.conf2014

YOUR DATA ADVENTURE

The Analytics-Enabled SOC > SIEM Use Cases

Fred Wilmot (CISSP)

Director, Global Security Practice

Sanford Owings

Principle Consultant, Splunk Services

splunk>

Disclaimer

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 the 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.

Fred Wilmot | Director, Global Security Practice

(fred|Securityczar)@splunk.com

Minister of Silly Walks
"Electric Mayhem"
@fewdisc

- Strategy
  - Drives Security Practice Strategy globally
  - Works on Splunk's hardest Security Use Cases
  - Visualization and Analytics using Splunk
  - Solves strategic product/implementation challenges
- Research
  - Digital Forensics /Assessment Tools
  - Social Risk/User behavior modeling
  - ML/Advanced Statistical Analysis
  - Threat Intelligence
- Product
  - Influence product strategy for security content and features in the field and through the factory.

Sanford Owings| Principal Consultant, Splunk Services

sowings@splunk.com

sowings
(muppet disguise)

Sanford Owings (Sowings) began his computing career in 1990 in a word processing lab with network administration on PCs and various flavors of Unix. A computer science education at Berkeley (with more system and network administration thrown in) showed him the light twenty years later.

Sanford began using Splunk in early 2010, working to integrate it as an OEM reporting solution into an email appliance. Since March 2012, he has worked as a member of the Professional Services team at Splunk, leveraging his development background while assisting customers.

In his free time, he enjoys spending time with his wife Erin, cooking, cycling and traveling.

Agenda

- Why do we use SIEMs?
- How to Achieve these ‘SIEM’ use cases?
- Security Maturity Model: How do I get there?
- Where do we Start?
- Questions?
- Appendix

Why do we use SIEMS?

splunk>

Not Really…

But we may feel that way because we don't really know what problem we are solving, we don't have the right people, or process to leverage our technology.

Lack of internal knowledge leads to external guidance…

Gartner SIEM MQ 2014

"…the **rise in successful targeted attacks** has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection"

Threat Management
Real-time monitoring and reporting of user activity, data access and application activity, in combination with effective ad hoc query capabilities….

capabilities that aid in targeted attack detection"

Product/Service Rating
Real-Time Monitoring
Threat Intelligence
Behavior Profiling
Data and User Monitoring
Application Monitoring
Analytics
Log Management and Reporting
Deployment/Support Simplicity

What capabilities are you looking for from SIEM?

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Compliance	Threat Management	SIEM
Real-Time Monitoring	2.0%	18.0%	15.0%
Threat Intelligence	2.0%	9.0%	10.0%
Behavior Profiling	2.0%	10.0%	7.0%
Data and User Monitoring	10.0%	10.0%	8.0%
Application Monitoring	2.0%	10.0%	6.0%
Analytics	2.0%	23.0%	8.0%
Log Management and Reporting	55.0%	10.0%	26.0%
Deployment/Support Simplicity	25.0%	10.0%	20.0%
Total	100.0%	100.0%	100.0%

Source: Gartner (June 2014)

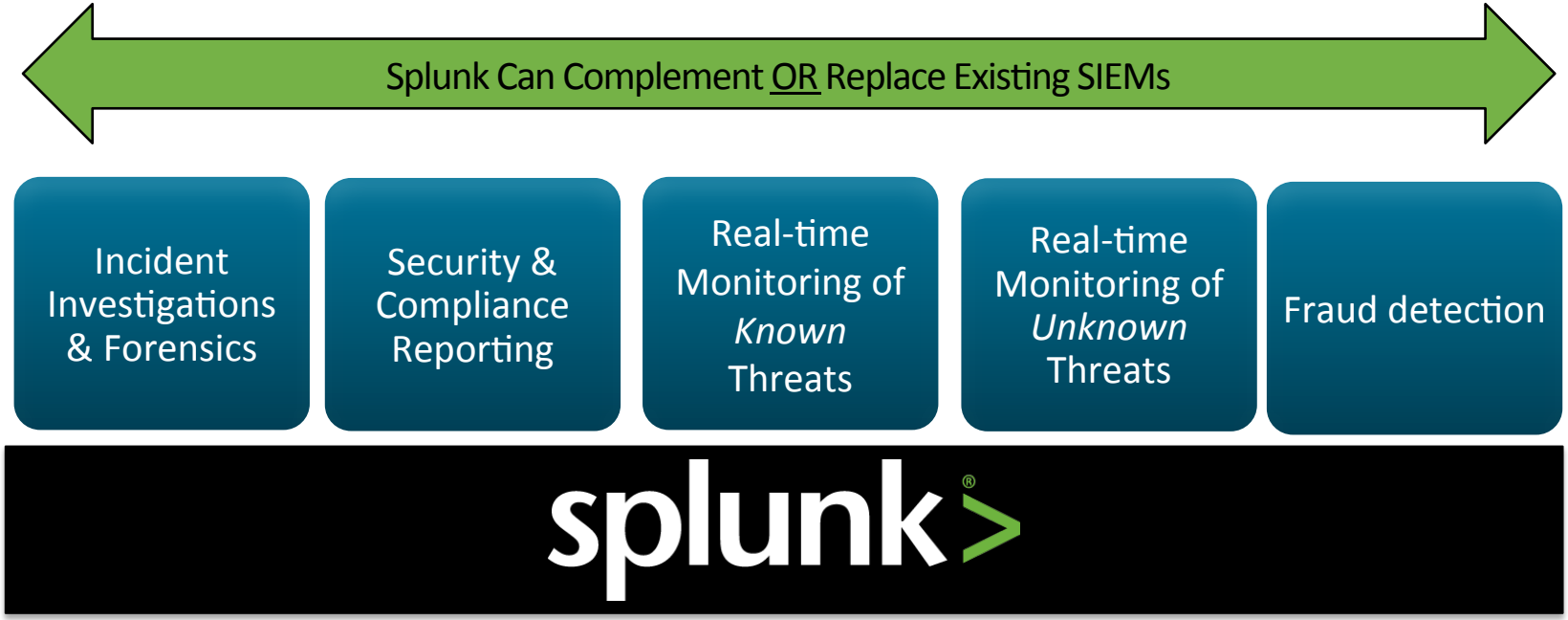
Why Splunk Compared to SIEM

	Legacy SIEM	Splunk
Data sources	Limited	Any technology, device
Custom Device Support	Difficult	Easy
Add Intelligence	Difficult	Easy
Customized Reporting	Required 3rd party App	Built-in (from search)
Speed of Search/Reporting	Slow and Unusable	Fast and Responsive
Correlation	Difficult (rule-based)	Easy (search-based)
Scalability	Limited	Extensible

Be Pragmatic, not Dogmatic. Be prepared to challenge your assertions if you want to mature your operations

Top Five Splunk Security Use Cases

More than a SIEM; a Security Intelligence Platform



Moving Past SIEM to Security Intelligence

splunk>

Small Data. Big Data. Huge Data.

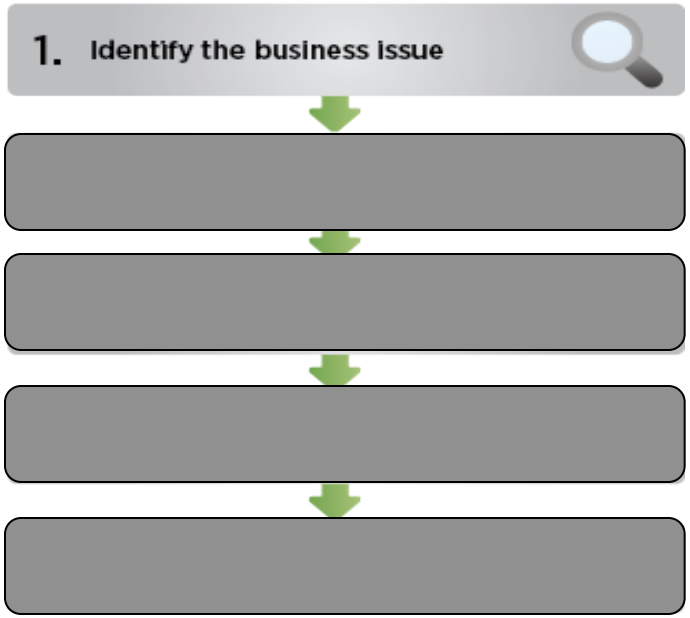
Splunk software complements, replaces and goes beyond traditional SIEMs.

How do we achieve Analytics Enabled SOC?

splunk>

A journey of a thousand miles begins with a single step. **Lao-tzu**, *The Way of Lao-tzu*

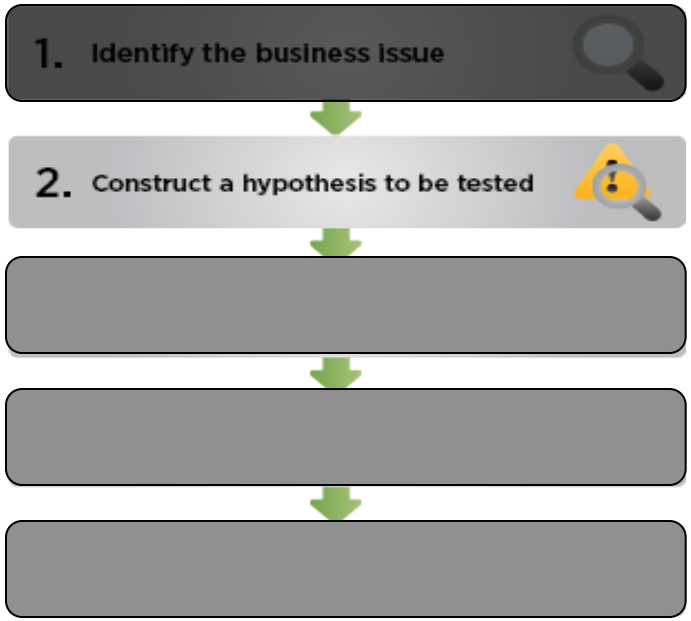
A Methodology for Analytics-Enabled SOC: Map the Business to the Threat Model



What does the business care about?

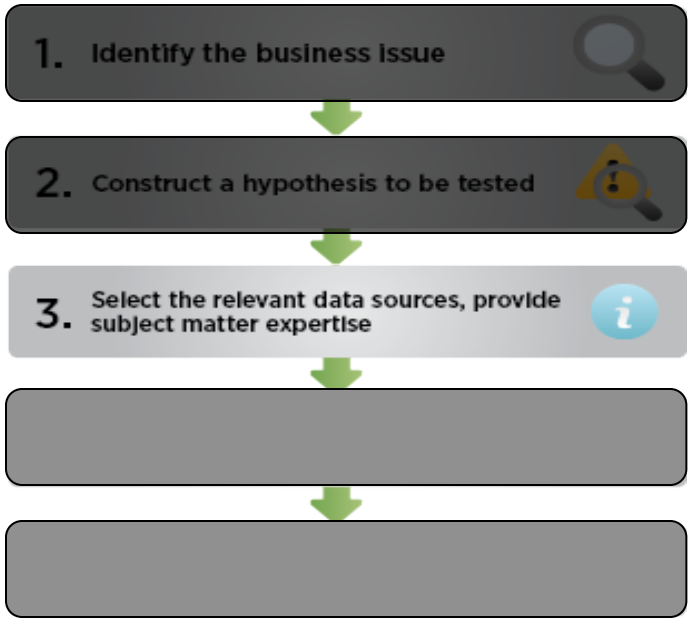
- Market Sentiment?
- Fraud?
- Denial of Service?
- Intellectual property theft?
- Sensitive data/customer data leak?
- Brand reputation?
- Industrial sabotage?
- Corporate espionage?

