Keeping Track Of All The Things

A use-case and content management story

Matt Parks | Manager, Kaiser Permanente
Ruperto Razon | Sr. Threat Analyst, Kaiser Permanente

8/12/2017 | ver 5.2.2
Our Purpose

- Share our lessons learned in consolidating artifacts of our migration from a previous SIEM to our current SIEM/logging solution

- Describe the process our team developed to manage our security use-case and content development efforts

- Provide you some answers to a few familiar questions
What Questions? These Questions

- What does our security coverage look like, from a use-case perspective?

- Bob in accounting was infected by <insert-threat-of-the-day-here>, who else was infected?

- How are we tracking towards our high level security goals for the year?

- What does your development team do all day?
Who are you guys?

Matt Parks
Manager, Security Analytics, Cyber Risk Defense Center

▶ Matthew.Parks@kp.org
▶ linkedin.com/in/matthewparks
Who are you guys?

Ruperto Razon
Sr. Threat Analyst, Security Analytics, Cyber Risk Defense Center

- Ruperto.S.Razon@kp.org
- linkedin.com/in/PertoRazon
- @thatperto
Cyber Risk Defense Center (CRDC)

New approach:
Monitor intel and align with kill chain

CTI: Advanced Warning

Infiltration: Malware

Escalation: Lateral Movement

Exfiltration

Traditional SOC approach:
Respond to billions of alerts

Tier 1 Analysts

Tier 2 Analysts

Tier 3 Analysts
Advanced and Actionable Intelligence

MODIFIED KILL CHAIN

- Reconnaissance
  - Threat Intelligence
  - Tools: Threat Feeds (paid, Open Source, Internal)
  - Contextual Information (Virus Total, whois, etc.)
  - Farsight
  - Industry Relationships
  - Law Enforcement

- Exploitation
  - Infiltration
  - Tools: Malware Detonation
  - Network Intrusion Detection and Prevention
  - Endpoint Security
  - SMTP Gateways
  - Layer 7 Detection and Prevention

- Lateral Movement
  - Tools: Endpoint Security Devices
  - OS Logging
  - User modeling
  - PCAP data

- Reach Objective
  - Tools: Network DLP
  - Endpoint DLP
  - Email DLP
  - PCAP data
  - Cloud Security technology

DATA LAYER

- Splunk
- Other Big Data Platforms

ACTIONABLE INTELLIGENCE
Let’s start from the middle….

Pre-Migration (Summer 2015)

- 2TB+ data/day
- 128 Threat Use-Cases
- 60 Scheduled Reports
- 652 “Knowledge Objects”
- 15+ Documentation Repositories

Migration Complete (Spring 2016)

- 4TB+ data/day
- 43 Threat Use-Cases
- 33 Scheduled Reports
- 121 Knowledge Objects
- 4 Documentation Repositories
Where We Are Today

- 8+TB data/day
- 60+ distinct sourcetypes
- 75+ Custom Threat Use-Cases
- 100+ Scheduled Reports/Dashboards/Form Searches
<table>
<thead>
<tr>
<th>Name</th>
<th>Date Modified</th>
<th>Size</th>
<th>Kind</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre GoldenEye</td>
<td>Jun 21, 2017, 11:53 AM</td>
<td>2 KB</td>
<td>TextEd.ument</td>
</tr>
<tr>
<td>2017-04-02-13.04.41</td>
<td>2 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-04-02-13.04.41</td>
<td>2 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-04-02-13.04.41</td>
<td>2 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-04-02-13.04.41</td>
<td>2 KB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By using the following correlated events we can learn to understand the underlying behavior of the goldeneye botnet and take necessary action to mitigate it.

### Monitor for Malicious Domain Changes

- **Domain Name:** Example.com
- **IP Address:** 192.168.1.1

Note: Domain names should be reviewed to ensure they are legitimate and not being abused. Monitor for changes in the resolution of known malicious domains.

### Alert on Unusual Network Traffic

- **Source IP:** 10.0.0.1
- **Destination IP:** 10.0.0.2

Alert on unusual network traffic to detect potential reconnaissance or lateral movement activity.

### Monitor System Logs for Malicious Activity

- **Log Source:** Linux System Logs
- **Event ID:** 4624

Monitor system logs for specific event IDs to detect malicious activity such as privilege escalations or credential theft.

