endpoint Solution, Endpoint Visibility
Our legacy Endpoint Solution was not able to prevent some modern attacks.

We lacked visibility at our Endpoints.

We didn’t always have the information to answer when and how attackers or malware got on our systems.

Our Managed SOC was focused on traditional threats not modern threats.
Test then deploy an Advanced Endpoint Solution (EDR/EPP?)
- We really wanted Prevention, Detection, and Response but didn’t want to buy two solutions
- Integrate the logs into Splunk for alerting and correlation

Collect the right logs from all endpoints
- Advanced Security Audit Policy Settings
- PowerShell
- USB
- Custom locations

Create new use cases to detect advanced attacks and address our gaps

Regular Red Team type testing to validate our use cases and verify the gaps were remediated
Why Splunk for EDR?

▶ We wanted all of our logs in one place to make it easy to search and correlate

▶ Splunk Forwarder allows us greater flexibility
  • Filter out unwanted or low value events to save bandwidth and license costs
  • Efficiently collect logs from remote locations over slow links
  • Collect additional logs not stored in the Windows Event Logs
  • Collect Host Information

▶ Sysmon
  • Provides rich information beyond what the built-in Windows logging/tools provide. Allows us to hunt effectively

▶ PowerShell Logs to look for modern attacks. Favorite tool for attackers

▶ USB Logging to verify Malware source and look for data loss from Insiders
Key Benefits from Approach

▶ Advanced Endpoint Prevention allows us to focus our resources on what we could not prevent

▶ Excellent Visibility at the Endpoint
  • High Fidelity Alerts to assist with hunting and forensics
  • What happened on a given system
  • Was there any lateral movement
  • How did it enter a given system
  • What tools were being used
  • Detect Reconnaissance
  • Searching for Hashes from IOC’s or Threat Intel
Our Journey

Highlights from 2009 - 2017
<table>
<thead>
<tr>
<th>src</th>
<th>dest_port</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legacy Search**

Data comes from AD

Data comes from AD Sites & Services

GeoIP Location Data

Ingress / Egress Location

Data comes from AD

Data comes from AD Sites & Services

GeoIP Location Data
Splunk Enterprise at TransAlta Corp.

- Windows Logs (AD, IIS, DHCP, DNS, Device-USB)
- Anti-Malware (SCEP)
- Firewalls (Palo Alto, Cisco, CheckPoint)
- Honeywell Card Access
- Syslog Server (Network Devices)
- Threat Lists, Blacklist Data (Bad IP's, C&C's)
- Remote Access (PS, OSCP, DirectAccess, Palo Alto)
- Advanced Threat Protection (FireEye, Palo Alto)

IT Security & Operations Architecture

- DMZ Deployment Server & Cloud Forwarder
- Enterprise Security Search Head 28 Cores
- Energy Data (SCADA)
- Cloud Services (Azure, O365, etc.)
- AdHoc / Operations Search Head 28 Cores
- Operational Data (Performance, KPI's, Correlation)
- ServiceNow (Reporting, KPI's, Correlation)
- Configuration Audits
- Vulnerability Detection (Nessus)
- Store Metrics (Data Domain)
- Endpoint Logs & Forensics (Scripts, EMET, Sysmon, SCCM)
- Unstructured Data (Varonis)

Deployment Server For Internal Configuration

- Indexer 28 Cores
- 2TB SSD Storage
- 7TB SAS Storage

Consumers of Splunk Information

- IT Admin
- Management
- Executives

Energy Data

Cloud Services

Advanced Threat Protection

IT Security Search Head

AdHoc / Operations Search Head

DMZ Deployment Server

Cloud Forwarder

Indexer
### Align SIEM Dashboards, Reports, Alerts to Critical Security Controls V6.1

