“Explosions In The Sky”

Building Splunk ‘Cloud First’ On Our Journey To A ‘Lean’ SOC

Nick Bleech

Head of Information Security, Travis Perkins

.conf2016

splunk>

Agenda

- Introduction
- Beginning – SIEM ‘Mark One’
- Csfs For SIEM ‘Mark Two’
- Csfs For ‘Lean’ SOC
- Operating Model
- Monitoring Architecture
- Productionization
- Benefits We’ve Realized And Future Roadmap

Travis Perkins: ‘Bricks & Mortar - And More’

- Travis Perkins plc is the UK's largest product supplier to the building, construction, and home improvement markets
- We’re a group of 20+ businesses, some of the UK building industry’s most popular brands and businesses that span distribution to the trade, building supply chain, and consumer ‘Do-It-Yourself’ markets
- We have over 27,000 colleagues working with us, each of whom are proud members of their local communities

Travis Perkins

Travis Perkins: ‘Bricks & Mortar - And More’

- We sell and distribute building materials and tools in many different forms. In 2015 our earnings exceeded £5.9bn. See www.travisperkinsplc.com for further information

- We have an exciting team dedicated to exploring innovation within the world of construction

- Super-strength workwear, bacteria-grown bricks, nanotechnology paint, 3D printed buildings and self-healing concrete and pipes are just some examples of what the future of our industry may look like

Travis Perkins

Speaker - Nick Bleech

- I’m currently CISO for the Travis Perkins Group
- The UK's largest Building Materials Group
- I started in IT Security technology R&D in 1985
- Moved on to security management and architect roles in Aerospace, Government, Financial Services & Consulting
- Before Travis Perkins I was the CISO at Rolls-Royce plc
  - Served on the board of the Jericho Forum
  - Expert group which established core principles for ‘Cloud’ Security

Speaker - Nick Bleech

- My team at Travis Perkins tackles practical challenges including:
  - Security Monitoring
  - Incident Response
  - Driving the governance to tackle Cloud Computing
  - Data Security
  - Internet of Things
  - Agile Development practices
  - Information System Lifecycle security risks
- Team member Gary Richardson is our Splunk Architect and Lead Analyst

Introduction – Travis Perkins Challenges

- Complex IT, mix of on-premise legacy systems/services and the cloud services progressively replacing them
- ‘Cloud First’ i.e. all new solutions must deploy into Cloud and interwork with on-premise as needed
- This meant rolling Splunk out in the Cloud then extending back to on-premise rather than the other way round (although our technical pilot/ PoV was on-premise)

Introduction – Travis Perkins Challenges

- Need to be able to adapt data source interfaces at low cost / complexity using open source
- Many parallel IT change / new build projects in flight - e-com, ERP, supply chain etc.
- SIEM Business drivers balanced between Incidents, Investigations, and Compliance use-cases - need flexible and adaptable technology
- No pre-existing internal or external 'SOC', no preference to engage a Managed Security Services Provider due to velocity of change and aim to grow in-house expertise

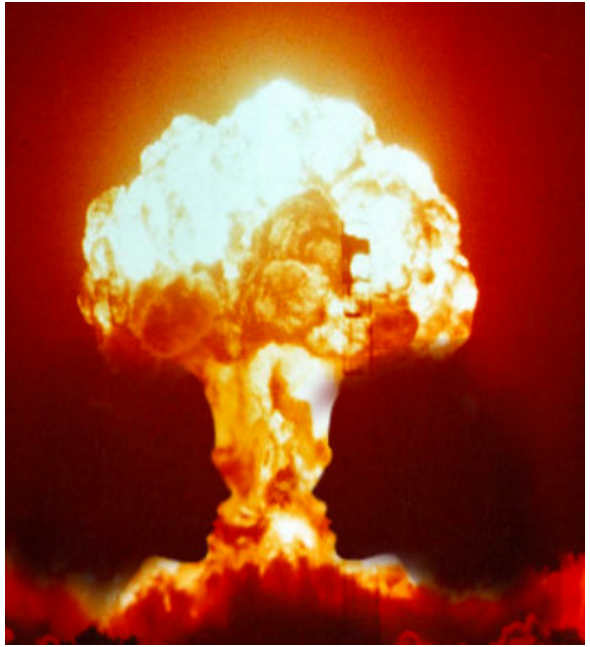
The Beginning

SIEM ‘mark one’ that was tagged **‘never again’**

- The ‘Big Bang’:

- Acquire SIEM hardware & software – one size fits all - ($$$$$)
- Connect as many sources as possible (Look Ma - all those connectors!)
- No data source is too large or too complex
- When budget/time/resources run out:

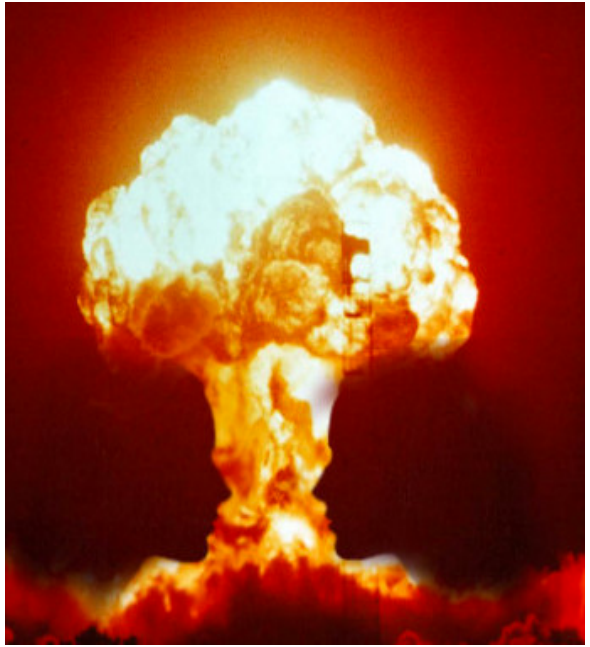
Oh dear...stop!