A Methodology for Analytics-Enabled SOC: Construct a Hypothesis



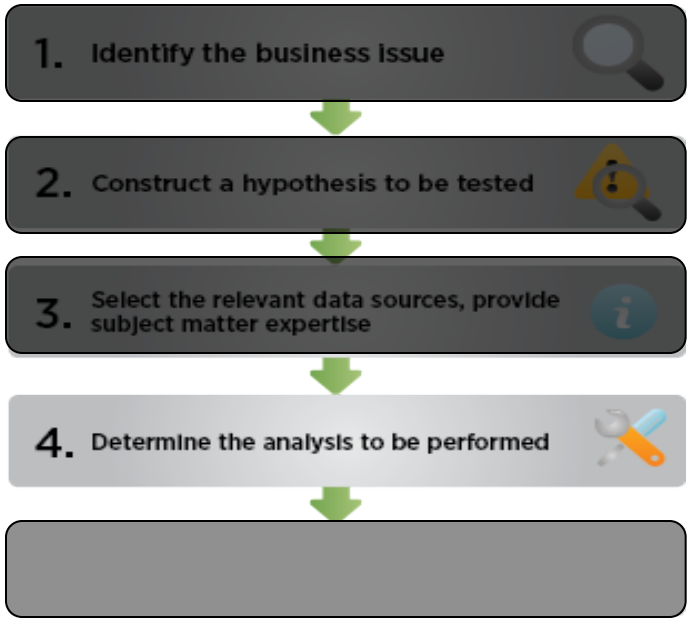
- How could someone gain access to data that should be kept private?
- What could cause a mass system outage does the business care about?
- How could we find exfiltration of sensitive information if it was happening?

A Methodology for Analytics-Enabled SOC: It's about the Data



- What visibility do we need?
- For data exfiltration, start with URLs.
- DNS requests, proxy logs, web logs, mail logs
- Beg, borrow, and steal SME expertise from system owners

A Methodology for Analytics-Enabled SOC: Data Evaluation

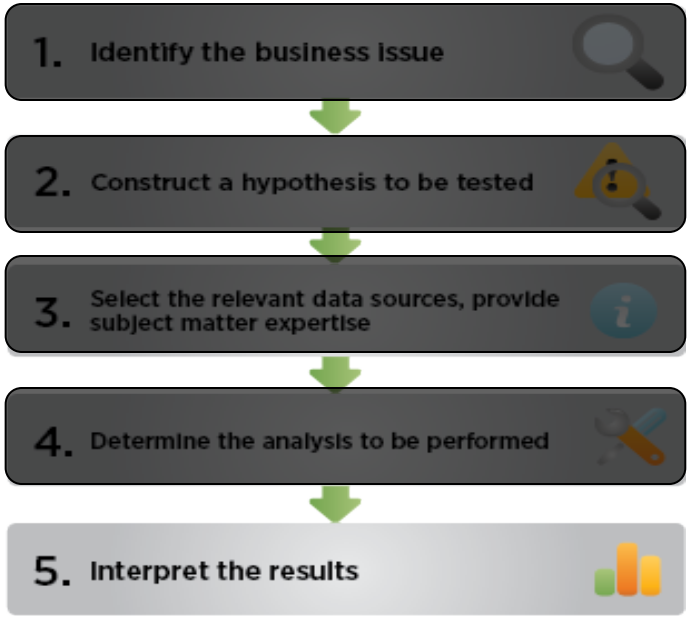


- For data exfiltration, start with what's normal and what's not (create a statistical model)
- How do we 'normally' behave?
- What patterns would we see to identify outliers?
- Look for other patterns based on uniqueness, frequency, periodicity, volume, duration, newness, duration, locality, etc.

Spoiler Alert! DNS Exfiltration Indicators

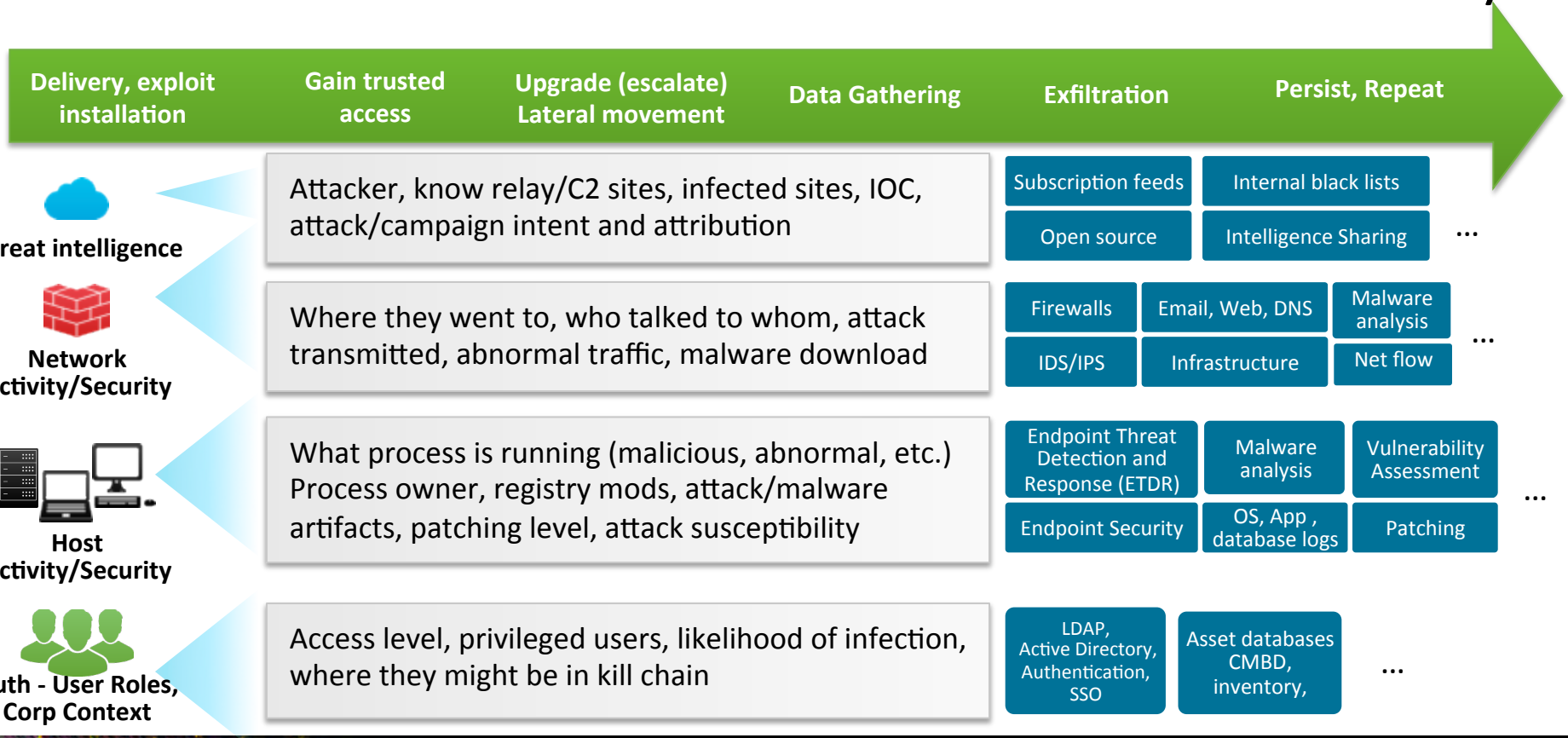
- 1) Look @ all DNS traffic for multiple levels of DNS strings. look for hexadecimal strings.
- 2) Look for this 3rd level to be less than 40 bytes in length... like *.domain.com, where * is longer than 40 bytes
- 3) Look for multiple DNS Name lookups to sketchy foreign domains, and look at the frequency in a short time span.
- 4) DNS TXT or SRV record queries to any foreign or high entropy domains
- 5) ANY DNS response to a loopback or RFC 1918 space/bogon space. (5.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12) could indicate a C2 channel
- 6) Look for multiple DNS queries to the same non-obvious or foreign domain during off-hours times in the office = check for frequency, and periodicity.
- 7) DNS queries to dynamic DNS providers (like OpenDNS)
- 8) DNS queries not followed by a proxy request for connection
- 9) Identify recurring interval or beaconing following any of the above (zero variance behavior)
- 10) Look for Teredo IPv6 addresses
- 11) Look for large TXT or NULL payloads (tunneling), and TXT that isn't 7-bith clean
- 12) Look for CNAME chains if they resolve internally
- 13) look for changes in authoritative name servers and their IP addresses as well.

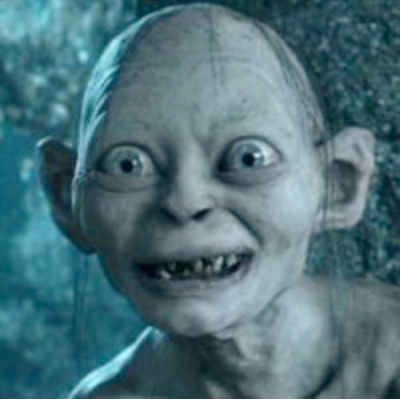
A Methodology for Analytics-Enabled SOC: Analysis + context



- Increase in business communications overseas?
- Does your statistical model need to change due change, business growth, or volume of data?
- Implemented a new service or application?
- Added employees overseas?
- Enriching/synthesizing outliers with visualizations?

Need to Connect the “Data-dots” to See the Whole Story





Methodology Parting Thoughts

Security Intelligence requires traditional IT data sources, not just security technology.

- What patterns/correlations of weak-signals in ‘normal’ IT activities would represent ‘abnormal’ activity?
- Heuristic detection approaches (SIEM historical standard) are best used with other detection approaches (Statistical/Behavioral)
- Threat modeling MUST be associated with critical data assets and employees
- Context is hardest and most critical to add, give yourself lead time…**BUT DO IT**
- What is rarely seen, newly seen, or a behavioral/statistical deviation?
- What normal activities occur during abnormal times?

Security Maturity Model with Splunk: How do I get there?

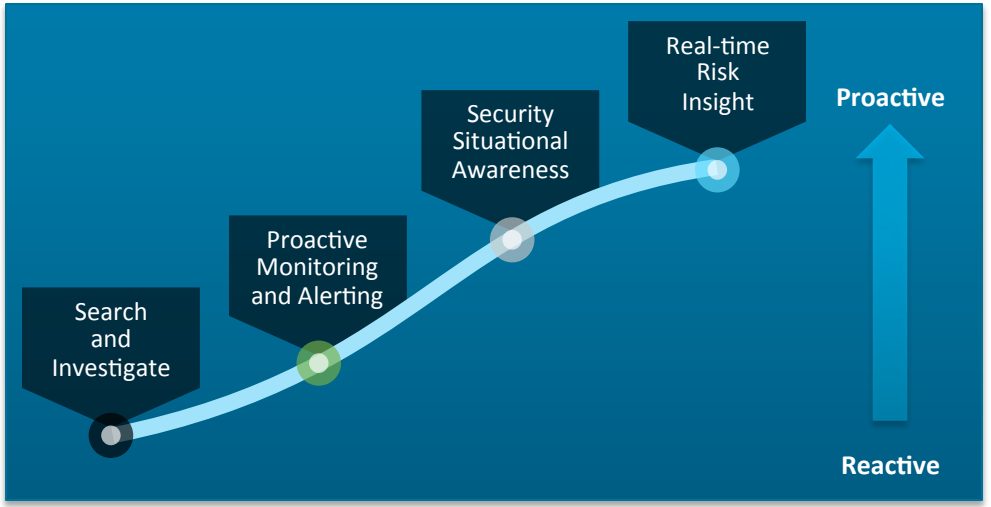
splunk>

Maturity Model for Security Operations

- ❑ APT detection/hunting (kill chain method)
- ❑ Counter threat automation
- ❑ Threat Intelligence aggregation (internal & external)
- ❑ Fraud detection – ATO, account abuse,
- ❑ Insider threat detection

- ❑ Replace SIEM @ lower TCO, increase maturity
- ❑ Augment SIEM @ increase coverage & agility
- ❑ Compliance monitoring, reporting, auditing
- ❑ Log retention, storage, monitoring, auditing

- ❑ Continuous monitoring/evaluation
- ❑ Incident response and forensic investigation
- ❑ Event searching, reporting, monitoring & correlation
- ❑ Rapid learning loop, shorten discover/detect cycle
- ❑ Rapid insight from all data



Security Operations Roles/Functions

- ❑ Tier 1 Analyst
- ❑ Tier 2 Analyst
- ❑ Tier 3 Analyst
- ❑ Audit/Compliance
- ❑ Security Analyst
- ❑ CSIRT
- ❑ Forensics
- ❑ Engineering
- ❑ Fraud analyst
- ❑ Threat research/Intelligence
- ❑ Malware research
- ❑ Cyber Security/Threat

Honest Questions, Honest Answers

- What is the talent level of my (Security) team?
- Do I have existing mature skill sets I can leverage/need to keep?
- What is the business's appetite for change?
- Am I building a Security Organization for Hunting and Advanced Threats, or doing what I can with the team/resources I have?
- Can I be successful implementing new processes around this methodology?

