The Art of Detection

Using Splunk Enterprise Security

Doug Brown  |  Senior Information Security Analyst, Red Hat
95B6 922E 47D2 7BC3 D1AF F62C 82BC 992E 7CDD 63B6

September 27, 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.
May this presentation improve the security of organizations great and small.
Doug “trustedsubject” Brown
Fond of SELinux
SplunkTrust member
Author of more than a dozen Splunkbase apps, incl Auditd
2016 Developer Revolution Award Winner
Contributor to ES roadmap
Preparing for a Successful ES Engagement:
• https://www.splunk.com/blog/2016/10/24/preparing-for-a-successful-enterprise-security-ps-engagement.html
Overview

1. Operational Security at Red Hat
2. A New Triage Paradigm
3. Correlation Search Development Process
4. Extensions and Customizations
5. Case Study
Leading Open Source vendor
Global team of 14 people, dealing with various aspects of corporate security
Splunk customer since v4.1
TB+ license

Needed tool to support workflow and whole incident management lifecycle
Cost & risk of developing/maintaining our own tool was considered greater than ES
Implemented ES at end of last year
Enterprise Security is just a framework upon which to \textit{build} a world-class security operation
A New Triage Paradigm

Our strategy to address alert fatigue and find what really matters.
What Makes An Alert Actionable?

One or more of these?

- High Confidence?
- A Realised Threat?
- Must Be Rectified By Human?
- Substantial Evidence?
Intrinsically Actionable
We falsely think we can detect "badness"

Our detection mechanisms are bias towards early stages of the kill-chain where there's greater entropy and lower fidelity

The hidden problem is that due to our assumption we're not actually detecting the genuinely bad things that present a real risk to organisation

Solution

- Change-based correlation searches
- Risk-based incident detection
- Auto-close notables (no analyst triage required)
- Triage high-risk objects, prioritised by urgency (object priority x aggregated risk)
Alert Fatigue

Result

- Abstract rather than concrete approach to operational security allows unknown threats to be detected
- Analysts can concentrate on hunting and prioritise their triage time
- Analysts triage less than 6 objects in a shift (often none)
- Changes the notion of what constitutes a false-positive

Requirements/Assumptions

- Bad actor changes something in order to achieve their actions on objective
- Sufficient data across attack surface ingested and normalised
- Identity and asset prioritisation
- Team of creative analysts
- Suite of correlation searches
Q: Why bother raising notables if they’re not triaged?
  • A: To summarise and retain evidence
  • A: Provide the means for higher-order correlation searches that perform meta-analysis of trends and anomalies across notables

Q: If not triaging notables, which dashboards are used first for triage:
  • A: “Security Posture” & “Risk Analysis”

Q: Why stop triaging notables raised by high-fidelity correlation searches?
  • A: If they are intrinsically actionable, then they should be triaged by an analyst
Security Event Tiering

**Tier 1**
Raw information and events from security tools
Typically low fidelity (“could be bad”) and not intrinsically actionable

**Tier 2**
Behaviour-based correlation search notables
Typically medium fidelity (“looks bad”) and generally not intrinsically actionable

**Tier 3**
Object risk/sequence-based correlation searches
High fidelity (“likely bad”) and requires attention

**Tier 4**
Abstract risk-based correlation searches
High fidelity (“likely bad”) and requires attention
Correlation Search Development Process
1st: The Idea
How we produce a behaviour of interest

- What is the org concerned about?
- What does it look like?
2nd: The Source
How we prepare the data into the form required

- Scope and Abstraction
- Period and Acceleration
- Cleaning, Checking and Filtering
- Enrichment and Modelling
3rd: The Metric
How we measure the behaviour of interest

- Signatures and Blacklists
- Statistics and Bounds
- Set Operations
- State Machines
4th: The Conditions

How do we determine when the behaviour is of interest

- Simple Threshold / Predicate
- Dynamic Threshold / Predicate
- Multi-Stage Conditionals
- Sequences
Extensions and Customizations

Developing a SIEM to meet the needs of your team.
Enrichment

Internal

- Network Sessions (DHCP lease, VPN session)
- User Endpoints (learnt devices)
- pDNS (derived from DNS logs / wire data)
- Notable Comment Key-Value Extraction
- Internal Subnets
- User Watchlist
  (https://splunkbase.splunk.com/app/3591/)
- Notable Macro