The Beginning

Lessons learnt – **the hard way**

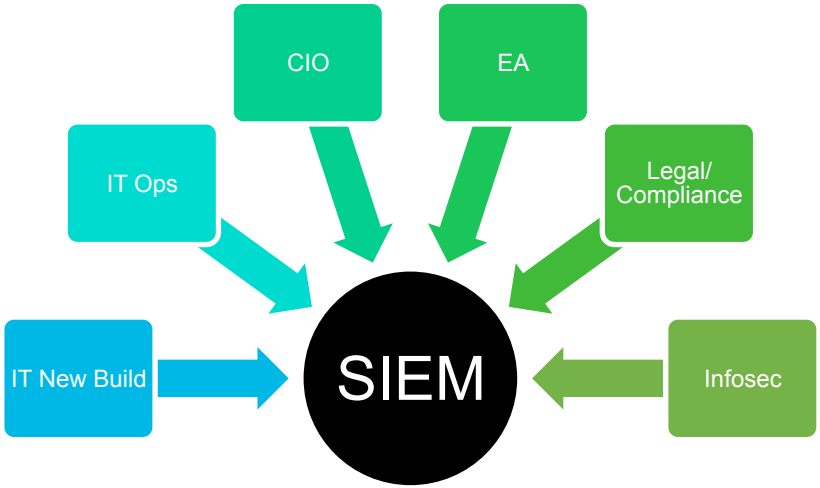
- Must show early cost/benefit to retain stakeholder buy-in
- Need service integration architecture - not just SIEM infrastructure
- No long term strategy initiated/developed
- SIEM projects very similar to Data Warehouse & Business Intelligence app projects
- This experience gave other security improvement projects a bad name!



Worst of all… CISO was replaced!

Critical Success Factors For SIEM ‘Mark Two’

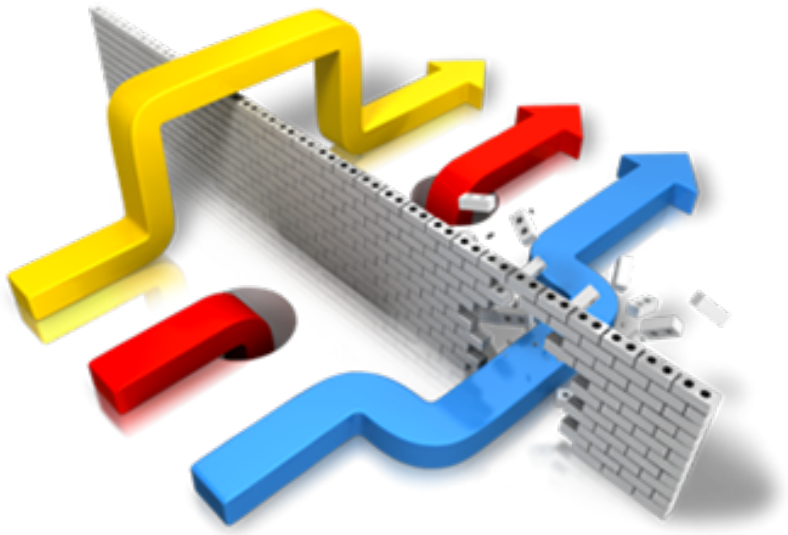
- Plan/Deliver incrementally - no ‘big bang’
- Grow ‘Lean’ SOC: Develop clear roles for IT Ops Service Ops vs. Infosec forensics
- Design Op team alerting carefully for maximum effectiveness
- Monitoring architecture to include both ‘agent-based’ & ‘agentless’ data collection
- Acknowledge and meet multiple stakeholder needs



Critical Success Factors For ‘Lean’ SOC

Plan/Deliver incrementally:

- Roll out the most effective handling/ response process to cover most likely scenario
- Train teams on new process, tune data source and Splunk correlation searches
- ‘Rinse - Wash - Repeat’



Critical Success Factors For ‘Lean’ SOC

Develop clear roles for IT Ops Service Ops vs. Infosec forensics teams:

- IT Ops catch, gather info, dispatch for further investigation/remediation
- Infosec forensics have specialist skills including Splunk training
- Enable follow up detailed investigation post initial response