How Do I Determine My Maturity Level?

Pre-Engagement Posture Discussion

- What is your current SecOps model?
  - Insourced/outsourced/hybrid?
  - Incident Response plan? BIA?
  - what do you when you find something significant?

Threat Priority Matrix

- What are the risks to the business?
  - Establish business priorities
  - Model Threats and Business process
  - Design detection/prevention logic

Talent Capability Model

- How capable are my people?
  - Beginner/Intermediate/Advanced responders
  - are you investing in Threat Intelligence and Malware analysts?
  - How much collaboration happens between security and subject experts?

How Do I Determine My Maturity Level? (cont'd)

Content Strategy

- Data Acquisition mapped to threats/use cases
- Response by: Alerts/reporting/integration
- Manifest process and methodology into technology
- "How will I implement my playbook?"

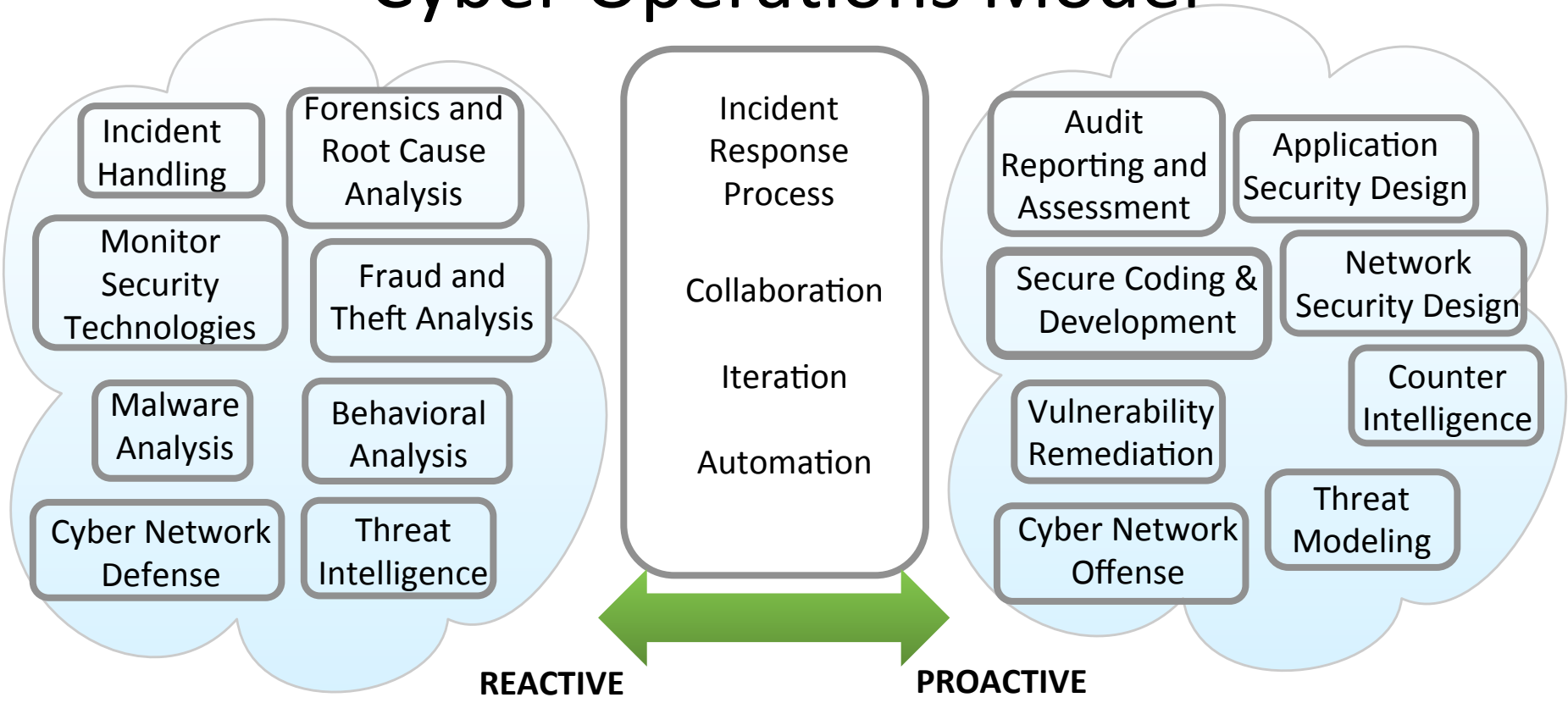
Post-Engagement Evaluation

- Does the work we did, translate to reducing business Risk?
- Is it measurable?
- Does it enable Security team to iterate and automate?
- Does it move the organization up the Security Maturity Model?

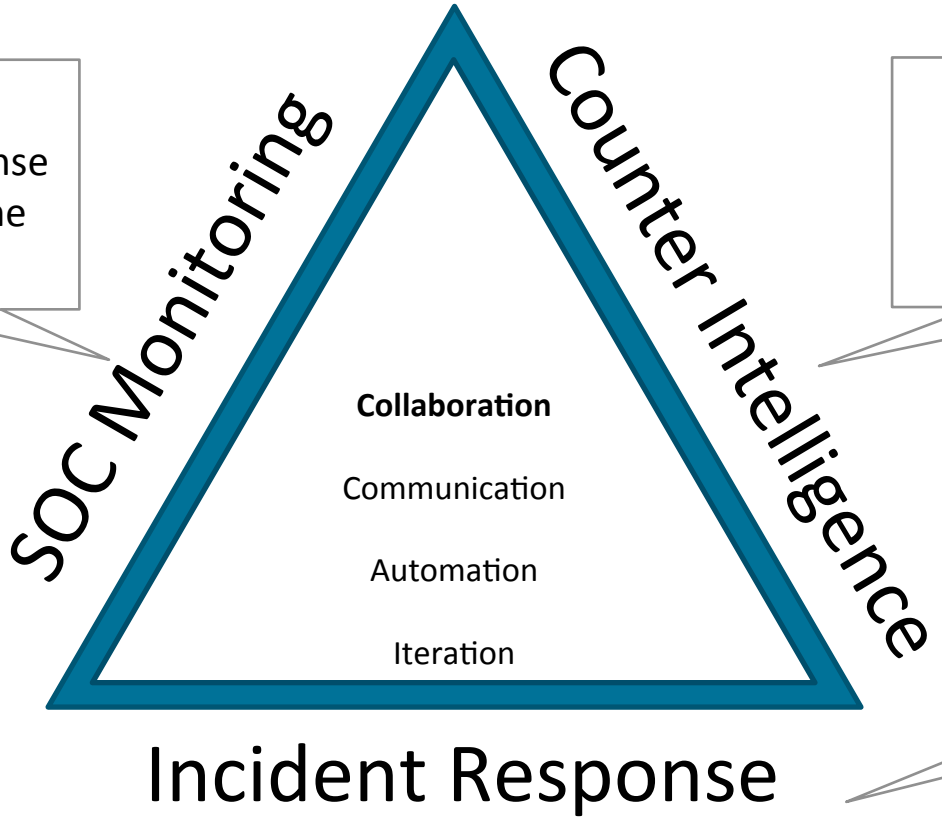
Talent Capability Model Scale

Cyber Ops Model	% Ops Time	Response Tier	Security Role	# Operators	Buisiness Unit	Splunk Role
Advanced (Level 3-4)	100	Tier 1	Analysts/SOC Operators(leads capable of multiple roles. tier 2, 3)	12	Security	User/Operator
24/7/365	70	Tier 2	Deep investigation/wire captures/RE/Threat Intel/ [IR team]	4	Security	Power User
	50	Tier 2	Content Developers {rules logic,custom content/ Environment Architecture	3	Security	Developer
	50	Tier 3	Counter-Intel {OSI/Threat stuff, briefings, Incident Analysis}	3	Security	Power User/Dev
	20	Tier 3	Security System Administrators	2	Security	Admin
	10	as needed	Subject Matter Experts (IT/mail/Apps/DevOps/DBA) [IR Driven]	4	Various	Power User
Intermediate (Level 2	100	Tier 1	Analysts/SOC Operators (leads perform in roles)	4	Security	User/Operator
24/7/365	50	Tier 2	Deep investigation/wire captures[IR team]	2	Security	Admin/Power User
	20	Tier 3	Counter-Intel {Threat Intelligence/Active Defense/custom content/Engineerir	2	Security	Admin/Developer
	10	as needed	System Administrators [IR Driven]	1	IT	Admin
	10	as needed	Subject Matter Experts (IT/mail/Apps/DevOps/DBA) [IR Driven]	4	Various	Power User
Basic (Level I)	100	Tier 1	NOC/SOC (likely automated analysis/SIEM)	2	IT/Security	User/Operator
8-5/M-F (MSSP)	50	Tier 2	Deep investigation/wire captures[IR team]	1	Security	Admin/Developer
	20	Tier 3	Security SME{Threat Intelligence/Active Defense/custom content/Engineerin	1	Security	Admin/Power User
	10	as needed	System Administrators [IR Driven]	1	IT	Power User
	10	as needed	Subject Matter Experts (IT/mail/Apps/DevOps/DBA) [IR Driven]	4	Various	Power User
None (Level 0)	100	Tier 1/2	NOC/SOC (likely automated analysis/SIEM)	2	IT/Security	User/Operator
event driven			Deep investigation/wire captures[IR team]		IT/Security	Admin/Developer
	10	as needed	System Administrators [IR Driven]		IT/Security	Power User
	10	as needed	Subject Matter Experts (IT/mail/Apps/DevOps/DBA) [IR Driven]	1 to 4	Various	Power User

Cyber Operations Model



Cyber Operations Model



Automation
Machine-time response
Triage using machine data and context

Iteration
Threat Modeling, Intelligence Gathering, Research, hunting

Collaboration
Incident Response
Forensic analysis
Operate on machine data and Threat Intelligence

In order to gain a complete view of Operational Security, we need to see the iteration of Counter Intelligence in Monitoring

Security Intelligence combines methodology, technology, collaboration as context for smarter security decisions