External

- Autonomous System Lookup
  (https://splunkbase.splunk.com/app/3531/)
- In-line Whois
  (https://splunkbase.splunk.com/app/3506/)
- pDNS
  (https://splunkbase.splunk.com/app/3050/)
- Democracy Index
Enrichment
Network Sessions and BYOD Devices

Attribution of network activity to a specific user/device

Network Sessions lookup:
- Source: VPN session / DHCP lease start events
- KVStore Collection-based temporal lookup
- “Appended” by scheduled search run every few minutes
- Another scheduled search periodically prunes old sessions from the lookup to ensure size doesn’t grow indefinitely
- Fields: start, src_mac, src_ip, user, nt_host, assigned_ip

Check carefully your events aren’t lying to you.
Enrichment
Network Sessions and BYOD Devices

Attribution of device to a specific user

User Endpoints lookup:
- Source: Auth events with src_ip
- KVStore Collection-based lookup
- “Appended” by scheduled search run periodically
- Uses Network Sessions lookup to determine MAC address
- Fields: key(network_session_src_mac), os_type, nt_host, user, updated

Automatically learns about devices, when last used and who owns them.

ES asset source with asset priority mirroring the user that owns the device.
Enrichment
Notable Comment-derived Dynamic Enrichment

- The fields in notables are fixed* but analysts find information during triage
- We want to be able to add field values dynamically so they can be pivoted upon and to ensure the investment of analyst time in triaging notables is most effectively reused
- If we associate a notable with a user, it can then appear in their swimlane
- Free-form prose with Key-Value pairs according to CIM-based taxonomy.
Enrichment
Scheduled Search To Build Extraction Lookup

| `incident_review`

| rename comment as _raw | extract mv_add=true | rename _raw as comment

| search user=* OR src_ip=* OR …

| stats values(user) as user values(src) as src ... by rule_id

| mvexpand <multi_value_fields>

| outputlookup incident_review_comment_extractions
**Enrichment**

**Dynamic Notable Enrichment**

This macro is used by all ES' notable dashboards, etc.

Example of custom commands appended to macro to add arbitrary and dynamic notable enrichment.

**SA-ThreatIntelligence/local/macros.conf:**

```bash
[notable_by_id(1)]
definition = `get_notable_index` \n| `get_event_id` \n| search event_id="$event_id$" \n| ... \n| lookup user_watchlist _key AS user OUTPUT start AS watchlist_start, end AS watchlist_end, reason AS watchlist_reason, comment AS watchlist_comment, creator AS watchlist_creator \n| eval watchlist=if(isnotnull(watchlist_start),if(watchlist_start<_time AND watchlist_end>_time,watchlist_reason + ": " + if(isnull(watchlist_comment),"no comment",watchlist_comment) + " (" + watchlist_creator + ")","On watchlist either before or after this notable"),null())
```
Customizations

E-mail Workflow Action

- Workflow actions are just links
- We can use URL encoded mailto: links with tokens
- Each workflow action is then an e-mail template that auto-populates
- Approach allows us to PGP sign e-mails
Customizations

Risk Object Value

- Provides means to sort notable table and search across notables
- Use eval in correlation searches to add "risk_object_value" field to notables
- Add "Table Attribute" via "Incident Review Settings" dashboard

E.g. … | eval risk_object_value=if(like(src_ip,"10.%"),src_ip,dest_ip)
Customizations
Custom Identity and Asset Information

- Inability to add arbitrary identity/asset information is a common complaint
- Create a csv lookup and apply to [default] stanza in props.conf
  - LOOKUP-zd_identities_supplementary = identities_supplementary user