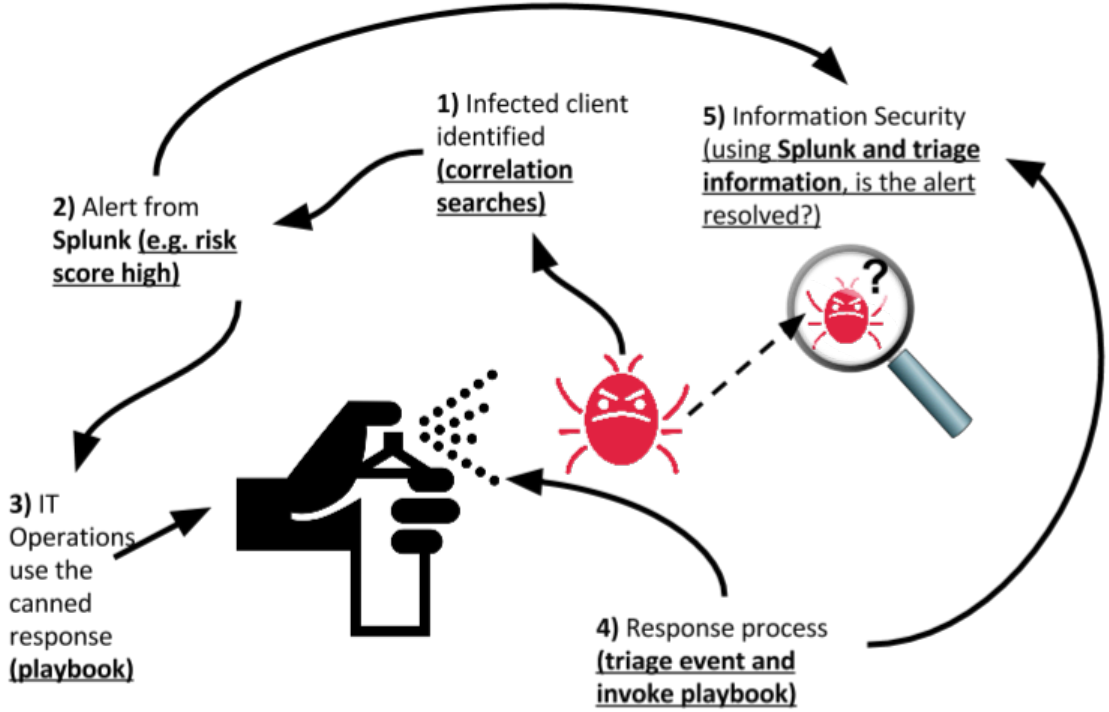
Critical Success Factors For ‘Lean’ SOC

Design Op team alerting carefully for maximum effectiveness without detailed knowledge of Splunk or other tools

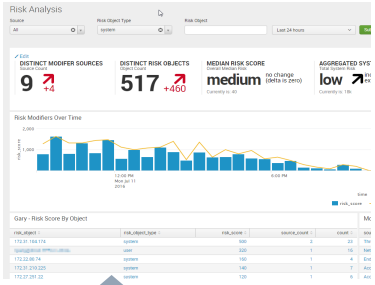
- Use Splunk/ES risk scoring appropriately
- An alert can be like a finger on a spray can: a little alert can trigger a lot of response if you put the right stuff in the can...

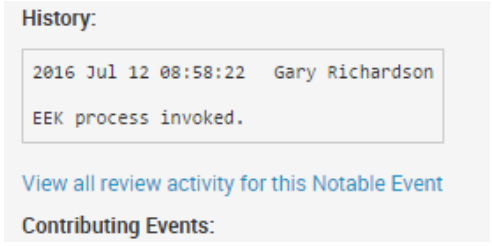
Operating Model

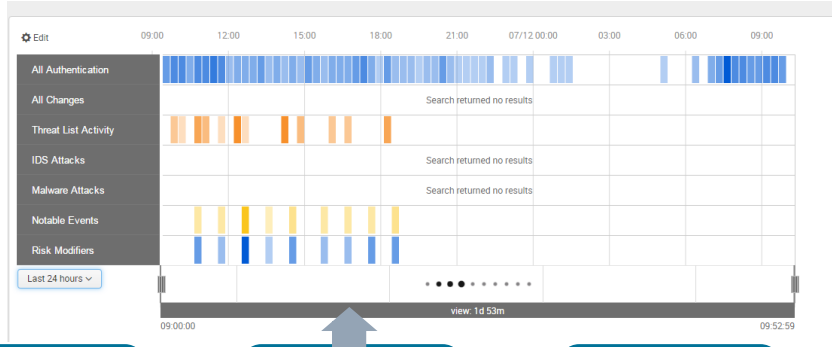
Canned alerts are 80% effective in the first instance, and always provide value by gathering some additional information



Splunk Response Process







Risk score triggers alert for target

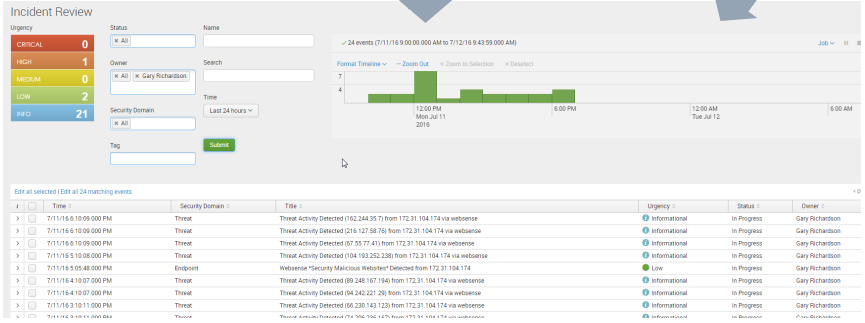
OPs team responds, gathers info, claims notable events & updates them with info

OPs team creates incidents for automated in-depth malware scans an/or automated forensics, updates events

OPs team submits any binary samples from target to enterprise AV vendor, requests AC scan & cleanup

Infosec confirm using Splunk & data collected by Ops that target is clean.

If target is not clean, IS can request rebuild or access to target for more forensics



Notes

1. Integration with ServiceNow is planned
2. Process is Pareto-inspired: 80% of events can be handled by this process, on 80% of the infrastructure (Windows, server/client) and resolved at least 80% effective in the first instance
3. For events which OPs cannot resolve (no skills, no access) they can always add value by collecting information about the target