Where do we start? Integration Examples

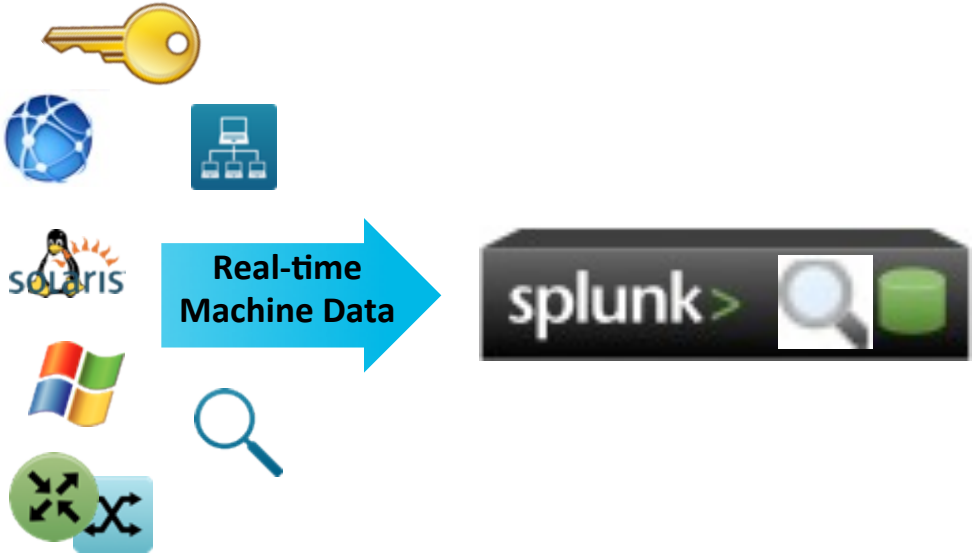
splunk>

Maturity Model Type Integrations

1) I have no visibility into my data, and I need to operate on that data
2) I have a SIEM, it doesn't do what I want. I need to augment with visibility and context
3) I have visibility, and context, I need threat intelligence and workflow and integration
4) I don't have a SIEM, but I also don't have any resources to do that

Lets look at an MSSP that supports your threat profile

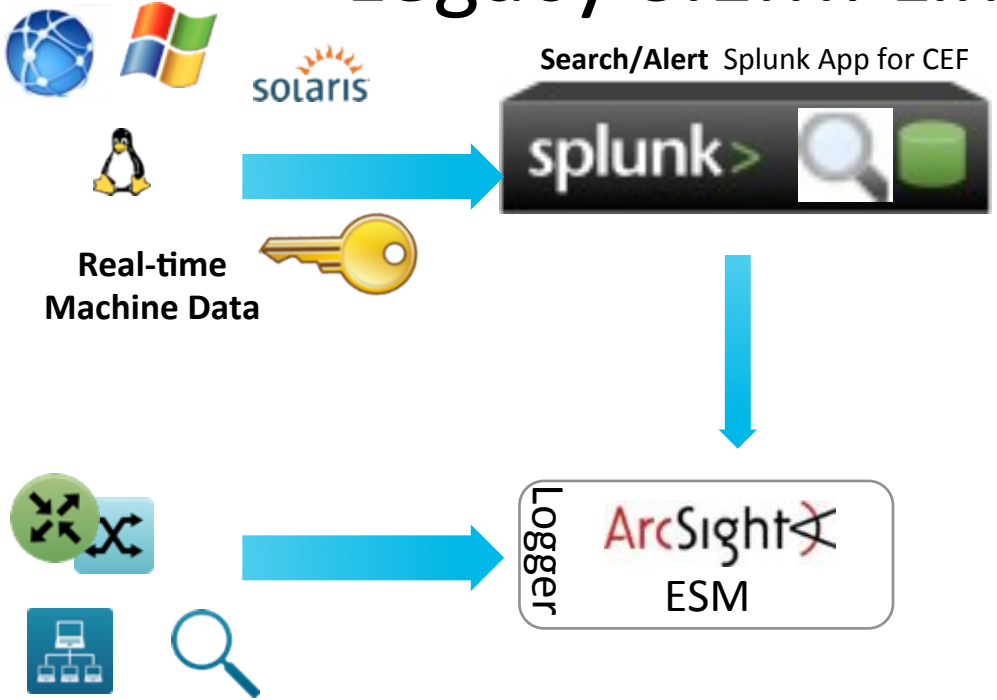
No SIEM: Getting Visibility First



"I'm not a security shop, I just need to see all my data first"

- Splunk for incident investigations/ forensics
- Splunk for alerting/reporting/ dashboarding
- Begin building data consumption towards use cases

Legacy SIEM: Limited Visibility



"I have a subset of security in my SIEM, I need more visibility across IT data"

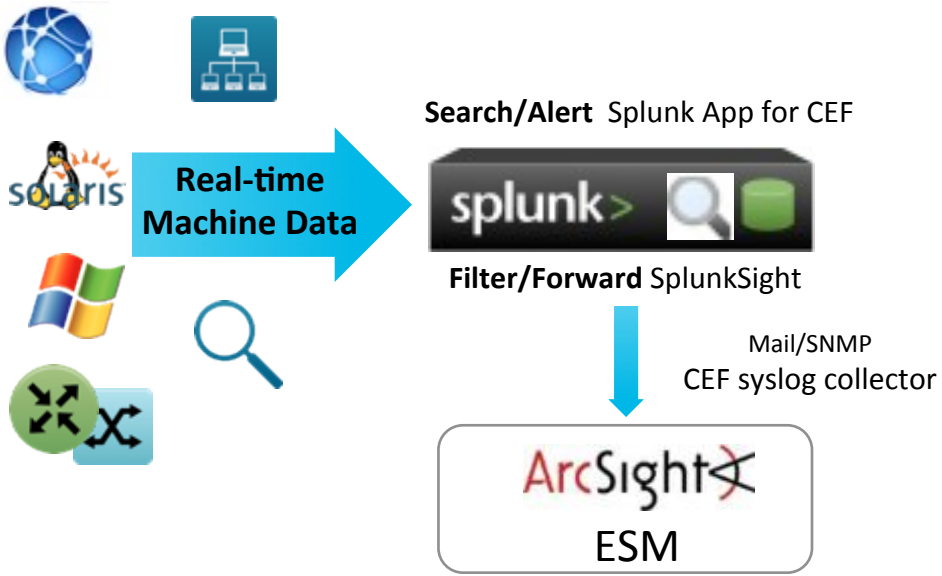
Different data sent to Splunk and SIEM

- **Splunk** for log aggregation, incident investigation/forensics, enrichment
- **ArcSight** for correlation, alerts, Analyst workflow

options for Splunk-to-ESM data flow:

1. At index time, Splunk can forward data to ArcSight: **SplunkSight**
2. At search time, Splunk can forward CEF format to ArcSight: **Splunk App for CEF**
3. Splunk alerts to ArcSight ESM via SNMP trap, e-mail, web services

Legacy SIEM: Splunk to ArcSight ESM



Using Splunk Forwarders for native log consumption

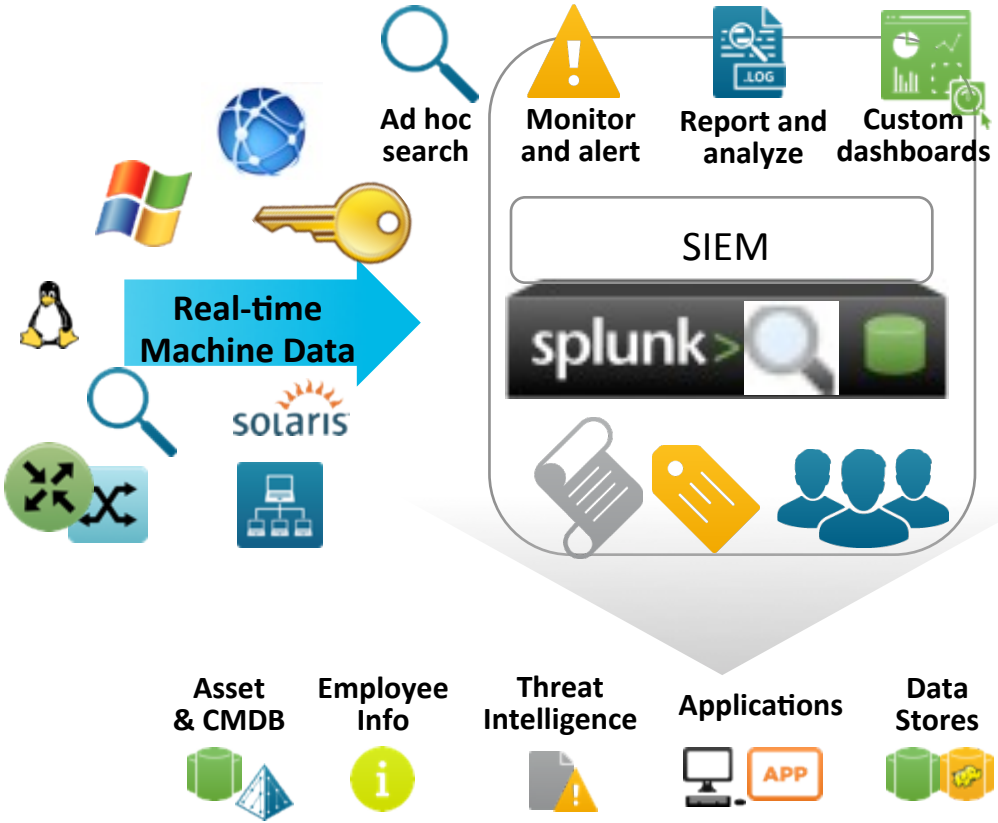
"I have a mature playbook my analysts use in SIEM"

- **Splunk** for log aggregation, incident investigation/forensics, enrichment
- **ArcSight** for correlation, alerts, Analyst workflow

options for Splunk-to-ESM data flow:

1. At index time, Splunk can forward raw or filtered data to ArcSight: **SplunkSight**
2. At search time, Splunk can forward selected, and/or enriched events in CEF format to ArcSight: **Splunk App for CEF**
3. Splunk alerts to ArcSight ESM via SNMP trap, e-mail, web services

SOC Integrated components



"II have many products leveraging my methodology and playbook"

Decisions on workflow made by automation/ prioritization feeding multiple tuned products

- **Critical ➔ Automatic tickets for SME resolution, Investigation (i.e. Archer)**
- **High/Med➔ Triage by type: automated action result/analyst action (i.e. SIEM)**
- **Low ➔ prioritized and funneled (i.e. Remedy)**
- Methodology driven, business process melded with technology and analyst skill sets
- Archer, JIRA, Remedy, ServiceNow integrations, Security tools like Palo Alto, Mandiant, FireEye, Checkpoint, Sourcefire
- Packets, flows, Threat Intel, enrichment, context