### Conclusion

By implementing these monitoring strategies, organizations can detect and respond to the goldeneye botnet effectively. It is essential to continuously review and adapt the monitoring configurations to stay ahead of evolving threats.
Artifacts of Note

- Naming conventions
- Search logic
- Knowledge objects
- Scheduling of searches/reports
- Asset Categories
- Recipients/Users
- Original Requestor
- Tribal Knowledge
Scrum in 100 Words

- Scrum is an agile process that allows us to focus on delivering the highest business value in the shortest time.

- It allows us to rapidly and repeatedly inspect actual working software (every two weeks to one month).

- The business sets the priorities. Teams self-organize to determine the best way to deliver the highest priority features.

- Every two weeks to a month anyone can see real working software and decide to release it as is or continue to enhance it for another sprint.
What does a Scrum look like?

**Product Owner**
The Holder of Product Value
Determines what needs to be done and sets the priorities to deliver the highest value

Traditional approach: Controls the work

**ScrumMaster®**
The Servant Leader
Protecting the Scrum process and preventing distractions

Traditional approach: No equivalent

**Development Team**
The Self-Organizing Group
Takes on and determines how to deliver chunks of work in frequent increments

Traditional approach: Gets told what to do by the project manager
The Scrum Advantage

OVERALL PROJECT TIME LINE

REQUIREMENTS → DEVELOP & TEST → DEPLOY

CHANGE CONTROL

PRODUCT MANAGER PRIORITIZATION

PRODUCT BACKLOG → NEW → NEW → NEW

GO

SPRINT 1 DEV/TEST

SPRINT 2 DEV/TEST

SPRINT 3 DEV/TEST/DEPLOY
Scrum Framework Process

**SPRINT 0**
- Planning Exercise To Prepare For Sprints
- Duration 1-2 Weeks as Needed
- Create Initial Product Backlog:
  - Requirement
  - Acceptance Criteria
  - Story Points
  - Prioritization

**SPRINT 1**
- Shippable Product For Selected User Stories
- Duration = 2 Weeks

- **Day 1**
  - Sprint Planning
    - To Review & Select Highest Priority User Stories For The Sprint From The Backlog
  - User Story Dev & Test
  - Daily Scrum w/Team (15m):
    - Did Yesterday
    - Do Today
    - Blockers?
  - Work Demos To Team

- **Days 2-13**

- **Day 14**
  - Sprint Review:
    - Story Review
    - Approve Demos
  - Sprint Quality Retrospective:
    - Start
    - Stop
    - Continue

**SPRINT 2, 3, 4 ....**
- Shippable Product For Selected User Stories
- Duration = 2 Weeks
- Repeat

**New User Stories Created In Product Backlog**

**Product Backlog Grooming & User Story Prioritization**
Example Story

**Summary**

MW Attacking IP High Data Rate Outbound

**Issue Type**

Story

**Assignee**

Matt Parks

**Epic Link**

Security Analytics Operations

**Sprint**

JIRA Software sprint field

**Completed sprints**

Use Case Content Sprint 9

**Story Points**

13

**CRDC Tag**

MW ▫ SA ▫

Use the "CRDC Tag" field as a replacement for the default "Label" field. CRDC Tag uses the Label Manager Plugin.

**Actual Work**

13

**TL; DR**

Alert for attackers with high volume outbound

---

As a member of the team I need to do detect attacking IPs that are receiving a high ratio of data so we can detect potential attacker activity corresponding with potential data exfiltration and respond accordingly.

Acceptance Criteria:

- All sub-tasks are Complete and the correlation search/model has been implemented and is enabled in Production as at least Informational or a low Severity/Confidence
- New Story Created for TV Team to do use case validation

Fix Version/s

- Start typing to get a list of possible matches or press down to select.

Priority

Medium

**Attachment**

Drop files to attach, or browse.

**Linked issues**

relates to

Realm timeout to search for issues to link. If you leave it blank, no link will be made.
So what do we do with all this JIRA Data?

- Improve situational awareness
- Visualize our JIRA activity
- Improve our development process
- Answer questions
Bob in accounting was infected by `<insert-threat-of-the-day-here>`, who else was infected?
Anyone heard of Wannacry?