Risk Analysis

Source: All | Risk Object Type: system | Risk Object: | Last 24 hours | Sub

Edit

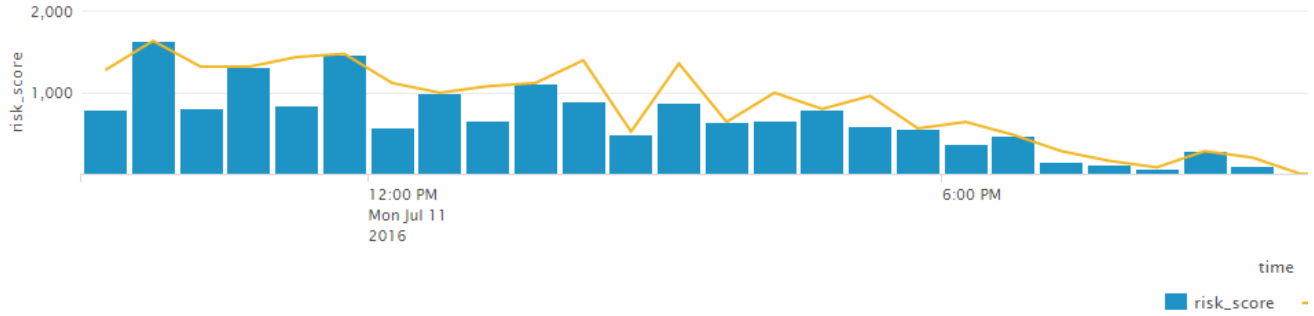
DISTINCT MODIFER SOURCES
Source Count
9 +4

DISTINCT RISK OBJECTS
Object Count
517 +460

MEDIAN RISK SCORE
Overall Median Risk
medium (no change (delta is zero))
Currently is: 40

AGGREGATED SYS
Total System Risk
low inc ex
Currently is: 18k

Risk Modifiers Over Time



Gary - Risk Score By Object

risk_object	risk_object_type	risk_score	source_count	count
172.31.104.174	system	500	2	23
[redacted]	user	320	1	16
172.22.80.74	system	160	1	4
172.31.210.225	system	140	1	7
172.27.251.22	system	120	1	6

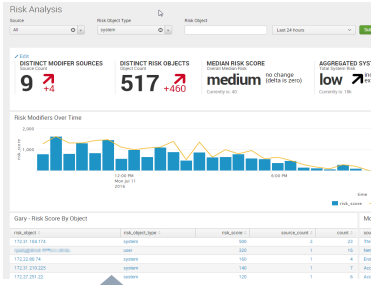
History:

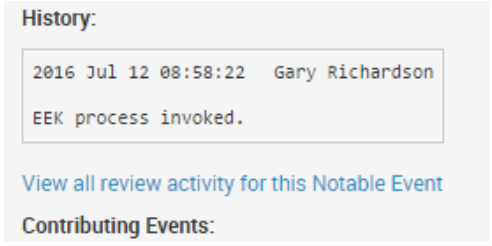
```
2016 Jul 12 08:58:22   Gary Richardson

EEK process invoked.
```

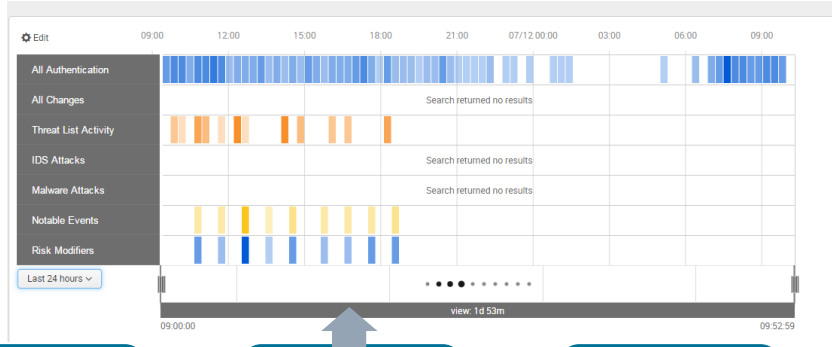
View all review activity for this Notable Event

Contributing Events:

Splunk Response Process







Risk score triggers alert for target

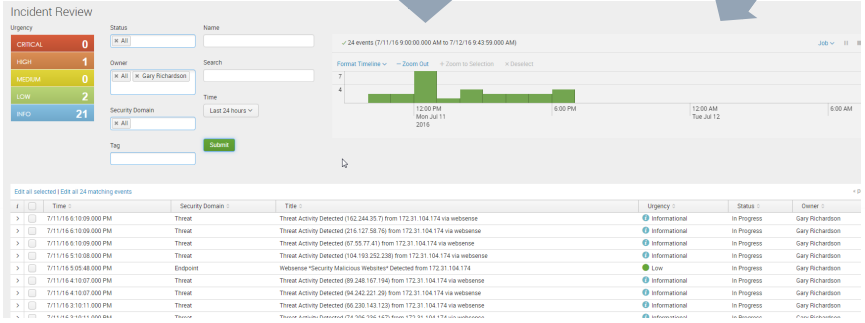
OPs team responds, gathers info, claims notable events & updates them with info

OPs team creates incidents for automated in-depth malware scans an/or automated forensics, updates events

OPs team submits any binary samples from target to enterprise AV vendor, requests AC scan & cleanup

Infosec confirm using Splunk & data collected by Ops that target is clean.

