Analytic Stories or How I Learned to Stop Worrying and Respond to Threats

David Dorsey | Principal Research Engineer

September 2017 | Washington DC
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.
Splunk Security Research Team
• We really just create memes all day

Been around for almost 15 years now, mainly on defensive side

RE, IR, File Analysis, Network Analysis, Machine Learning

Loves
• BBQ
• Pie

Dislikes
• Pants
• Socks
Agenda

- Level setting
- Analytic story anatomy
- Building an analytic story
- Analytic story in action
Level Setting

What are we talking about?
What Should We Take From This Talk

- Analytic Stories Will Help
  - Demonstrate the value of your data
  - Get value from your data quicker
  - Prioritize data ingestion
  - Understand your defensive posture
  - Resolve incidents faster
  - Empower your analysts
Why Are We Here

Analytic Story

- It’s about understanding, not detection
- Empowering the analyst
- A collection of searches grouped together around a common theme
- Associated metadata
  - References
  - Industry Frameworks
  - Descriptions
  - Data Required
Detection Search
- Finds a specific behavior

Investigative Search
- Help investigate the detected event

Contextual Search
- Gathers context to enrich the detected event

Support Search
- Helps setup the detection search
Buzz Words

► Kill Chain

• The Cyber Kill Chain is where the stages of an attack are enumerated. And likewise, they can be used for protection of an organization's network.
  • Reconnaissance
  • Weaponization
  • Delivery
  • Exploitation
  • Installation
  • Command & Control
  • Actions on Objective
More Buzz Words

- Center for Internet Security Critical Security Controls
  - A list of 20 controls to implement to help secure your organization

- MITRE ATT&CK
  - Adversarial Tactics, Techniques, and Common Knowledge
  - Threat modeling methodology and suite of models for the various phases of an adversary's lifecycle
Analytic Story Anatomy

A story by any other name…
Building Blocks

- Manifest File
  - JSON Specification
- A story can consist of multiple searches
- A search can belong to multiple stories
Schemas

- Different schemas for searches and stories
  - Facilitate the many to many mappings

- Next few slides will focus on some of the fields we found useful to track
  - Why we found them useful
  - What are the benefits to tracking them
Why Many to Many

► Stories should contain multiple searches
  • More than one way to detect something
  • More than one behavior that should be detected by the story

► Searches belong to many stories
  • It’s often not clear right away what a specific behavior means
  • Consider schtasks.exe
    • Legitimate behavior by your sys admin?
    • Being used for lateral movement?
    • Being used for persistence?
    • Being used for privilege escalation?
BRACE YOURSELF

WALLS OF TEXT ARE COMING
Search Manifest

- analytic_story
  - List of stories this search belongs to
- author
- modification_time
- creation_time
- version
- status
  - Where in the development cycle is this?
Search Manifest - The Sequel

- search
  - The SPL

- search_id
  - Unique identifier

- search_name

- search_type
Search Manifest – Where’s the Data?

- **data_models**
  - List of any data models used by this search

- **data_sourcetypes**
  - List of any specific sourcetypes referenced in the search

- **data_source**
  - List of the sources of data for this search
    - Next gen firewall, ETDR agent, Microsoft Windows Event Logs

- **providing_technologies**
  - List of technologies that can provide that information
Search Manifest - Words

- **search_description**
  - High level description of the search and what its goal is

- **eli5**
  - Explain it like I’m 5 - Much more detailed explanation of the SPL

- **how_to_implement**
  - Some assembly required
Search Manifest – How Does This Fit

- Mappings

- Currently we map to three frameworks
  - Kill Chain
  - Center for Internet Security Critical Security Controls
  - MITRE ATT&CK
Why Do We Map?

- Multiple Frameworks
  - Each framework has its pros and cons
- Where the search, and ultimately the analytic story, fits into your defensive strategy
- Allows you to understand what part of your defense is strong
- Allows you to identify weaknesses in your defense
- Allows you to navigate a content library to find what you are interested in
Installation and Recon are relatively low in comparison

- Strongest in Actions on Objective
Search Manifest – When Do We Do Things

- Scheduling
  - cron_schedule
  - latest_time
  - earliest_time
Story Manifest!