- 14 separate JIRA Stories
- 3 new Correlation Searches
- 6 Research Stories
- 2 Tuning Requests
- 3 Stories for Follow-up/Remediation
What does our security coverage look like, from a use-case perspective?
Deployed Use-Case Visibility
Searches!
Note: <insertyourdatahere>

SA Visualization Dashboard

• Enabled Correlation Search Breakdown by Team
  • |rest /services/alerts/correlationsearches splunk_server=local | rename eai:acl:app as application, title as csearch_name | join type=outer app csearch_name | join type=outer app csearch_name | search status=Enabled | eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, ",") | designation = mvindex(splitdes, 0) | table designation security_domain, rule_title, csearch_name, description, severity, csearch, disabled, status | stats count by designation | sort –count

• Enabled Correlation Search Breakdown by Severity
  • |rest /services/alerts/correlationsearches splunk_server=local | search rule_title!="" | rename eai:acl:app as application, title as csearch_name | join type=outer app csearch_name | search status=Enabled | eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, ",") | designation = mvindex(splitdes, 0) | table designation security_domain, rule_title, csearch_name, description, severity, csearch, disabled, status | eval Severity=case(severity=="critical","1-critical","1"), severity=="high","2-high", severity=="medium","3-medium", severity=="low","4-low", severity=="informational","5-informational") | stats count by Severity
SA Visualization Dashboard (cont.)

- Use Case Count by Team / Severity
  ```bash
  |rest /services/alerts/correlationsearches splunk_server=local | rename eai:acl:app as application, title as csearch_name | join type=outer app csearch_name |rest /services/saved/searches| rename eai:acl:app as application, title as csearch_name, search as csearch|table app, csearch_name, search, disabled|eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, ",") | split(rule_title, ",") | table designation rule_title description, severity, status | eval Severity=case(severity=="critical","1-critical", severity=="high" ",2-high", severity=="medium","3-medium", severity=="low","4-low", severity=="informational","5-informational") | chart count as "Rule Count" by designation, Severity
  ```

- Changes in Triggered Notable Events - Past 30 Days - by Correlation Search
  ```bash
  `notable` | search search eventtype!=notable_suppression* | bin _time span=24h | stats count by _time, search_name | streamstats window=2 global=f current=t first(count) as previous by search_name | eval delta=count-previous | eval time=_time | table search_name, time, delta, count
  ```

- Enabled Use Case – Details
  ```bash
  `rule_title=""` | search search eventtype!=notable_suppression* | bin _time span=24h | stats count by _time, search_name | streamstats window=2 global=f current=t first(count) as previous by search_name | eval delta=count-previous | eval time=_time | table search_name, time, delta, count
  ```
SA Visualization Dashboard (cont.)

• Correlation Search Performance
  
  ```
  index=_internal host=<yourSHhost> source="*scheduler.log app="" savedsearch_name="" (app=DA-* OR app=SA-*)
  (savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname>) | eval run_time=run_time/60 | stats min(run_time) as "Min runtime (min)", avg(run_time) as avg_runtime, max(run_time) as max_runtime, count(eval(status!="continued")) AS total_exec, count(eval(status=="success")) as "Successful executions", count(eval(status=="skipped")) AS "Skipped executions" by app, savedsearch_name, user host | stats first(*) as * by savedsearch_name | eval interval_usage_ratio=round((median_runtime/schedule_period),2) | search total_exec>0 | rename savedsearch_name AS Rule_name app AS App avg_runtime AS "Avg runtime (min)" max_runtime AS "Max runtime (min)" user AS User total_exec AS "Total executions" | table Rule_name "Min runtime (min)" "Avg runtime (min)" "Max runtime (min)" "Total executions" "Successful executions" "Skipped executions" | sort -"Avg runtime (min)" "Total executions" "Successful executions" "Skipped executions" | join Rule_name [] rest splunk_server=* /servicesNS/-/-/admin/savedsearch/ earliest_time=0s latest_time=+2d@d search="is_scheduled=1" search="disabled=0" search="(eai:acl.app=SA-* OR eai:acl.app=DA-*)" | dedup title| rename title AS Rule_name dispatch.earliest_time dispatch.latest_time AS earliest_time dispatch.latest_time|table Rule_name cron_schedule earliest_time latest_time|sort SkipCount| rename savedsearch_name AS "Scheduled search name" count AS "Skip count" host AS Server | fieldformat scheduled_time=strftime(scheduled_time, "%c") | fieldformat _time=strftime(_time, "%c")
  ```