If target is not clean, IS can request rebuild or access to target for more forensics



Notes

1. Integration with ServiceNow is planned
2. Process is Pareto-inspired: 80% of events can be handled by this process, on 80% of the infrastructure (Windows, server/client) and resolved at least 80% effective in the first instance
3. For events which OPs cannot resolve (no skills, no access) they can always add value by collecting information about the target

Incident Review

Urgency

CRITICAL	0
HIGH	1
MEDIUM	0
LOW	2
INFO	21

Status: × All

Owner: × All × Gary Richardson

Security Domain: × All

Tag

Name

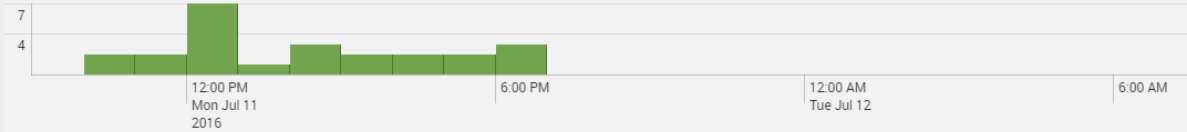
Search

Time: Last 24 hours

Submit

✓ 24 events (7/11/16 9:00:00.000 AM to 7/12/16 9:43:59.000 AM) Job

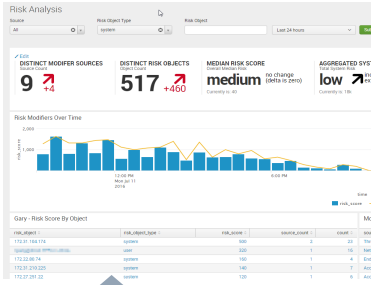
Format Timeline – Zoom Out + Zoom to Selection × Deselect

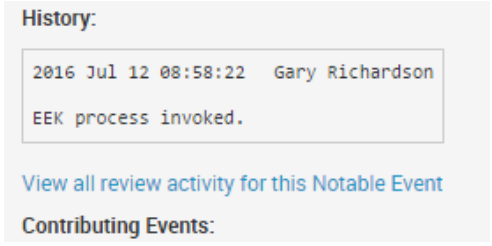


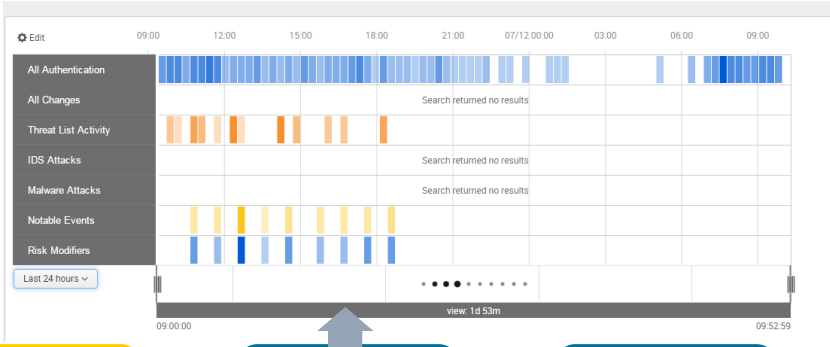
Edit all selected | Edit all 24 matching events

i	Time	Security Domain	Title	Urgency	Status	Owner
>	7/11/16 6:10:09.000 PM	Threat	Threat Activity Detected (162.244.35.7) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 6:10:09.000 PM	Threat	Threat Activity Detected (216.127.58.76) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 6:10:09.000 PM	Threat	Threat Activity Detected (67.55.77.41) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 5:10:08.000 PM	Threat	Threat Activity Detected (104.193.252.238) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 5:05:48.000 PM	Endpoint	Websense *Security Malicious Websites* Detected from 172.31.104.174	Low	In Progress	Gary Richardson
>	7/11/16 4:10:07.000 PM	Threat	Threat Activity Detected (89.248.167.194) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 4:10:07.000 PM	Threat	Threat Activity Detected (94.242.221.29) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 3:10:11.000 PM	Threat	Threat Activity Detected (66.230.143.123) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson
>	7/11/16 3:10:11.000 PM	Threat	Threat Activity Detected (74.206.236.167) from 172.31.104.174 via websense	Informational	In Progress	Gary Richardson

Splunk Response Process







Risk score triggers alert for target

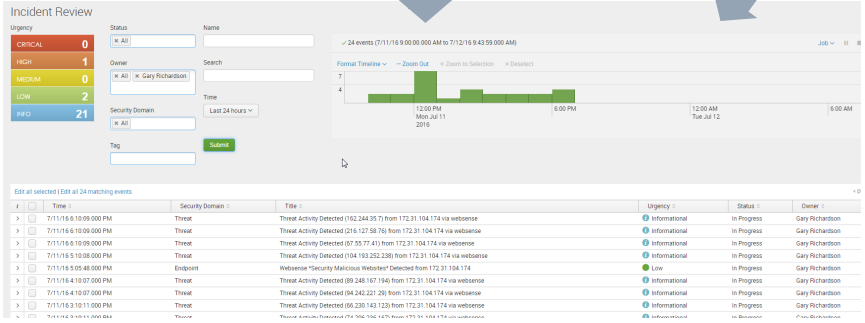
OPs team responds, gathers info, claims notable events & updates them with info

OPs team creates incidents for automated in-depth malware scans an/or automated forensics, updates events

OPs team submits any binary samples from target to enterprise AV vendor, requests AC scan & cleanup

Infosec confirm using Splunk & data collected by Ops that target is clean.

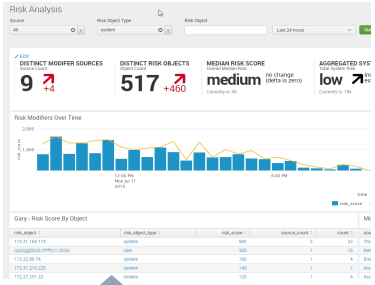
If target is not clean, IS can request rebuild or access to target for more forensics