<table>
<thead>
<tr>
<th>#</th>
<th>CSC</th>
<th>Security Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CSC 1</td>
<td>Inventory of All Assets and Unauthorized Access</td>
</tr>
<tr>
<td>2</td>
<td>CSC 2</td>
<td>Secure Configuration and Software Controls; manage applications and remote access</td>
</tr>
<tr>
<td>3</td>
<td>CSC 3</td>
<td>Identify continuous viability assessment and record changes in access control, systems</td>
</tr>
<tr>
<td>4</td>
<td>CSC 4</td>
<td>Controlled User Access Privileges</td>
</tr>
<tr>
<td>5</td>
<td>CSC 5</td>
<td>Maintain, analyze, and resolve vulnerabilities</td>
</tr>
<tr>
<td>6</td>
<td>CSC 6</td>
<td>Email and Web Application Security</td>
</tr>
<tr>
<td>7</td>
<td>CSC 7</td>
<td>Malware Detection</td>
</tr>
<tr>
<td>8</td>
<td>CSC 8</td>
<td>Limitation and Port, Protocol Management</td>
</tr>
<tr>
<td>9</td>
<td>CSC 9</td>
<td>Access Control</td>
</tr>
<tr>
<td>10</td>
<td>CSC 10</td>
<td>Secure Configuration of Devices such as Firewalls, Routers, and switches</td>
</tr>
</tbody>
</table>

#### Cybersecurity Framework (CSF) Core

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.AM Asset Management</td>
<td>PR.IP Information protection</td>
<td>DE.CM Continuous Monitoring</td>
<td>RS.MI Mitigation</td>
<td></td>
</tr>
<tr>
<td>ID.AM Asset Management</td>
<td>PR.AC Access Control</td>
<td>DE.AE Anomalies and Events</td>
<td>RS.AN Analysis</td>
<td></td>
</tr>
</tbody>
</table>

#### NSA Attack Mitigation

<table>
<thead>
<tr>
<th>Adversary Actions to Attack Your Organization</th>
<th>Severity</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Very High</td>
<td>Report &amp; Analyze</td>
</tr>
<tr>
<td>Get In</td>
<td>Very High</td>
<td>Report &amp; Analyze</td>
</tr>
<tr>
<td>Stay In</td>
<td>High/Med</td>
<td>Search &amp; Investigate</td>
</tr>
<tr>
<td>Stay In</td>
<td>Medium</td>
<td>Add Knowledge</td>
</tr>
</tbody>
</table>

#### Splunk

- High/Med: Search and Investigate
- Medium: Add Knowledge
- Low: Add Knowledge
- Very High: Report and Analyze
- High/Med: Search and Investigate
- Medium: Add Knowledge
- Low: Add Knowledge
Previous State of SOC (Based on SANS Maturity)

- Green Field
- IT Ops operated
- SIEM Based
- MSSP based SOC
- Pretty good SOC
- Adaptive, Effective and Efficient SOC

Monitor
- Security, Access and Network Data
- Limited Endpoint Data
- Limited Cloud Logs

Detect
- Traditional Threats & Operational Hygiene
- Splunk ES and Threat Intel Correlation

Response
- Manual Response
- IT Support Dependent
Our Target State for 2017 (Moving to Level 5)

- Green Field
- IT Ops operated
- SIEM Based
- MSSP based SOC
- Pretty good SOC
- Adaptive, Effective and Efficient SOC

### Monitor
- Additional log sources
- PowerShell Logs
- Sysmon Logs
- Advanced Windows Logs
- Advanced Endpoint Logs
- Cloud Logs

### Detect
- NERC Compliance
- Machine Learning
- Post compromise – Mitre.org
- Threat Hunting

### Response
- Partial automation of ticket creation with SNOW
- Containment automation with Firewall
- Enterprise Security Adaptive Response
# Sample List of Use Cases: We have about 60 New Ones