• Skipped Correlation Searches
  
  ```
  index=_internal host=<yourSHhost> source="*scheduler.log savedsplunker status=skipped (app=SA-* OR app=DA-*)
  (savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname>) | stats count values(scheduled_time) as scheduled_time values(_time) as _time by host savedsearch_name, app | sort -SkipCount | rename savedsearch_name AS "Scheduled search name" count AS "Skip count" host AS Server | fieldformat scheduled_time=strftime(scheduled_time, "%c") | fieldformat _time=strftime(_time, "%c")
  ```
How are we tracking towards our high level security goals for the year?
Status Metricization

Used to show completeness of status regardless of velocity in a given Scrum related to Epic that have heretofore been unaccomplished but are tied to the current Sprint.

**12.17 %**

Completion Percentage History

**Should we develop this incredibly well designed use-case?**

*no*

**Excessive Extraneous Authentication Trend**

596,713 number of things - 209,501
Metricization Dashboard

- Percent Completometer
  - `index=<yourindex> sourcetype=<yoursourcetype> | head 5000 | search bytes<9801 | head 1 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | fields percent`

- CompleteTruthiness
  - `index=<yourindex> sourcetype=<yoursourcetype> | head 110 | search bytes<9801 | tail 1 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | fields percentCompleteNumber ofindex=* | head 1 | eval sourcetype=0 | table sourcetype`

- Visualization of Velocity of Completeness
  - `index=<yourindex> sourcetype=<yoursourcetype> | head 100 | search bytes<9801 | head 1 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | fields percentComplete`

- Completion Percentage History
  - `index=<yourindex> sourcetype=<yoursourcetype> | head 10000 | search bytes<9801 bytes>4 | head 7 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | rename bytes as "Timechart Histor-o-meter"`

Searches!
Note: <insertyourdatahere>
Metricization Dashboard (cont.)

- Should we develop this incredibly well designed use-case?
  - index=<yourindex> | stats count | eval countresult=if(count=5,"no","yes") | rename countresult AS value | table value count

- Completion Percentage History
  - index=<yourindex> sourcetype=<yoursourcetype> | head 10000 | search bytes<9801 bytes>4 | head 7 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | rename bytes as "Timechart Histor-o-meter"

- Excessive Extraneous Authentication Trend
  - | tstats prestats=t count where index=<yourindex> sourcetype=<yoursourcetype> by _time span=1d | timechart count

Searches!
Note: <insertyourdatahere>
JIRA Epic Tracking
Searches!
Note: <insertyourdatahere>

- **JIRA Epic Tracking**
  - Stories Completed By Epic 2017
    - `jira issues <issue filter> | join type=left "Epic Link" [jira issues 10412 | rename Key AS "Epic Link" | fields "Epic Link" "Epic Name"] | stats count(Key) AS "Story Count" by "Epic Name"`
  - Story Summaries by Epic
    - `jira issues <issue filter> | stats count(Key) AS "Story Count" values(Key) AS "Story ID" values(Summary) AS Summary by "Epic Link" | join type=left "Epic Link" [jira issues 10412 | rename Key AS "Epic Link" | fields "Epic Link" "Epic Name"] | table "Epic Link" "Epic Name" "Story Count" "Story ID" Summary`
What does your development team do all day?
In General, This Is What We Do...
This Is What We’re Doing Right Now

![Demo SA JIRA Current Sprint Dashboard](image-url)
Searches!
Note: <insertyourdatahere>