![User role analysis](image)
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin_city</td>
<td>San Francisco</td>
</tr>
<tr>
<td>admin_country</td>
<td>US</td>
</tr>
<tr>
<td>admin_fax_ext</td>
<td>Admin Email: <a href="mailto:admin@linuxfoundation.org">admin@linuxfoundation.org</a></td>
</tr>
<tr>
<td>admin_name</td>
<td>Jim Zemlin</td>
</tr>
<tr>
<td>admin_organization</td>
<td>The Linux Foundation</td>
</tr>
<tr>
<td>admin_phone</td>
<td>+1 4157239709</td>
</tr>
<tr>
<td>admin_phone_ext</td>
<td>Admin Fax: +1 9712582363</td>
</tr>
<tr>
<td>admin_postal_code</td>
<td>94129</td>
</tr>
<tr>
<td>admin_street</td>
<td>1 Letterman Drive, Building D, Suite D4700, Suite 102</td>
</tr>
<tr>
<td>creation_date</td>
<td>1997-03-07T05:00:00Z</td>
</tr>
<tr>
<td>dnssec</td>
<td>unsigned</td>
</tr>
<tr>
<td>domain_name</td>
<td>KERNEL.ORG</td>
</tr>
<tr>
<td>name_server</td>
<td>NS11.CONSTELLIX.COM, NS21.CONSTELLIX.COM, NS31.CONSTELLIX.COM, NS41.CONSTELLIX.COM, NS51.CONSTELLIX.NET, NS61.CONSTELLIX.NET</td>
</tr>
<tr>
<td>registrant_city</td>
<td>San Francisco</td>
</tr>
<tr>
<td>registrant_country</td>
<td>US</td>
</tr>
<tr>
<td>registrant_fax_ext</td>
<td>Registrant Email: <a href="mailto:admin@linuxfoundation.org">admin@linuxfoundation.org</a></td>
</tr>
<tr>
<td>registrant_name</td>
<td>Jim Zemlin</td>
</tr>
<tr>
<td>registrant_organization</td>
<td>The Linux Foundation</td>
</tr>
</tbody>
</table>
User Watchlist Editor
https://splunkbase.splunk.com/app/3591/

- Provides interface to add/edit/remove watchlist users and meta-data
- Able to be integrated with ES Identity sources:

```plaintext
| lookup user_watchlist_key AS identity OUTPUT end AS watchlist_end
| eval watchlist=if(isnotnull(watchlist_end),if(watchlist_end>now(),"true",null()),null())
| fields - watchlist_end
```
A Snort alert has been raised by the following action: Please see Next Steps for triage process.

<table>
<thead>
<tr>
<th>Additional Fields</th>
<th>Value</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic SID</td>
<td>14061</td>
<td></td>
</tr>
<tr>
<td>Destination ASN</td>
<td>67.205.128.0/18</td>
<td></td>
</tr>
<tr>
<td>Destination ASN Subnet</td>
<td>67.205.186.140</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>apple.com:cyber-security-analysis.site</td>
<td></td>
</tr>
<tr>
<td>HTTP Method</td>
<td>GET</td>
<td></td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Macintosh</td>
<td></td>
</tr>
<tr>
<td>Source MAC Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Subnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td><a href="http://apple.com/cyber-security-analysis.site">http://apple.com/cyber-security-analysis.site</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>en/index.php?jess=4fe6937f7eb1ce0ba857ebde544f5c&amp;os=OS X 10.12&amp;app=Mackeeper&amp;volume=Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://track.trafficanalytics.com/load_m.php?os=OS%20X%2010.12&amp;app=Mackeeper&amp;">http://track.trafficanalytics.com/load_m.php?os=OS%20X%2010.12&amp;app=Mackeeper&amp;</a></td>
<td></td>
</tr>
</tbody>
</table>

| Correlation Search:     | Network - 00002.001-DEV-GEN-INV: Snort alert - Rule |

| History                  | 2017 Aug 9 2:18:42 pm Douglas Brown E-mailed the associate to check if Mackeeper is installed. |

| View all review activity for this Notable Event |

| Contributing Events:    | View bro events for | Original Hitlist and full 2017-01-18 19:15:28 18:42|

| Adaptive Responses:     |                      |

<table>
<thead>
<tr>
<th>Response</th>
<th>Mode</th>
<th>Time</th>
<th>User</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notable</td>
<td>saved</td>
<td>2017-08-09T15:11+0000</td>
<td>admin</td>
<td>success</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>saved</td>
<td>2017-08-09T15:11+0000</td>
<td>admin</td>
<td>success</td>
</tr>
</tbody>
</table>