<table>
<thead>
<tr>
<th>No</th>
<th>Security Essentials</th>
<th>Domain</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Geographically Improbable Access (Superman)</td>
<td>Access Domain</td>
<td>medium</td>
</tr>
<tr>
<td>2</td>
<td>New Local Admin Account</td>
<td>Access Domain</td>
<td>medium</td>
</tr>
<tr>
<td>3</td>
<td>New Logon Type for User</td>
<td>Access Domain</td>
<td>medium</td>
</tr>
<tr>
<td>4</td>
<td>Significant Increase in Interactive Logons</td>
<td>Access Domain</td>
<td>medium</td>
</tr>
<tr>
<td>5</td>
<td>First Time Accessing a GitHub Repository</td>
<td>Data Domain</td>
<td>medium</td>
</tr>
<tr>
<td>6</td>
<td>Remote PowerShell Launches</td>
<td>Network Domain</td>
<td>medium</td>
</tr>
<tr>
<td>7</td>
<td>Source IPs Communicating with Far More Hosts Than Normal</td>
<td>Network Domain</td>
<td>medium</td>
</tr>
<tr>
<td>8</td>
<td>Sources Sending Many DNS Requests</td>
<td>Network Domain</td>
<td>medium</td>
</tr>
<tr>
<td>9</td>
<td>Sources Sending a High Volume of DNS Traffic</td>
<td>Network Domain</td>
<td>medium</td>
</tr>
<tr>
<td>10</td>
<td>Concentration of Hacker Tools by Filename</td>
<td>Endpoint Domain</td>
<td>medium</td>
</tr>
<tr>
<td>11</td>
<td>Anomalous New Listening Port</td>
<td>Endpoint Domain</td>
<td>medium</td>
</tr>
</tbody>
</table>
New Log Configuration

Sysmon, PowerShell, Windows Events
Sysmon Configuration

- We used SwiftOnSecurity’s config as a baseline and modified it to meet our needs
- Key Sysmon Configuration options
  - Exclude Splunk Binaries
    - `<Image condition="is">C:\Program Files\Splunk\bin\splunkd.exe</Image>`
    - `<Image condition="is">C:\Program Files\Splunk\bin\btool.exe</Image>`
  - Include LSASS for Mimikatz type operations
    - `<TargetImage condition="is">C:\windows\system32\lsass.exe</TargetImage>`
- GPO (Group Policy) used for configuration updates
Sysmon – Splunk Configuration

- Splunk Forwarder installed on all Endpoints
- Splunk Sysmon 6.0 TA installed on Search Heads
- Inputs.conf Deployed through Deployment Server to Endpoints
  - ####### Sysmon #######
  - [WinEventLog://Microsoft-Windows-Sysmon/Operational]
  - disabled = false
  - renderXml = true
  - index = yourindex
PowerShell Configuration

- Splunk Forwarder installed on all Endpoints
- WMF 5.1 (Windows Management Framework) deployed to legacy systems (Windows 7). Windows 10 includes WMF 5.X
- Group Policy Configured for Logging
  - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- Deployment Server used to push out configuration
- Inputs.conf for PowerShell (We exclude events that will not be required for forensics or created too much noise)
  - [WinEventLog://Microsoft-Windows-PowerShell/Operational]
  - disabled = false
  - index = yourindex
  - blacklist1 = 4105,4106
  - blacklist2 = EventCode="4103" Message="(?::SplunkUniversalForwarder\bin\splunk-powershell.ps1)"
  - Etc… We have around 6 implemented
Windows Event Logs

▶ Base Config from Ultimate Windows Security and MalwareArchaeology

▶ Enabled Advanced Security Audit Policy Settings
  • Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.