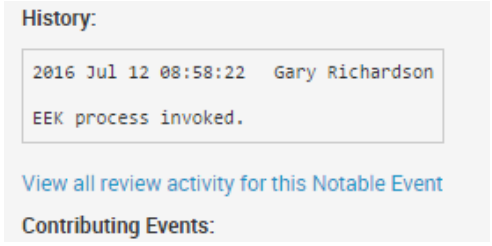


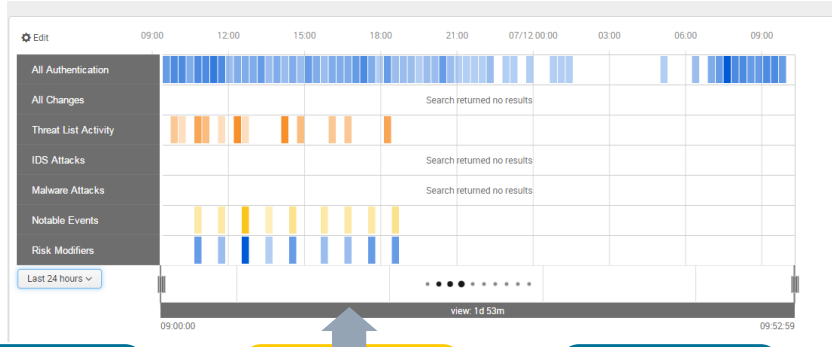
Notes

1. Integration with ServiceNow is planned
2. Process is Pareto-inspired: 80% of events can be handled by this process, on 80% of the infrastructure (Windows, server/client) and resolved at least 80% effective in the first instance
3. For events which OPs cannot resolve (no skills, no access) they can always add value by collecting information about the target

Splunk Response Process







Risk score triggers alert for target

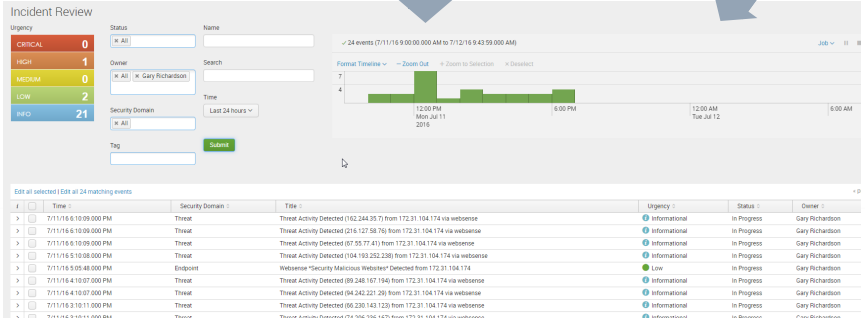
OPs team responds, gathers info, claims notable events & updates them with info

OPs team creates incidents for automated in-depth malware scans an/or automated forensics, updates events

OPs team submits any binary samples from target to enterprise AV vendor, requests AC scan & cleanup

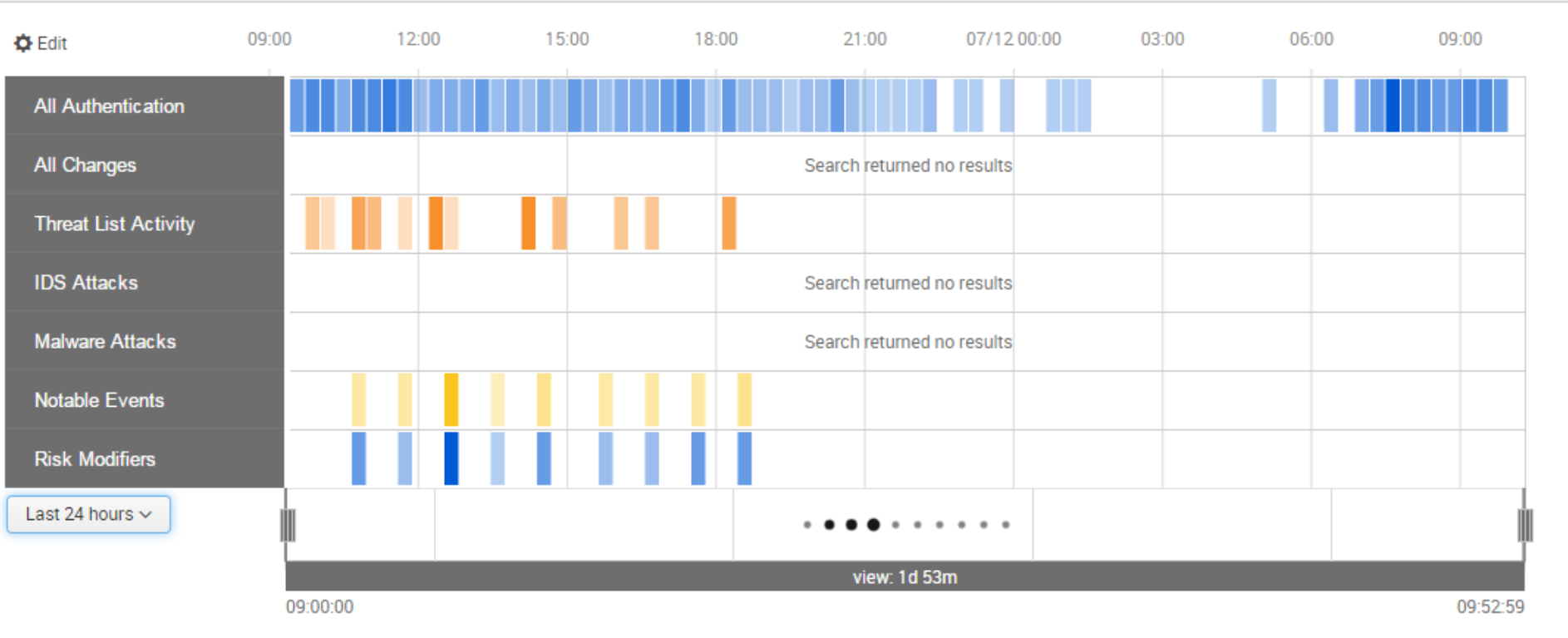
Infosec confirm using Splunk & data collected by Ops that target is clean.