- author
- requestor
- id
- version
- modification_time
- creation_time
Story Manifest – The Info

- name
- category
  - High level categories
- description
- narrative
- references
Story Manifest – The Searches

- detection_searches
- investigative_searches
- contextual_searches
- support_searches
Building An Analytic Story
Developing Stories

▲ Can be time consuming, so why do it?
▲ Empower analysts to explore events
  • Many contextual and investigative searches are shared across stories
  • Quicker response times
▲ Demonstrate value of the data you are ingesting
▲ Allows you to prioritize what data you want to ingest
▲ Map your defensive posture
▲ Allows you to prioritize what new analytics to write
How We Develop Stories

► Analytic stories allows for flexibility in topic
  • Threat actors
  • Malware families
  • Malware techniques
  • Malware of the day

► Standard Process
  • Knowledge Acquisition
  • Codification
  • Testing
  • Deploy
Knowledge Acquisition

- The sites you go to and learn from become the references
Codification

- Start with the basics of the story manifest
- Some fields are easy to fill out
  - id
  - creation_time
  - modification_time
  - version
  - author
  - requester
  - name
  - references
Codification

Some require some thought

- category
- description
- narrative
Detection Searches

- No idea is too horrible at this point
- Don’t have to worry about the details… yet
  - USN Journal Deletion
  - Deleting Shadow Copies
  - Spike in File Writes
  - Common Ransomware Extensions
  - Common Ransomware Notes
  - Detect SMB Traffic Allowed
  - Detect Spike in SMB Traffic
  - Monitor TOR traffic
Still, no idea is too horrible at this point

Searches to give you a better understanding of your environment

- Monitor Successful Backups
- Monitor Unsuccessful Backups
- Windows Updates Install Failures
- Windows Updates Install Successes
- Common Vulnerabilities Used By Ransomware
Once again, no idea is too horrible at this point

What would you want to know to help scope this event

• Backup Status of Endpoint
• Patch Status of Endpoint
• Vulnerability Status of Endpoint
• Get Authentication Logs For Endpoint
• Get Notable History
• Get User Information from Identity Table
Investigative Searches

- Things get tricky here
- Don’t have to worry about the details… yet
  - Get Process Info
  - Get Process Information For Port Activity
  - Investigate Web Activity
  - Get Parent Process Info
At this point, we have an outline of a story

- Bunch of searches
- References

Need to start filling in the details
Let’s write the search

```plaintext
index=* (sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR tag=process) (process=*vssadmin* OR process=*wmic*) cmdline=*delete* cmdline=*shadow* | stats count min(_time) as firstTime max(_time) as lastTime by dest, user, process, cmdline | `ctime(firstTime)` | `ctime(lastTime)`
```
It’s All About The Data

► What type of data do we need (data_source field)
  • Endpoint Intelligence

► Where can we get this data (providing technologies)
  • Carbon Black Response
  • CrowdStrike Falcon
  • Sysmon

► Fill out data_sourcetypes or data_models as appropriate
The Details

► Search Description
  • The vssadmin.exe utility is used to interact with the Volume Shadow Copy Service. Wmic is an interface to the Windows Management Instrumentation. This search looks for either of these tools being used to delete shadow copies

► How to Implement
  • To successfully implement this search, you need to be ingesting logs with both the process name and command line from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

► ELI5
  • This search looks for execution of vssadmin or wmic with both the "delete" and "shadow" parameters passed on the command line. The two arguments are searched for separately because we can't predict the number of spaces between the words on the command line. The search will return the number of times this activity was observed, and the times of the first and last event."
The Mappings