Adding Context

splunk>

Faster/Better Decisions with Context

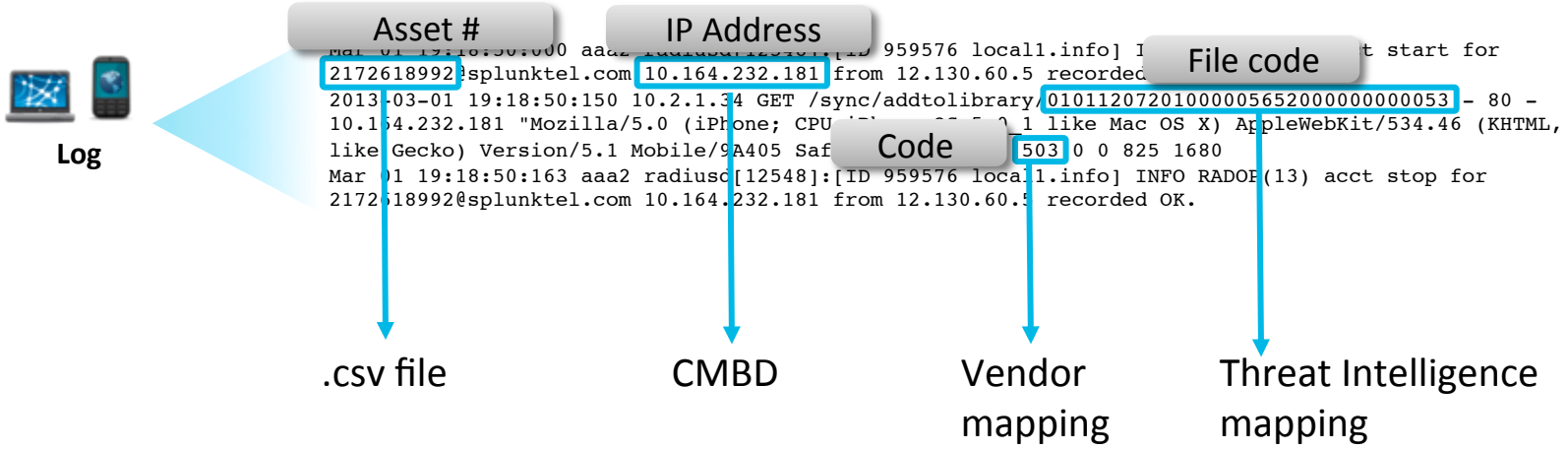
Real-time Machine Data

splunk>

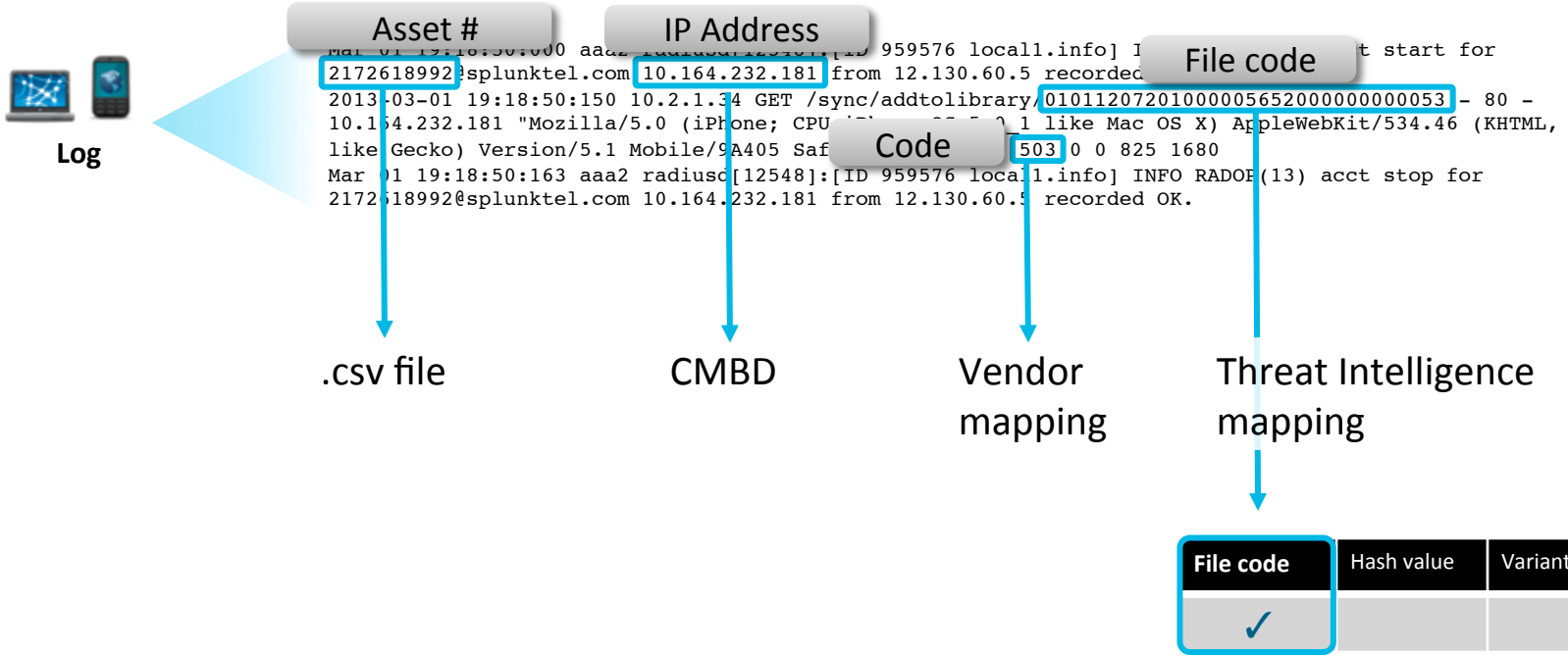
External Lookups

References – Coded fields, mappings, aliases
Dynamic information – Stored in non-traditional formats
Environmental context – Human maintained files, documents
System/application – Available only using application request
Intelligence/analytics – Indicators, anomaly, research, white/blacklist
AND MORE…

Encoded log with threat and asset context



Encoded log with threat and asset context

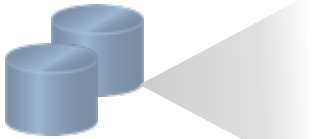


Encoded log with threat and asset context

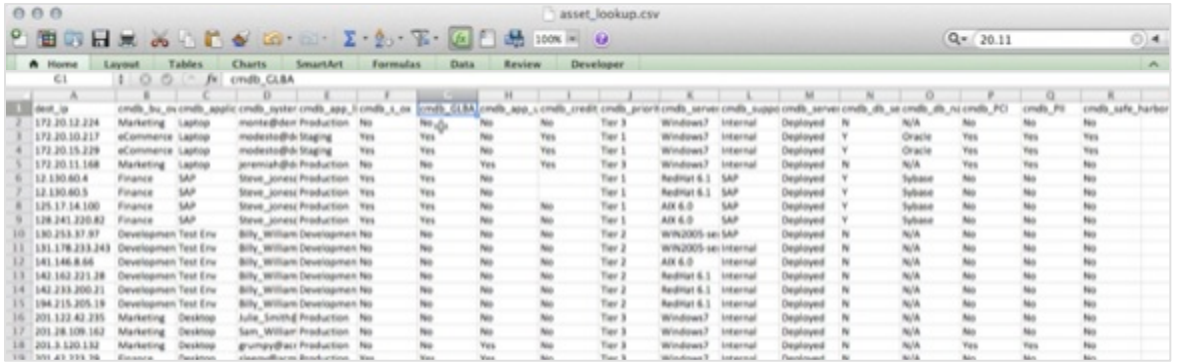
Log

```
Mar 01 19:18:50:000 aaa2 radiusd[12548]:[ID 959576 local1.info] INFO RADOP(13) acct start for
2172618992@splunktel.com 10.164.232.181 from 12.130.60.5 recorded OK.
2013-03-01 19:18:50:150 10.2.1.34 GET /sync/addtolibrary/0101120720100000565200000000053 - 80 -
10.164.232.181 "Mozilla/5.0 (iPhone; CPU iPhone OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML,
like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3" 503 0 0 825 1680
Mar 01 19:18:50:163 aaa2 radiusd[12548]:[ID 959576 local1.info] INFO RADOP(13) acct stop for
2172618992@splunktel.com 10.164.232.181 from 12.130.60.5 recorded OK.
```

External Lookup using .csv



Threat info (various)
Product code (file)
Asset (CMDB, various)



Automate Context: IOC lookups - Filename

Search

```
`malware` | stats count by signature,file_name,src,dest | lookup local=true apt1_filenames file_name OUTPUT is_apt1 | search is_apt1=true
```

Last 4 hours

45,419 matching events

Save

18 results from 8:47:00 AM to 12:47:15 PM on Wednesday, March 20, 2013

Export Options

50 per pag

Overlay: None

	signature	file_name	src	dest	count	is_apt1
1	none	2012ChinaUSAviationSymposium.zip	10.11.36.1	PARLCHARLYC01	1	true
2	none	2012ChinaUSAviationSymposium.zip	10.11.36.15	PARLCHARLYC01	1	true
3	none	2012ChinaUSAviationSymposium.zip	10.11.36.19	PARLCHARLYC01	1	true
4	none	2012ChinaUSAviationSymposium.zip	10.11.36.21	PARLCHARLYC01	1	true
5	none	2012ChinaUSAviationSymposium.zip	10.11.36.24	PARLCHARLYC01	1	true
6	none	2012ChinaUSAviationSymposium.zip	10.11.36.25	PARLCHARLYC01	1	true
7	none	2012ChinaUSAviationSymposium.zip	10.11.36.27	PARLCHARLYC01	1	true
8	none	2012ChinaUSAviationSymposium.zip	10.11.36.28	PARLCHARLYC01	2	true
9	none	2012ChinaUSAviationSymposium.zip	10.11.36.3	PARLCHARLYC01	2	true
10	none	2012ChinaUSAviationSymposium.zip	10.11.36.32	PARLCHARLYC01	1	true
11	none	2012ChinaUSAviationSymposium.zip	10.11.36.38	PARLCHARLYC01	1	true
12	none	2012ChinaUSAviationSymposium.zip	10.11.36.40	PARLCHARLYC01	1	true
13	none	2012ChinaUSAviationSymposium.zip	10.11.36.43	PARLCHARLYC01	1	true

Automate Context: IOC lookups - CIDR

Search

```
| `src_dest_tracker("allowed")` | lookup local=true apt1_blocks CIDRblock as src OUTPUT CIDRblock,is_apt1 | lookup local=true apt1_blocks.csv CIDRblock as dest OUTPUTNEW CIDRblock,is_apt1 | search is_apt1=true
```

Last 24

17,753 matching events

Save

969 results from 2:00:00 PM March 19 to 2:14:22 PM March 20, 2013

Export Options

« prev 1 2 3 4 5 6 7 8 9 10 next »

Overlay: None

turn on auto-open

	src	dest	count	sourcetype	CIDRblock	is_apt1
1	222.66.224.98	1.16.0.0	3	fortinet	222.64.0.0/13	true
2	222.66.224.98	1.19.11.11	3	fortinet	222.64.0.0/13	true
4	222.66.224.98	10.120.220.21	1	juniper:junos:idp	222.64.0.0/13	true
5	222.66.224.98	10.121.175.224	1	juniper:junos:idp	222.64.0.0/13	true
6	222.66.224.98	10.121.245.92	1	juniper:junos:firewall	222.64.0.0/13	true
7	222.66.224.98	10.121.37.17	1	juniper:junos:idp	222.64.0.0/13	true
8	222.66.224.98	10.121.45.90	2	juniper:junos:firewall	222.64.0.0/13	true
9	222.66.224.98	10.122.68.227	1	juniper:junos:firewall	222.64.0.0/13	true
10	222.66.224.98	10.123.105.247	2	juniper:junos:idp	222.64.0.0/13	true
11	222.66.224.98	10.123.139.156	1	juniper:junos:firewall	222.64.0.0/13	true
12	222.66.224.98	10.123.141.235	1	juniper:junos:firewall	222.64.0.0/13	true
13	222.66.224.98	10.123.170.54	2	juniper:junos:idp	222.64.0.0/13	true
14	222.66.224.98	10.123.178.139	2	juniper:junos:idp	222.64.0.0/13	true

Adding Intelligence

splunk>

Internal Threat Intelligence

Context for Security

- Directory User Information (personal e-mail, access, user privs)
- Proxy information (content)
- DLP & Business Unit Risk (trade secrets/IP lists)
- Case History/Ticket Tracking
- Malware/AV
- HR/Business Role

- Application Usage & Consumption (In House)
- Database Usage /Access Monitoring (privileged)
- Entitlements/ Access Outliers (In House)
- User association based on geography, frequency, uniqueness and privilege