If target is not clean, IS can request rebuild or access to target for more forensics

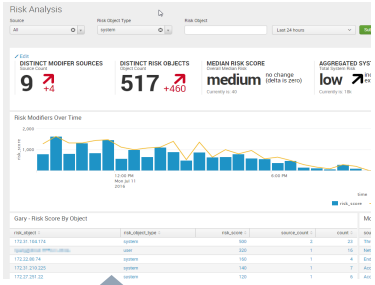


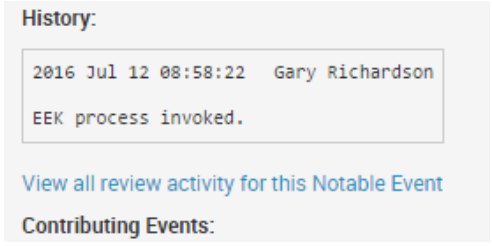
Notes

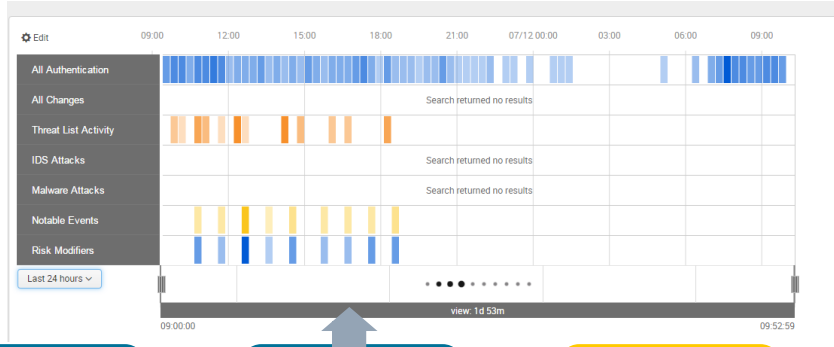
1. Integration with ServiceNow is planned
2. Process is Pareto-inspired: 80% of events can be handled by this process, on 80% of the infrastructure (Windows, server/client) and resolved at least 80% effective in the first instance
3. For events which OPs cannot resolve (no skills, no access) they can always add value by collecting information about the target


Edit
09:00
12:00
15:00
18:00
21:00
07/12 00:00
03:00
06:00
09:00
All Authentication
All Changes
Search returned no results
Threat List Activity
IDS Attacks
Search returned no results
Malware Attacks
Search returned no results
Notable Events
Risk Modifiers
Last 24 hours
view: 1d 53m
09:00:00
09:52:59

Splunk Response Process







Risk score triggers alert for target

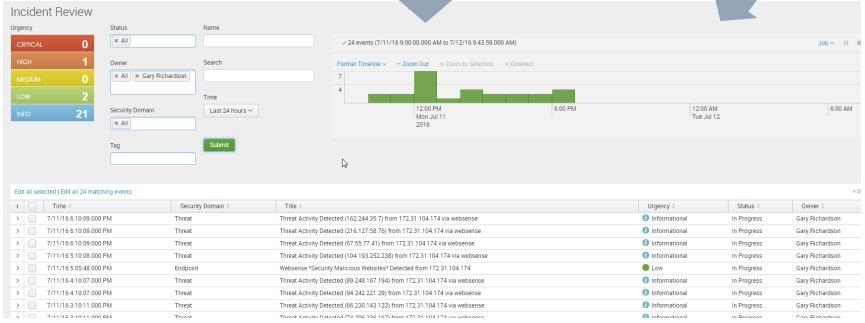
OPs team responds, gathers info, claims notable events & updates them with info

OPs team creates incidents for automated in-depth malware scans an/or automated forensics, updates events

OPs team submits any binary samples from target to enterprise AV vendor, requests AC scan & cleanup

Infosec confirm using Splunk & data collected by Ops that target is clean.