► Kill Chain Phase
  • Actions on Objective

► CSC 20
  • CSC 8 – Malware Defenses
  • CSC 10 – Data Recovery Capability

► ATT&CK
  • Execution
Why Did I Just Do All That

- Allows you to prioritize what data you want to ingest
- Demonstrate value of the data you are ingesting
- Empower analysts to explore events
- The beginnings of orchestration
- Map your defensive posture
- Allows you to prioritize what new analytics to write
Analytic Story In Action
Analytic Stories At Splunk

- Not just theory, we’re here to help
- Enterprise Security Content Updates
  - Library of Analytic Stories
  - Stories distributed as an app on SplunkBase
  - AR Action to automatically gather context and begin investigation
Analytic Stories At Splunk

Total Analytic Stories: 25

Categories:
- Vulnerability
- Best Practices
- Malware

Analytic Stories Updated in Last 2 Weeks: 25

Analytic Stories by CIS Critical Security Control:

Critical Security Control: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 18

Analytic Stories:
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 18

© 2017 SPLUNK INC.
**Ransomware**

**Description:**
Activities, techniques, and best practices associated with detecting, investigating, and mitigating your risk to ransomware

**Narrative:**
Ransomware is an ever-present risk to many enterprises where by an infected host encrypts business critical data until the victim pays the attacker a ransom. There are many types and varieties of Ransomware which can affect an enterprise. Attackers can deploy Ransomware to enterprises through spear phishing campaigns, drive by downloads as well as through traditional remote service-based exploitation. In the case of the WannaCry campaign there was self-propagating wormable functionality that was used to maximize infection. To effectively combat Ransomware organizations can apply several techniques to detect and or mitigate the effects of Ransomware.

**Attack:**
- Command and Control
- Windows Management Instrumentation
- Masquerading
- Commonly Used Port
- Indicator Removal on Host
- Exfiltration Over Alternative Protocol
- Exfiltration
- Registry Run Keys / Start Folder
- Defense Evasion
- Execution
- Persistence

**Kill Chain Phases:**
- Command and Control
- Actions on Objective
- Delivery

**CIS 20:**
- CIS 10
- CIS 8
- CIS 9
- CIS 6
- CIS 12
- CIS 5
- CIS 3

**Data Model:**
- Application_State
- Change_Analysis
- Network_Traffic
- Updates
- Vulnerabilities

**Technologies:**
- Bro
- Carbon Black
- CrowdStrike Falcon
- Linux
- Microsoft Windows
- Netbackup
- OS X
- Palo Alto
- Splunk Enterprise Security
- Splunk Stream
- Sysmon
Analytic Stories At Splunk

ESCU - Deleting Shadow Copies

**Configuration in ES**

**Description**
The `vssadmin.exe` utility is used to interact with the Volume Shadow Copy Service. `Wmic` is an interface to the Windows Management Instrumentation. This search looks for either of these tools being used to delete shadow copies.

**EQL**
This search looks for execution of `vssadmin` or `wmic` with both the "delete" and "shadows" parameters passed on the command line. The two arguments are searched for separately because we can't predict the number of spaces between the words on the command line. The search will return the number of times this activity was observed, and the times of the first and last event.

**Search**

```kql
index=* (sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon /Operational OR tag=process) (process=*vssadmin* OR process =*wmic*) cmdline=*delete* cmdline=*shadow* | stats count min (_time) as firstTime max(_time) as lastTime by dest, user, process, cmdline | `ctime(firstTime)` | `ctime(lastTime)`
```

**Data Models**

- Carbon Black
- CrowdStrike Falcon
- Sysmon
- Tanium
- Ziften

**Att&ck**

**Execution**

**Kill Chain Phases**

**Actions on Objective**

- **CIS 20**
  - CIS 8
  - CIS 10

**Asset at Risk**

**Endpoint**

**Confidence**

**medium**
Analytic Stories At Splunk

Context

- ESCU - Get Authentication Logs For Endpoint
- ESCU - Get Backup Logs For Endpoint
- ESCU - Get Notable History
- ESCU - Get Update Logs For Endpoint
- ESCU - Get User Information from Identity Table
- ESCU - Get Vulnerability Logs For Endpoint
Analytic Stories At Splunk