External Threat Intelligence

Consumable Sources

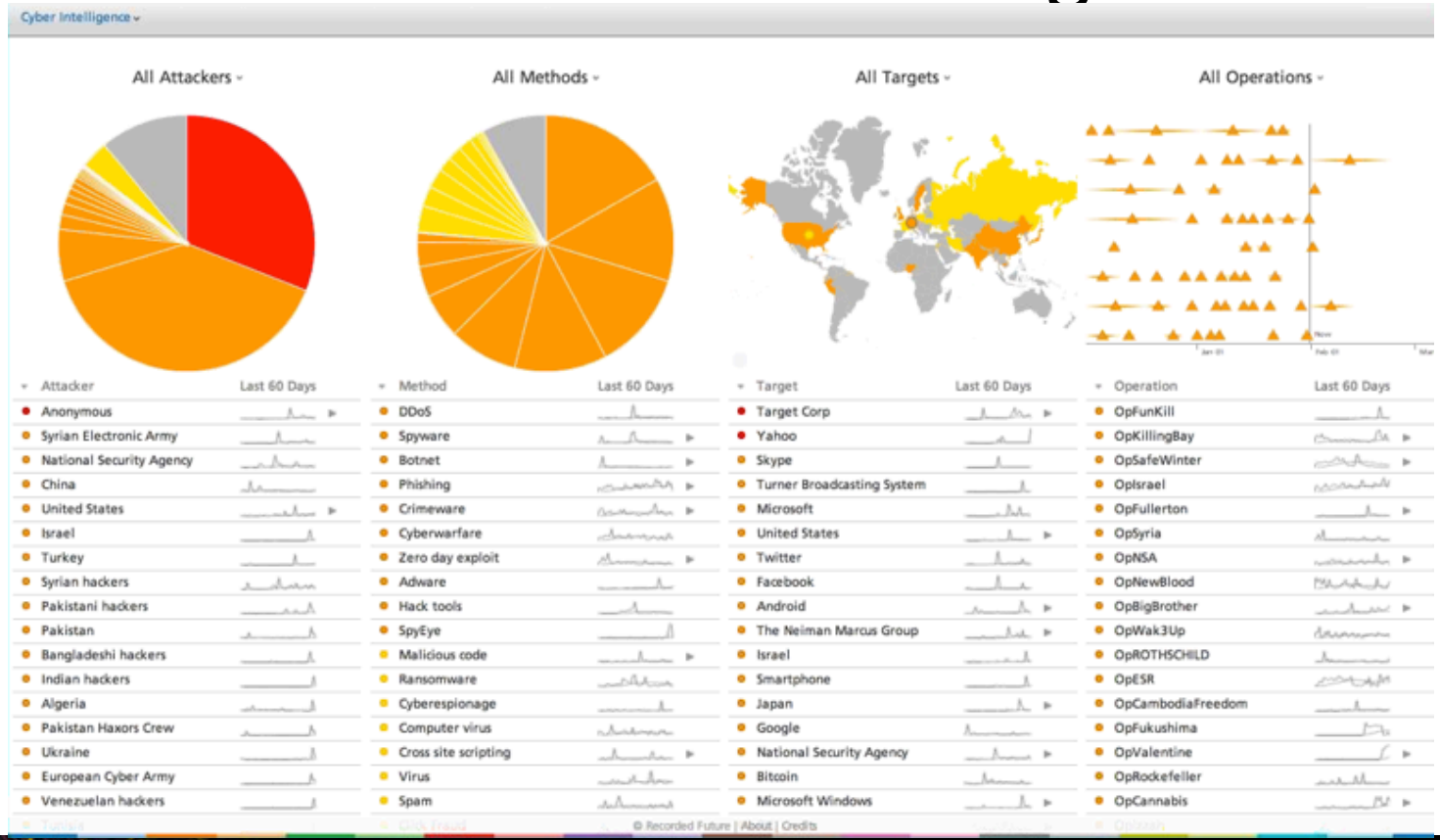
- **OSINT (free Sources)**
- Dell SecureWorks
- Verisign iDefense
- **Symantec Deepsight**
- McAfee Threat Intelligence
- **SANS/Whitelist/Blacklist**
- **CVEs CWEs, OSVDB (Vulns)**
- **iSight Partners**
- **ThreatStream**
- ATLAS
- **ThreatConnect**
- **Farsight**
- **Palo Alto Wildfire**
- **Crowdstrike**
- **AlienVault OTX**
- **RecordedFuture**
- **Team Cymru**
- **ISACs or US-CERT**
- **FireEye/Mandiant**
- Vorstack
- cyberUnited
- ThreatGrid
- **ZeroFox**
- **Norse Corporation**

External Threat Intelligence Integration

```
import httplib, urllib
params = urllib.urlencode({'apikey':
'f6dbdee2dc8c6118933b90178657877cc2cede3023ce0eba4xxxxxxxxxxxxxx', 'ip': '46.229.160.7', 'method':
'ipview'})
#headers = {"Content-type": "application/x-www-form-urlencoded", "Accept": "text/plain"}
headers = {"Content-type": "application/x-www-form-urlencoded", "Accept": "application/json"}
conn = httplib.HTTPConnection("us.api.ipviking.com:80")
conn.request("POST", "/api/", params, headers)
response = conn.getresponse()
print response.status, response.reason
data = response.read()
print(data)
conn.close()
```

Most Integrations are APIs or Modular Inputs – EASY!

External Threat Intelligence



splunk> Enterprise Security

Administrator | App | Manager | Alerts | Jobs | Logout

Home | Security Posture | Incident Review | Access | Endpoint | Network | Identity | Audit | Threat Intelligence | Resources | Search | Configure | Help | About

NorseCorporation

Norse Intelligence on Int...nal traffic last 24 hours

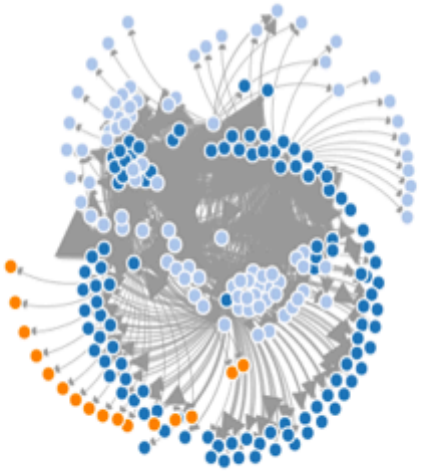
Project HoneyPot

US-CERT

Virus Bulletin

Wildlist

Highlight Node



```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="8ddb7d26-b275-446c-bbaa-387e6b29135b" last-modified="2014-02-12T02:21:38"
xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>Careto "The Mask" Espionage Campaign</short_description>
  <description>This IOC detects activity revealed in the Kaspersky report
  unveiling the mask. The Mask is an advanced threat actor that has been
  involved in cyber-espionage operations since at least 2007. The name "Mask"
  comes from the Spanish slang word "Careto" ("Ugly Face" or ?Mask?) which
  the authors included in some of the malware modules. The main targets of
  Careto fall into several categories: Government institutions, Diplomatic /
  embassies, Energy, oil and gas, Private companies, Research institutions,
  Private equity firms, and Activists. The Mask?s implants can intercept
  network traffic, keystrokes, Skype conversations, analyse WiFi traffic, PGP
  keys, fetch all information from Nokia devices, screen captures and monitor
  all file operations.</description>
  <authored_by>@iocbucket</authored_by>
  <authored_date>2014-02-12T01:05:09</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="d8799972-a5b1-49de-a4e4-a3691a732b4d">
      <IndicatorItem id="8d6b0f66-0351-4ca0-b21c-19c895b25bbc"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">linkconf.net</Content>
      </IndicatorItem>
      <IndicatorItem id="a9d87fad-e313-48cc-b858-d8caaad2edcb"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">redirserver.net</Content>
      </IndicatorItem>
      <IndicatorItem id="4d5623fc-66c4-45c6-8804-3c0737c30a35"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">swupdt.com</Content>
      </IndicatorItem>
      <IndicatorItem id="de7165e5-f647-4f81-b82e-5c4f0a210e5e"
      condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">shlink32.dll</Content>
```

Raw IOC Not Easy

IOC Alerts

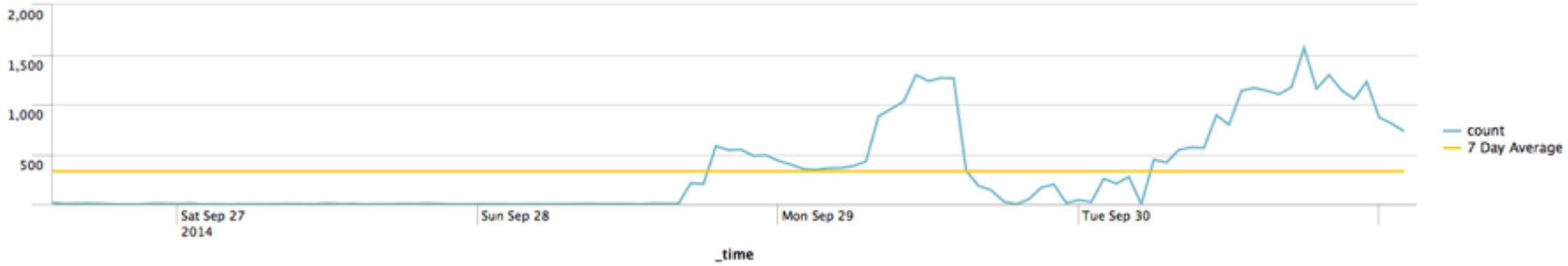
Splunk Indicators of Compromise Engine

Edit | More Info

Most Recent Indicators Found (last 24 hours)

Time Detected	Indicator Type	Matching Sourcetype	Indicator ID
10/01/14 02:16:20.000 AM	ipv4-addr	linux_secure	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	linux_secure	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	websense	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	bro_conn	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	linux_secure	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	dhcpd	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	dhcpd	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	linux_secure	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	bro_http	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f
10/01/14 02:16:20.000 AM	ipv4-addr	bro_ssh	mandiant:object-232deffc-063f-4e83-9027-1b930af4a09f

Number of Matching Indicators over time (last 7 days)



Context+Threat Intelligence:TLD against GeoIP

How would I find all the URLs by their Top Level Domain, and compare them with their geolocation to validate they are legitimate on a map?

Matching against TLD & GeoIP

```
sourcetype=bluecoat url=* | lookup faup url | fields url_domain url_tld |
geoip url_domain | eval
url_domain_country_code=lower(url_domain_country_code) | eval
tld_match=if(url_tld == url_domain_country_code, "true", "false")

#Run FAUP as a lookup across all bluecoat URLS

#generate the geolocation telemetry for url_domain

#determine if the url country code is = to the TLD
```

Now, show me on the map where they are…

```
sourcetype=bluecoat url=* | dedup url | lookup faup url OUTPUT url_subdomain url_domain url_tld | fields url_domain url_tld | geoip url_domain | eval
url_domain_country_code=lower(url_domain_country_code) | eval tld_match=if(url_tld == url_domain_country_code, "true", "false")
```

All time

53 matching events

Save | Create

Show timeline

Views:

Map | Geo Results | Events

22 results with location information (5 distinct locations) over all time

Questions?

splunk>

Some Content For You

- Archer Integration Technology add-on template
- Scripts for ticket system alerting
- SA-VA, ES Vulnerability Assessment/Risk calculation tool

Follow @Splunksec on twitter for these releases today after our session!

What You Can Do for the Security Practice

- We love to dig through new data sets
- Share cool, hard use cases with us
- Share knowledge to help us better the product
- All your desires and concerns for features and uses

Partner with us, we will do the same!

- Help with integrations, use cases, features functions.
- Our job is to help you get to your highest maturity level

Thank you!