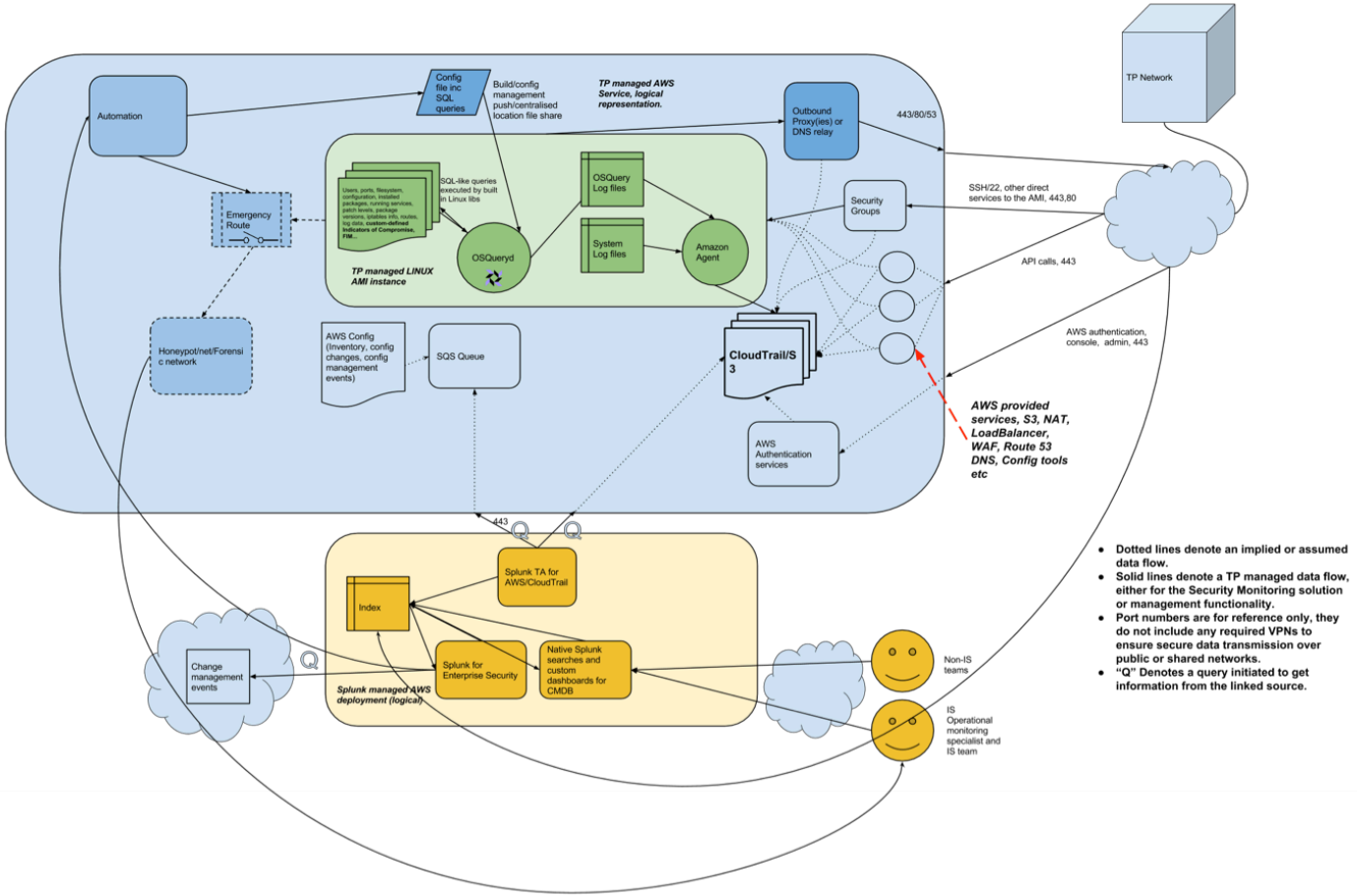
If target is not clean, IS can request rebuild or access to target for more forensics



Notes

1. Integration with ServiceNow is planned
2. Process is Pareto-inspired: 80% of events can be handled by this process, on 80% of the infrastructure (Windows, server/client) and resolved at least 80% effective in the first instance
3. For events which OPs cannot resolve (no skills, no access) they can always add value by collecting information about the target

AWS Monitoring Architecture



Monitoring Architecture (1)

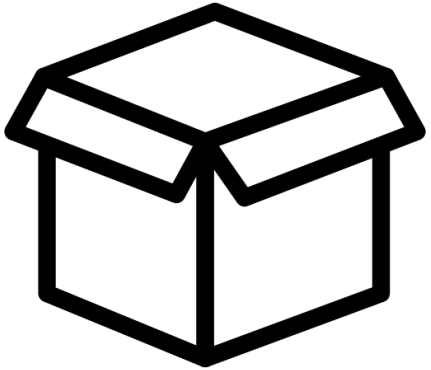
- Allow for both ‘agent-based’ & ‘agentless’ data collection to trade off:
  - Performance, data volumes, server/network impacts and ‘IT politics’!
- Standard Splunk data source integration methods:
  - Cloud / “as a service” products e.g. ServiceNow and FireEye ETP publish APIs, which can be accessed using Splunk apps or Splunk RESTful API data source configurator
  - Excellent AWS app enables both collection of AWS native log data (AWS Auth etc) and ingestion / indexing of application data from AWS S3 buckets
  - Standard Splunk Forwarder sends on prem data to Splunk Cloud

Monitoring Architecture (2)

- Open source data integration: Highly scalable and performant, **OSQuery** for host based IDS and FIM (PCI compliant) across whole AWS estate
  - No central server required (as would be the case for OSSEC)
  - Easy to deploy in 'continuous integration' automated pipelines
- Although OSQuery output not Splunk Common Information Model compliant, Splunk immediately understands its json format data
- Enables meaningful correlation searches to be written once data is indexed
- We are free to choose where we parse out meaningful source data for each use case - in OSQ or in Splunk - or both

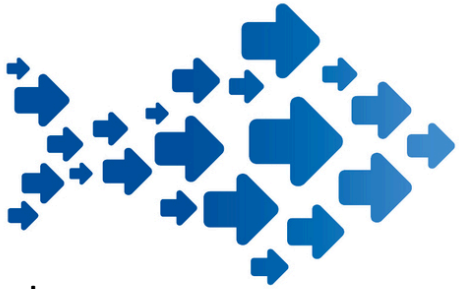
Productionization

- We ran an on prem pilot / proof of value using “found” hardware
  - Bore an uncanny resemblance to hardware from our previous SIEM…
- We got a working solution, but speed, storage, and reliability issues arose
- Analysts not good SysAdmins - so get better not minding infrastructure
- Per our Cloud First strategy, we considered two options:
  - host within our own AWS VPCs, or
  - purchase the Splunk Cloud SaaS
  - In terms of cost/benefit, Splunk Cloud option came out ahead
- Migration took 2 days to get basic functionality up and running



Benefits Obtained And Future Roadmap

- Quicker from ingesting new data to creating meaningful correlation searches
- We were used to having console access to edit .conf files on-prem; but fewer concerns now Splunk Cloud increasing functionality in the GUI
- Splunk CloudOps are taking pain out of managing host infrastructure
- Intrinsic risk-score based correlation in Slunk/ES has been pivotal in several security incidents
- Our architecture and approach now serve as blueprint for IT Ops and App support teams to leverage Splunk for non-security event/log monitoring



THANK YOU

splunk>