▶ Excluded high volume and low value events (4674)
  • Privilege use, Non Sensitive Privilege Use

▶ Since we are using Sysmon we excluded Detailed Process Tracking Events
  • 4688 - Detailed Tracking, Process Creation
  • 4689 - Detailed Tracking, Process Termination

▶ Event Count Comparison for same 2 hour window
  • Sysmon generated 1.8 Million events across 1,600 hosts
  • 22.6 Million events were created for 4674 (21.9M), 4688/4689 (.7M)
### Windows Event Logs – High Volume Events

**First Set of Events**
- **EventCode**: 4574, **Signature**: An operation was attempted on a privileged object, **Count**: 21,876,702
- **EventCode**: 4524, **Signature**: An account was successfully logged on, **Count**: 441,732
- **EventCode**: 4554, **Signature**: An account was logged off, **Count**: 412,357
- **EventCode**: 4688, **Signature**: A new process has been created, **Count**: 397,231
- **EventCode**: 4669, **Signature**: A process has exited, **Count**: 357,193

**Second Set of Events**
- **Process_Name**: C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE, **Count**: 3,755,723
- **Process_Name**: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe, **Count**: 1,454,790
- **Process_Name**: C:\Windows\System32\lsass.exe, **Count**: 1,415,541
- **Process_Name**: C:\Windows\explorer.exe, **Count**: 1,136,301
- **Process_Name**: C:\Windows\System32\svchost.exe, **Count**: 1,067,223
- **Process_Name**: C:\Windows\System32\RuntimeBroker.exe, **Count**: 1,012,705
Endpoint Detection and Forensics

Sysmon, PowerShell, Windows Events
Storage and Bandwidth

1,727

1,716
User Investigation (First Phase based on HR/Management Approvals)
### User Investigation (Continued from Previous Slide)

#### Internet Traffic

<table>
<thead>
<tr>
<th>src_ip</th>
<th>src_port</th>
<th>displayname</th>
<th>department</th>
<th>src_zone</th>
<th>tac_location desks</th>
<th>dest_ip</th>
<th>dest_port</th>
<th>country</th>
<th>region</th>
<th>city</th>
<th>app</th>
<th>category</th>
<th>sentMB</th>
<th>receivedMB</th>
<th>volMB</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>80</td>
<td>John Doe</td>
<td>Marketing</td>
<td>Global</td>
<td>Head Office, T2,4V2</td>
<td>142.152.124.7</td>
<td>Canada</td>
<td>Alberta</td>
<td>Calgary</td>
<td>104.17</td>
<td>53.14</td>
<td>60.45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.3</td>
<td>80</td>
<td>Jane Smith</td>
<td>Sales</td>
<td>Global</td>
<td>Head Office, T2,4V2</td>
<td>209.99.177.200</td>
<td>Canada</td>
<td>Alberta</td>
<td>Edmonton</td>
<td>2.67</td>
<td>938.07</td>
<td>540.73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.4</td>
<td>80</td>
<td>John Doe</td>
<td>Marketing</td>
<td>Global</td>
<td>Head Office, T3,4V2</td>
<td>208.76.197.223</td>
<td>United States</td>
<td>Washington</td>
<td>Redmond</td>
<td>2.88</td>
<td>853.03</td>
<td>488.30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.5</td>
<td>80</td>
<td>Jane Smith</td>
<td>Sales</td>
<td>Global</td>
<td>Head Office, T2,4V2</td>
<td>142.152.7.222</td>
<td>Canada</td>
<td>Alberta</td>
<td>Calgary</td>
<td>2.88</td>
<td>337.00</td>
<td>343.09</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.6</td>
<td>80</td>
<td>John Doe</td>
<td>Marketing</td>
<td>Global</td>
<td>Head Office, T2,4V2</td>
<td>209.99.177.199</td>
<td>Canada</td>
<td>Alberta</td>
<td>Edmonton</td>
<td>10.39</td>
<td>254.30</td>
<td>366.68</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.7</td>
<td>80</td>
<td>Jane Smith</td>
<td>Sales</td>
<td>Global</td>
<td>Head Office, T2,4V2</td>
<td>208.76.197.194</td>
<td>United States</td>
<td>Washington</td>
<td>Redmond</td>
<td>9.12</td>
<td>236.71</td>
<td>347.93</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.8</td>
<td>80</td>
<td>John Doe</td>
<td>Marketing</td>
<td>Global</td>
<td>Head Office, Data Centre</td>
<td>209.99.177.179</td>
<td>Canada</td>
<td>Alberta</td>
<td>Edmonton</td>
<td>2.67</td>
<td>251.09</td>
<td>216.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.9</td>
<td>80</td>
<td>Jane Smith</td>
<td>Sales</td>
<td>Global</td>
<td>Head Office, Data Centre</td>
<td>209.99.177.200</td>
<td>Canada</td>
<td>Alberta</td>
<td>Edmonton</td>
<td>1.96</td>
<td>266.74</td>
<td>267.80</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### External Emails Sent