@SplunkSec

security@splunk.com

splunk>

Appendix

- SA-VA (How it works)
- SplunkSight (How it works)
- TA-Archer (How it works)

Adding Context:

Splunk > Nmap + CVE=Risk Score

splunk>

Problem

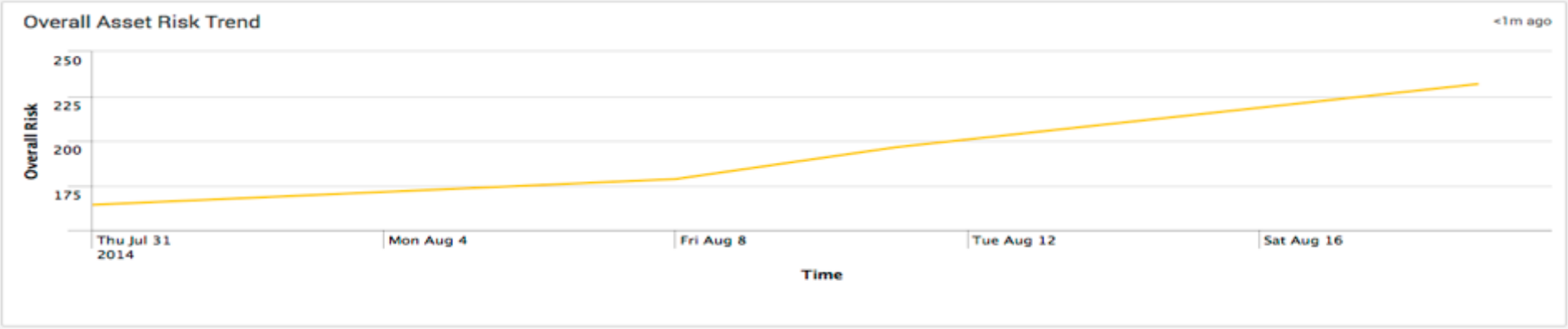
- Network complexity and attack surface is growing
- No central location for exploit information
- Manual system prioritization based on risk is (nearly) impossible
- Analysis must be done regularly as new exploits are released

Solution: SA-VA

- Automated exploit database aggregation
  - SA-VA automatically parses National Vulnerability Database http://nvd.nist.gov/ and Offensive Security's Exploit-DB https://github.com/offensive-security/exploit-database
- Scheduled vulnerability scan
- Integration with Splunk Enterprise Security assets
  - SA-VA integrates with your existing security solutions to give a clearer picture

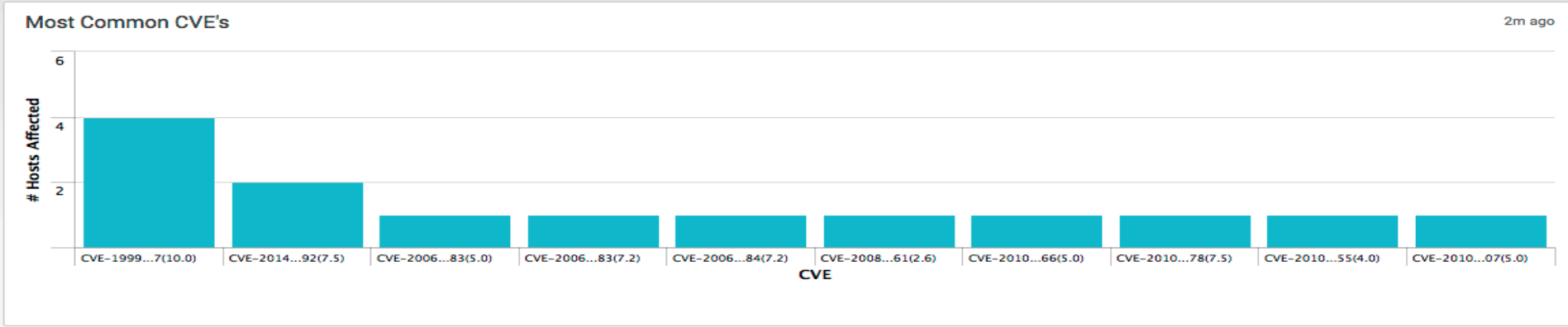
Solution: SA-VA

Monitor network risk trends



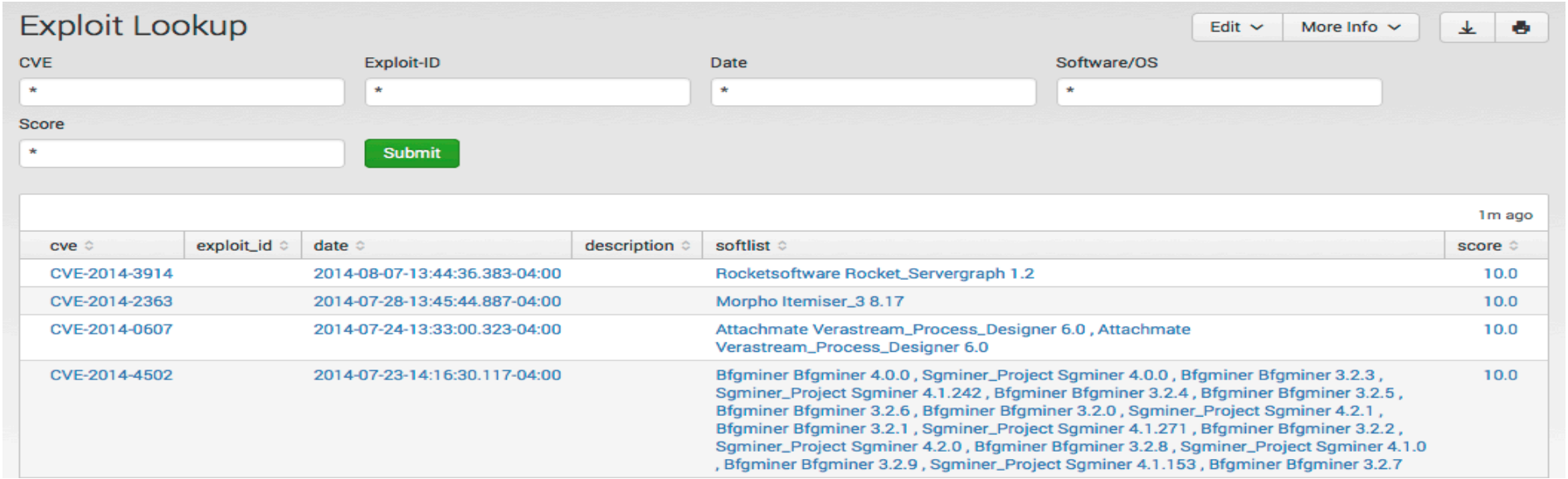
Solution: SA-VA

Isolate exploits affecting a large number of hosts



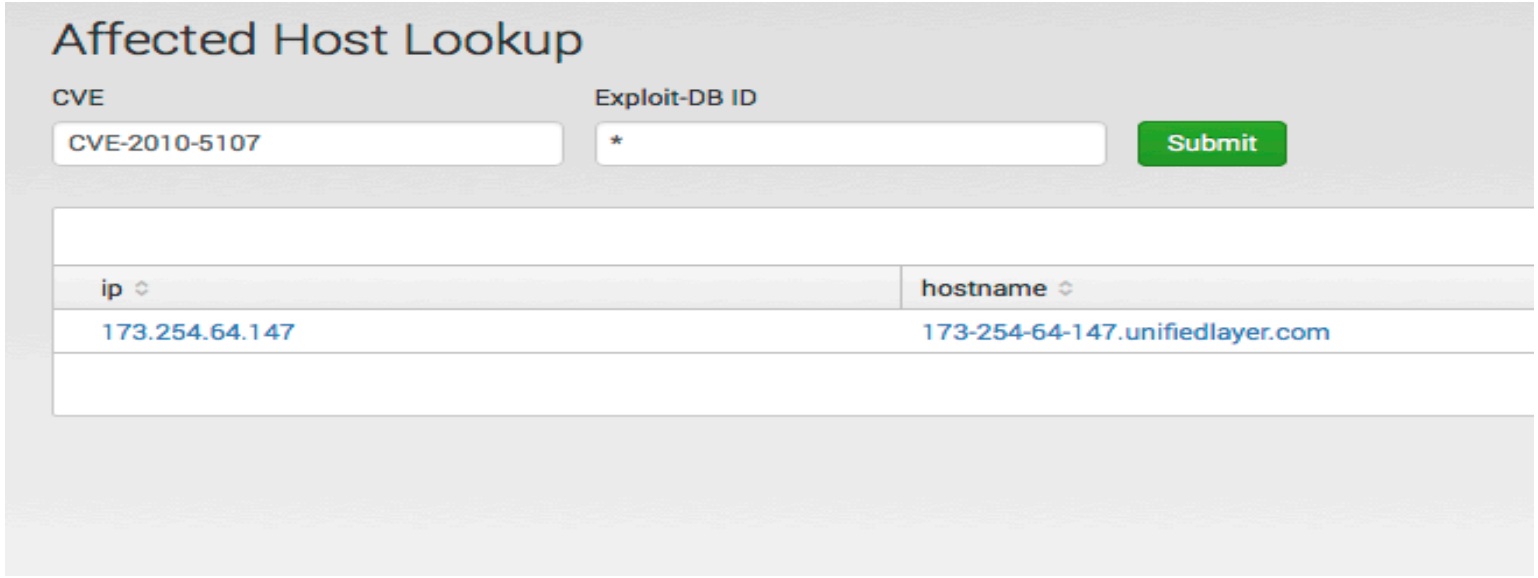
Solution: SA-VA

Access to information on thousands of exploits



Solution: SA-VA

View all hosts affected by specific exploits



Calculating Risk for Assets.csv

- Risk Percentage
  - Δ Risk Score / Reference Score (Gold Standard)
- Risk Score
  - Σ Service Score
- Service Score
  - CVSS Severity / (Current Year – Release Year)
- Every host scanned is assigned a risk percent as a function of the reference score, and an overall risk score
- Every service is assigned a risk percent score as a percentage of host's overall risk

Example

i	Time	Event
>	8/19/14 4:02:55.000 PM	127.0.0.1


```
{
    "risk": "374.00%",
    "hostname": "localhost",
    "host_score": "23.70",
    "services": {
        "88: Heimdal Kerberos ": {
            "cve": "CVE-2006-3083(7.2), CVE-2006-3084(7.2)",
            "score": "6.75%",
            "exploit_db": "None"
        },
        "Unidentified": {
            "score": "93.25%"
        },
        "22: OpenSSH 6.2": {
            "cve": "CVE-2014-1692(7.5), CVE-2014-2532(5.8), CVE-2014-2653(5.8), CVE-2013-4548(6.0)",
            "score": "93.25%",
            "exploit_db": "None"
        }
    },
    "dns": "localhost, 1.0.0.127.in-addr.arpa, 127.0.0.1 (scanned with localhost)",
    "time": "Tue Aug 19 16:02:55 2014",
    "os": "Apple Mac OS X 10.8 (Mountain Lion) (Darwin 12.0.0)",
    "open_ports": "22,88",
    "state": "up",
    "addresses": {
        "ipv4": "127.0.0.1"
    },
    "ref_score": "5"
}
```


Collapse

Configurability

- Provide custom arguments to Nmap scan in addition to preset scan arguments
- Whitelist to exclude sensitive hosts from scans
- Block specific vulnerabilities scoring on a host specific and global level
- Schedule and automate database updates and network scans based on your network needs

Summary

- Automate vulnerability database aggregation
- Schedule scans and database updates
- Whitelist machines sensitive to scans
- Multiple scan intensity options including custom arguments for VoIP, printers, and other sensitive systems
- Integration with Enterprise Security assets model
  - Appends fields to existing assets.csv
  - Create new assets.csv based on scan
- Calculated Risk prioritization score
  - Risk % = Δ Risk Score / Gold Standard
  - Risk Score = Σ (CVSS severity /(Current Year – Release Year))