| View Adaptive Response Invocations |

| Next Steps:              | |

- Snort-based IDS Notable Triage Process:
  1. Assign notable to yourself with "In Progress" status.
  2. Look at name of signature and Risk Object. Close notable with rationale if clearly a duplicate or False-Positive/Intrusion.
  3. Open Asset Investigator for Risk Object.
  4. Attempt to determine user in Authentication phase of malware (if not already notable) and add to notable with user="name" key-value pair. If still unknown, consult the malware threat map and signature list. If malware is unknown, add to notable with user="agent" key-value pair.
  5. Look back at least 7 days in Asset Investigator for concerning activity in the same lanes.
  6. If satisfied, close notable with rationale; otherwise, open a bug and drill-down search.
  7. If bug is open, add comment to notable with user="agent" key-value pair and add to notable with user="agent" key-value pair. If still unknown, consult the malware threat map and signature list. If malware is unknown, add to notable with user="agent" key-value pair.
  8. If satisfied, close notable with rationale; otherwise, consider pivoting on indicator to Malware and adding "Uncomfortable" tag to event_hash or contacts to associate by pivoting on email to email template.
  9. Add comment to notable indicating the associated hash has been contacted, and put state to "Pending".
  10. Close notable once consultation with associate has completed.
User and Asset Investigator Dashboards

Change in behaviour

Custom swimlanes

All Authentication
All Changes
IDS Attacks
Malware Attacks
Sinkhole
Notable Events
Risk Modifiers
Threat List Activity
Unusual pDNS

Search returned no results
Search returned no results
Search returned no results
Case Study

Third Man Correlation Search
Third Man Correlation Search
https://splunkbase.splunk.com/app/2830/

1st: The Idea
- No 2FA?
- Can we detect the use of phished credentials?
- Humans are predictable ∴ changes in pattern can be detected?
Third Man Correlation Search

2nd: The Source

Scope and Abstraction
- Authentication data model
- “Period” is abstraction of time

Period and Acceleration
- 30 days+
- Accelerated datamodel used to periodically update model
- Requires scheduled search to periodically remove old model entries

Cleaning, Checking and Filtering
- Check CIM normalisation
- Filter out new users

Enrichment and Modelling
- Autonomous System lookup: https://splunkbase.splunk.com/app/3531/
- KVStore lookup model: user, src_as, dest, app, wday, period (5 vectors)

```python
eval period=case(date_hour<5, 0, date_hour<8, 1, date_hour<12, 2, date_hour<17, 3, date_hour<20, 4, date_hour<24, 5)
```
Third Man Correlation Search
3rd: The Metric

- Set Operations Technology Add-On: [https://splunkbase.splunk.com/app/3516/](https://splunkbase.splunk.com/app/3516/)
- “unique_vectors” metric produced by `distinctfields` custom search command

* Diagram used for illustrative purposes only - does not represent a distinct set.
Third Man Correlation Search

4th: The Conditions

… | where unique_vectors>2
Third Man Correlation Search
5th: The Triage

Fields and Documentation

- user, src_ip, src_as, dest, app, unique_vectors, unique_vector_count

Analysis and Enrichment

- Drilldown search to table of user’s authentication activity

Actions and Remediation

- Raise notable
- Aggregate risk - scaled dynamically in-line by number of unique vectors
- Place user on watchlist? (https://splunkbase.splunk.com/app/3591/)

Fidelity and Refinement

- Check for apps or other vector values to filter out
- Check CIM normalisation for inconsistencies
- Consider extending earliest time to improve fidelity
Key Takeaways

1. How to build your SIEM with ES
2. “intrinsically actionable”
3. Changes in behaviour are key
4. Risk-centric view to incident detection
5. How to develop detection techniques
Q&A
Thank You

Don't forget to rate this session in the .conf2017 mobile app
Bonus Material
UTC field in all events/notables

- You may have noticed the ‘utc’ field in the screenshots
- Geographically distributed security teams have to speak a common time
- This is especially important when extracting evidence
  - … | table _time utc index source sourcetype host _raw

props.conf:

[default]
EVAL-utc = strftime(_time - (60 * 60 * tonumber(substr(strftime(_time,"%z"),2,2))) + (60 * tonumber(substr(strftime(_time,"%z"),4,2))), "%Y-%m-%d %H:%M:%S UTC"
Bonus Material
 rawData search in Incident Review dashboard

- Much of the information in notables is not searchable without knowing fieldnames
- One solution is to “recreate” _raw to include *all* the enrichment fields
- JSON Tools app (https://splunkbase.splunk.com/app/3540/)
- In the notable_by_id(1) macro, add:
  - … | mkjson
  - Must be before the $event_id$ search command but after enrichment

Notable search now works like core Splunk search.