- JIRA Current Sprint Dashboard
  - Current Sprint Stories Resolved
    - | jira issues <current sprint filter> | search Resolved!=null | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\"" | table Key Summary "TL; DR" Assignee_Name
  - Current sprint stories in progress
    - | jira issues <current sprint filter> | search Resolved=null | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\"" | table Key Summary "TL; DR" Assignee_Name
  - Closed in the last 24h - for morning call
    - | jira issues <current sprint filter> | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\"" | table Key Summary "TL; DR" Assignee_Name
  - Story points available
    - | jira issues <current sprint filter> | stats sum("Story Points") AS value | eval value=rnd(value,0)
  - Story points completed
    - | jira issues <current sprint filter> | search Resolved!=null | stats sum("Story Points") AS value | eval value=round(value,0)
  - Story points remaining
    - | jira issues <current sprint filter> | search Resolved=null | stats sum("Story Points") AS value | eval value=round(value,0)
Searches!
Note: <insertyourdatahere>

JIRA Current Sprint Dashboard

- Current Sprint Stories Resolved
  - | jira issues <current sprint filter> | search Resolved!=null | rex field=Assignee "\"displayName\": "(?<Assignee_Name>\w+\s+)" | table Key Summary "TL; DR" Assignee_Name

- current sprint stories in progress
  - | jira issues <current sprint filter> | search Resolved=null | rex field=Assignee "\"displayName\": "(?<Assignee_Name>\w+\s+)" | table Key Summary "TL; DR" Assignee_Name

- closed in the last 24h - for morning call
  - | jira issues <current sprint filter> | rex field=Assignee "\"displayName\": "(?<Assignee_Name>\w+\s+)" | table Key Summary "TL; DR" Assignee_Name

- story points available
  - | jira issues <current sprint filter> | stats sum("Story Points") AS value | eval value=round(value,0)

- story points completed
  - | jira issues <current sprint filter> | search Resolved!=null | stats sum("Story Points") AS value | eval value=round(value,0)

- story points remaining
  - | jira issues <current sprint filter> | search Resolved=null | stats sum("Story Points") AS value | eval value=round(value,0)
## Sprint Review/Monthly Demo

<table>
<thead>
<tr>
<th>Key</th>
<th>Summary</th>
<th>Assignee</th>
<th>Status</th>
<th>CRDC Tag</th>
<th>Story Points</th>
<th>Sprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case DBIR Present Coverage Evaluation 2017</td>
<td>Approved</td>
<td>SA, demo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AttackIP Long Duration Connection</td>
<td>Approved</td>
<td>SA, demo, es</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TV team test</td>
<td>Approved</td>
<td>SA, TV, demo, ttest</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AttackIP Successful Authentication</td>
<td>Approved</td>
<td>SA, demo, es</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TV team test</td>
<td>Approved</td>
<td>SA, TV, demo, ttest</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing xxxxxx Unknown TCP Traffic - High Volume Outbound</td>
<td>Approved</td>
<td>SA, TV, demo, ttest</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research: Long domain activity similar to the Wannacy sandbox domains</td>
<td>Approved</td>
<td>SA, demo, wannacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Correlation Search xxxxxx-WannaCry Ransomware-AV Infection</td>
<td>Approved</td>
<td>LM, SA, demo, es, ransomware, wannacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrade - Enterprise Security from xxxxx to xxxxx</td>
<td>Approved</td>
<td>OPS, SA, demo, es</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious external connection from PCI devices</td>
<td>Approved</td>
<td>SA, demo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a new Windows event logs dashboard</td>
<td>Approved</td>
<td>SA, demo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recap

- Gave you tips on how you can build a flexible content development process
- Shared with you a real-world example of how this flexible process works in practice
- Provided you with dashboards and searches that will improve visibility of your security posture, high-level goal tracking and content dev capacity
What will we do in the next 12 months?
What can you do in the next 12 months?

- Identify the key metadata in your currently deployed use-cases
- Listen to your dev team. Examine your current dev process and improve on the challenges identified by your team
- When building your process, work towards a minimum viable product (MVP)
96%
Do or do not, there is no try.

- Abraham Lincoln
Links!

▶ KP Career Site
  • https://www.kaiserpermanentejobs.org/

▶ Scrum Alliance
  • https://www.scrumalliance.org/

▶ Great Video on Thought Leadership
  • https://www.youtube.com/watch?v=_ZBKX-6Gz6A&sns=em

▶ Splunk App for Jira
  • https://splunkbase.splunk.com/app/1438/

▶ JIRA and Confluence Info
  • https://www.atlassian.com/
Questions?