<table>
<thead>
<tr>
<th>_time</th>
<th>src_user</th>
<th>recipient</th>
<th>subject</th>
<th>MSiSize</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-05-12 09:09:11</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.35</td>
</tr>
<tr>
<td>2017-05-12 10:30:37</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.23</td>
</tr>
<tr>
<td>2017-05-12 21:56:21</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.31</td>
</tr>
<tr>
<td>2017-05-11 21:56:21</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.31</td>
</tr>
<tr>
<td>2017-05-11 14:14:21</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.01</td>
</tr>
<tr>
<td>2017-05-10 15:01:41</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.02</td>
</tr>
<tr>
<td>2017-05-10 15:02:39</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.05</td>
</tr>
<tr>
<td>2017-05-10 15:07:53</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.10</td>
</tr>
<tr>
<td>2017-05-10 23:30:38</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.03</td>
</tr>
<tr>
<td>2017-05-11 19:15:53</td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td><a href="mailto:jmcnaght@aplan.com">jmcnaght@aplan.com</a></td>
<td>RE: Splunk Partner SEM reference</td>
<td>0.08</td>
</tr>
</tbody>
</table>

#### External Emails Received

<table>
<thead>
<tr>
<th>_time</th>
<th>src_user</th>
<th>recipient</th>
<th>subject</th>
<th>MSiSize</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-05-12 04:14:54</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Rule detected: Block External Emails with Blank Subject Line</td>
<td>0.04</td>
</tr>
<tr>
<td>2017-05-12 09:22:12</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Identity synchronization Error Report Friday 12 May 2017 09:22:12 GMT</td>
<td>0.04</td>
</tr>
<tr>
<td>2017-05-12 09:40:48</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Identity synchronization Error Report Friday 12 May 2017 09:40:48 GMT</td>
<td>0.02</td>
</tr>
<tr>
<td>2017-05-12 04:55:15</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Rule detected: Block External Emails with Blank Subject Line</td>
<td>0.15</td>
</tr>
<tr>
<td>2017-05-12 23:10:01</td>
<td><a href="mailto:communications@optix.com">communications@optix.com</a></td>
<td>uin.ibm.com</td>
<td>Cyber Sec News</td>
<td>0.23</td>
</tr>
<tr>
<td>2017-05-11 23:22:57</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Rule detected: Block External Emails with Blank Subject Line</td>
<td>0.36</td>
</tr>
<tr>
<td>2017-05-12 22:58:35</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Rule detected: Block External Emails with Blank Subject Line</td>
<td>2.84</td>
</tr>
<tr>
<td>2017-05-12 14:40:46</td>
<td><a href="mailto:postmaster@transalta.com">postmaster@transalta.com</a></td>
<td>uin.ibm.com</td>
<td>Top 7 tips for great email signature practices</td>
<td>0.03</td>
</tr>
</tbody>
</table>
Sysmon Example (Where did the Malware or Attack come from? Email, Web, USB, etc.)