<table>
<thead>
<tr>
<th>Response</th>
<th>Mode</th>
<th>Time</th>
<th>User</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESCU-Contextualize</td>
<td>adhoc</td>
<td>2017-09-22T01:54:49-0500</td>
<td>system</td>
<td>✓ success</td>
</tr>
<tr>
<td>Notable</td>
<td>saved</td>
<td>2017-09-21T15:55:31-0500</td>
<td>admin</td>
<td>✓ success</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>saved</td>
<td>2017-09-21T15:55:31-0500</td>
<td>admin</td>
<td>✓ success</td>
</tr>
</tbody>
</table>

View Adaptive Response Invocations
### Analytic Stories At Splunk

**ESCU Context**

**ESCU - Get Notable History**

<table>
<thead>
<tr>
<th>owner</th>
<th>priority</th>
<th>rule_name</th>
<th>search_name</th>
<th>severity</th>
<th>status, description</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Common Ransomware Notes</td>
<td>ESCU - Get Notable History</td>
<td>high</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:15:59.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Common Ransomware Notes</td>
<td>ESCU - Get Notable History</td>
<td>high</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:16:02.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Registry Keys Used For Persistence</td>
<td>ESCU - Get Notable History</td>
<td>medium</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:21:04.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Registry Keys Used For Persistence</td>
<td>ESCU - Get Notable History</td>
<td>medium</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:21:04.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Registry Keys Used For Persistence</td>
<td>ESCU - Get Notable History</td>
<td>medium</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:21:07.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Deleting Shadow Copies</td>
<td>ESCU - Get Notable History</td>
<td>high</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:21:24.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Common Ransomware Notes</td>
<td>ESCU - Get Notable History</td>
<td>high</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:21:57.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Common Ransomware Notes</td>
<td>ESCU - Get Notable History</td>
<td>high</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:22:02.000000:00</td>
</tr>
<tr>
<td>unassigned</td>
<td>unknown</td>
<td>Registry Keys Used For Persistence</td>
<td>ESCU - Get Notable History</td>
<td>medium</td>
<td>Event has not been reviewed</td>
<td>2017-09-21T11:25:24.000000:00</td>
</tr>
</tbody>
</table>

### ESCU - Get Backup Logs For Endpoint

**ESCU - Get Backup Logs For Endpoint**

<table>
<thead>
<tr>
<th>dest</th>
<th>search_name</th>
<th>signature</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>winterfell</td>
<td>ESCU - Get Backup Logs For Endpoint</td>
<td>An error occurred, failed to backup.</td>
<td>2017-09-17T23:53:30.434000:00</td>
</tr>
<tr>
<td>winterfell</td>
<td>ESCU - Get Backup Logs For Endpoint</td>
<td>The task was created.</td>
<td>2017-09-17T23:53:29.434000:00</td>
</tr>
<tr>
<td>winterfell</td>
<td>ESCU - Get Backup Logs For Endpoint</td>
<td>An error occurred, failed to backup.</td>
<td>2017-09-14T21:09:17.324000:00</td>
</tr>
<tr>
<td>winterfell</td>
<td>ESCU - Get Backup Logs For Endpoint</td>
<td>The task was created.</td>
<td>2017-09-14T21:09:16.324000:00</td>
</tr>
</tbody>
</table>
Where Do We Go From Here
Beyond Infinity

- Adding remediation steps into story
- Build out content library
- Add in more automation
Takeaways

▶ It’s about understanding, not detection
  • What data do you need
  • What behaviors are you looking for
  • What value are you getting from your data
  • What are the next steps you take to validate your discovery

▶ Allows you to map your defensive strategy
  • Know your strengths
  • Know your weaknesses

▶ Faster time to resolution
  • Save time (and $$$)
  • Quicker time to value
  • Uplevel your analysts
Stories For Everyone

- Enterprise Security Content Updates
- https://splunkbase.splunk.com/app/3449/
Thank You

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