We can quickly find all systems with a given file based on the SHA Hash or lookup on a resource like VirusTotal.
Bloodhound & Windows Security Event Log

Bloodhound generates a large amount of events in a short period of time
Various PowerShell Attacker Tools
Detecting Mimikatz
Sysmon and PowerShell to the Rescue
## Group Enumeration

**Sysmon and PowerShell**

### Group Enumeration with Sysmon

```plaintext
<table>
<thead>
<tr>
<th>Time</th>
<th>Host</th>
<th>User</th>
<th>Image</th>
<th>CommandLine</th>
<th>ParentImage</th>
<th>ParentCommandLine</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-10 09:06:24</td>
<td>C:\Windows\System32\svet.exe</td>
<td></td>
<td>C:\Windows\System32\svet.exe</td>
<td>&quot;C:\Windows\System32\svet.exe&quot; group /domain &quot;domain admins&quot;</td>
<td>C:\Windows\System32\svet.exe</td>
<td>C:\Windows\System32\svet.exe group /domain &quot;domain admins&quot;</td>
</tr>
<tr>
<td>2017-08-10 09:06:24</td>
<td>C:\Windows\System32\svet.exe</td>
<td></td>
<td>C:\Windows\System32\svet.exe</td>
<td>&quot;C:\Windows\System32\svet.exe&quot; group /domain &quot;domain admins&quot;</td>
<td>C:\Windows\System32\svet.exe</td>
<td>C:\Windows\System32\svet.exe group /domain &quot;domain admins&quot;</td>
</tr>
<tr>
<td>2017-08-10 09:06:18</td>
<td>C:\Windows\System32\svet.exe</td>
<td></td>
<td>C:\Windows\System32\svet.exe</td>
<td>&quot;C:\Windows\System32\svet.exe&quot; group /domain &quot;domain admins&quot;</td>
<td>C:\Windows\System32\svet.exe</td>
<td>C:\Windows\System32\svet.exe group /domain &quot;domain admins&quot;</td>
</tr>
<tr>
<td>2017-08-10 09:06:18</td>
<td>C:\Windows\System32\svet.exe</td>
<td></td>
<td>C:\Windows\System32\svet.exe</td>
<td>&quot;C:\Windows\System32\svet.exe&quot; group /domain &quot;domain admins&quot;</td>
<td>C:\Windows\System32\svet.exe</td>
<td>C:\Windows\System32\svet.exe group /domain &quot;domain admins&quot;</td>
</tr>
</tbody>
</table>
```

### Group Enumeration with PowerShell

```plaintext
<table>
<thead>
<tr>
<th>Time</th>
<th>Host</th>
<th>TaskCategory</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-10 09:06:24</td>
<td>WinEventLog\Microsoft-Windows-PowerShell\Operational</td>
<td>Execute a Remote Command</td>
<td>Creating Scriptblock text (1 of 1) net group /domain &quot;domain admins&quot; ScriptBlock ID: 00c718a-f732-474b-844e-c5e5e13cd4198 Path:</td>
</tr>
</tbody>
</table>
```
# Security Awareness with USB Drops

## USB Phishing Campaign

### Count of Serial Numbers by Host (One Insert/Removal ~8)

<table>
<thead>
<tr>
<th>host_name</th>
<th>dhcp_ip</th>
<th>dhcp_location</th>
<th>product</th>
<th>serial</th>
<th>count</th>
<th>usb_inserted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISK</td>
<td>#0000000070CE690#</td>
<td>216</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISK</td>
<td>#00000000550002B0#</td>
<td>145</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISK</td>
<td>#000000004F8460#</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISK</td>
<td>#000000004F8460#</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISK</td>
<td>#00000000C5C160#</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISK</td>
<td>#000000004466#</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

### Systems Inserting Phishing USB Over Time

![Graph showing the time over which systems are inserting phishing USBs](image)

#### Details with User and Location based on Local Signature

<table>
<thead>
<tr>
<th><em>time</em></th>
<th>host_name</th>
<th>SAMAccountName</th>
<th>DisplayName</th>
<th>Title</th>
<th>Manager</th>
<th>DepartmentName</th>
<th>serial</th>
<th>destlp</th>
<th>dhcp_lp</th>
<th>DHCP_Description</th>
<th>signature</th>
<th>EventCode</th>
<th>USBRevision</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-09 14:34:35</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:34:34</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:24:38</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:24:39</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:24:38</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:24:38</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:24:38</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-09 14:24:38</td>
<td></td>
<td></td>
<td></td>
<td>Sr Systems Analyst, Security</td>
<td>IT</td>
<td></td>
<td>#000000004F8460#</td>
<td></td>
<td></td>
<td>The workstation was locked</td>
<td>4000</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>2017-08-07 19:14:18</td>
<td></td>
<td></td>
<td></td>
<td>HR Business Partner, Australia</td>
<td>Gas Operations</td>
<td></td>
<td>#00000000550002B0#</td>
<td></td>
<td></td>
<td>The workstation was unlocked</td>
<td>4801</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
New Correlation Searches in ES
## Additional Benefits of Endpoint Logs 1 of 2

<table>
<thead>
<tr>
<th>Search</th>
<th>Application Crashes</th>
<th>Application Crashes for Office</th>
<th>Application Hangs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BSOD - Bugcheck</td>
<td>Computers Added and Removed</td>
<td>Computer Crashes</td>
</tr>
<tr>
<td></td>
<td>Desktop Service Status</td>
<td>Disk Issues</td>
<td>Disk Space Free</td>
</tr>
<tr>
<td></td>
<td>Logon Information by Computer</td>
<td>Logon Information by User</td>
<td>Memory Details by Host</td>
</tr>
<tr>
<td></td>
<td>Memory Errors</td>
<td>Microsoft Antimalware</td>
<td>Systems with Hardware Issues</td>
</tr>
<tr>
<td></td>
<td>Users with more than two Computers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**How to Search**

If you are not familiar with the search feature, see one of the following resources:

- **Documentation**
- **Tutorial**

**Search History**

- Expand your search history
Additional Benefits of Endpoint Logs 2 of 2

Desktop Service Status

Top 10 Crashing Apps

Top 10 Hosts with Crashing Apps

Top 10 Hosts with Hanging Apps

Top 10 Hanging Apps

BSOD or Bugcheck

Systems with less than 1GB on C:

Hosts with Bad Blocks

Systems with Low Memory Issues
What’s Next

Automation and Improvements
Automation and Continuous Improvements

- Splunk Enterprise Security Adaptive Response for High Fidelity Alerts
  - Add attacker IP to Firewall rule
  - Ransomware type indicators based Sysmon data. E.g. Shutdown workstation
- Use ES Glass Tables to Notable Events on the Cyber Kill Chain
- More Red Team Exercises to fine tune our alerts and capabilities
- SOC/Security team to validate current and new use cases with lab system
## References and Links

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Cheat Sheets</td>
<td><a href="https://www.malwarearchaeology.com/cheat-sheets/">https://www.malwarearchaeology.com/cheat-sheets/</a></td>
</tr>
<tr>
<td>Adversarial Tactics, Techniques &amp; Common Knowledge</td>
<td><a href="https://attack.mitre.org/wiki/Main_Page">https://attack.mitre.org/wiki/Main_Page</a></td>
</tr>
<tr>
<td>FireEye on PowerShell</td>
<td><a href="https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html">https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html</a></td>
</tr>
<tr>
<td>Sysmon Resources</td>
<td><a href="https://github.com/MHaggis/sysmon-dfir">https://github.com/MHaggis/sysmon-dfir</a></td>
</tr>
<tr>
<td>Splunk Security Essentials</td>
<td><a href="https://splunkbase.splunk.com/app/3435/#/details">https://splunkbase.splunk.com/app/3435/#/details</a></td>
</tr>
</tbody>
</table>
Q&A

Contact Information

• E-Mail: Kent_Farries@transalta.com
• You can find me on LinkedIn
Q&A
Thank You

Don't forget to rate this session in the .conf2017 mobile app.