SIEM Augmentation:

SplunkSight
Splunk > Arcsight

splunk>

Delivering Context to CEF for Analytics-driven Security

Datamodel Enrichments Enhance Decision Making

- Add context to events by using Splunk Add-ons and custom lookups
- Constrain, filter, or augment data via CIM or custom datamodels
- Aggregate events from multiple sources before forwarding

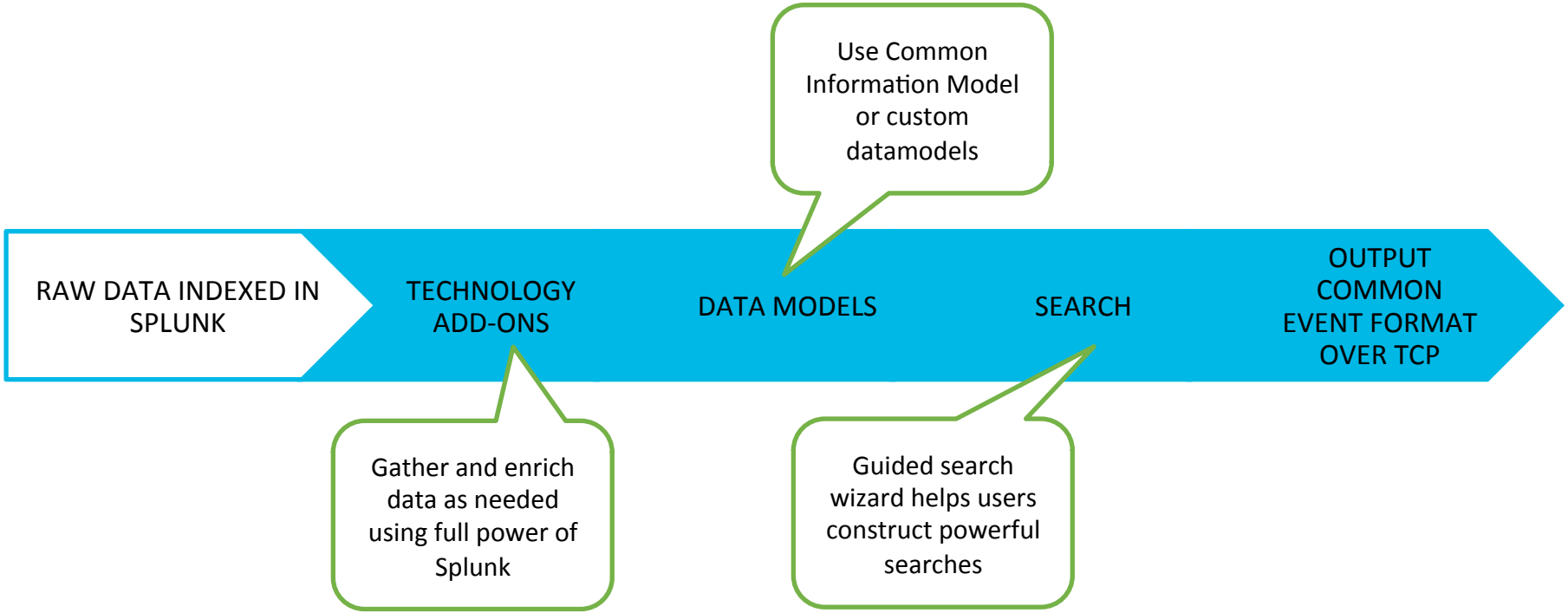
Connect and Visualize Disparate Data In Familiar Tools

- Gain faster, easier and deeper insights across all machine data
- Simply map Splunk fields to CEF fields without knowledge of the Splunk search syntax, using a new Guided UI

Automatically Deliver Insight from Splunk to the Front Lines

- Organizations where an incumbent SIEM is the Tier 1 tool can now receive augmented events and alerts
- Increase the value of threat intelligence by indicating important events

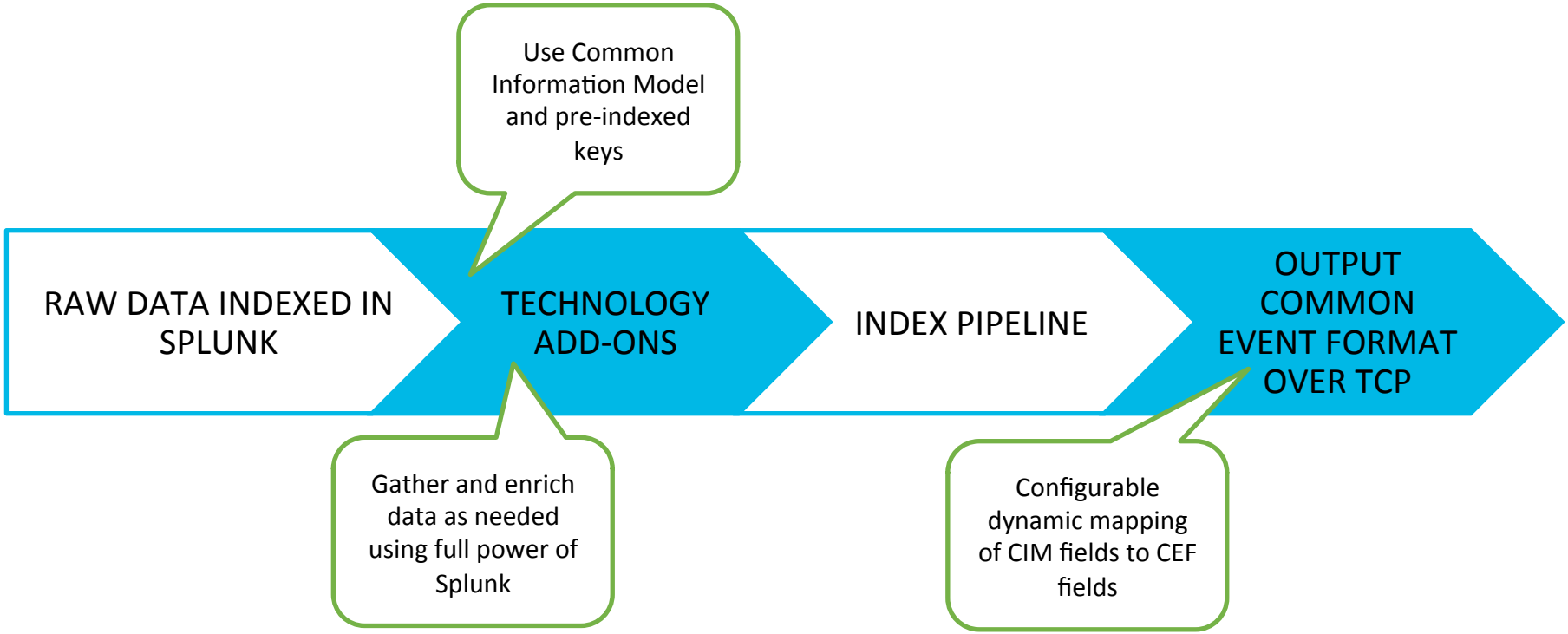
Inside Splunk App for CEF



Why Splunk app for CEF?

- For many data sources, dual feeding both Arcsight and Splunk , the same events is not feasible
- Splunk App for CEF enables CEF-formatted output based on **search results** in Splunk
- Field mappings from Splunk CIM to Arcsight CEF make configuration easy

Inside SplunkSight



Why SplunkSight?

- Scaling your CEF output structure should scale with Splunk architecture
- SplunkSight enables CEF formatted output based **indexed fields** in Splunk
- SplunkSight uses TCPOUT to process events directly on each indexer
- Index and sourcetype filters enable flexibility
- Field mappings from Splunk CIM to Arcsight CEF make configuration easy

Integration Challenges

- Splunk currently, cannot send CEF data directly to Arcsight ESM at scale, or index time.
- Logger agents tend to lose data in translation via Snare and syslog
- Splunk forwarders are not distributed across the entire infrastructure to capture raw windows events
- Target's challenge is 100% visibility, and ubiquity in their collection environment for host data collection
- single agent to feed both their collection and correlation technology.

We built SplunkSight to deal with these challenges

SplunkSight

Designed to be Highly scalable

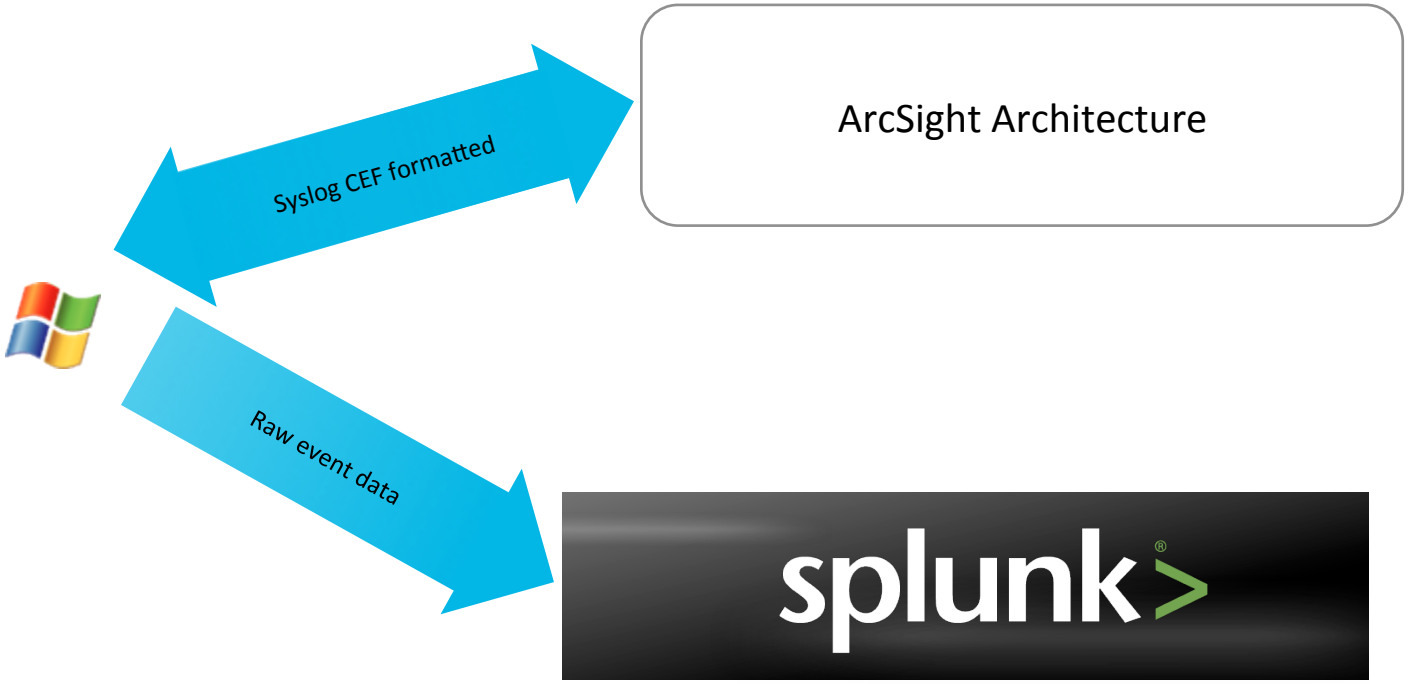
- Located on each Indexer as a separate socket-ized process
- Multi-threaded process to deal with scale
- Operates at index-time as opposed to search-time
- Does not impact the parsing or indexing queues in indexing pipeline
- Does not directly impact search behaviors or search pipeline performance

SplunkSight

Designed to be easily configurable

- Enable mapping from CIM to CEF in a .csv file
- Designed to work with metadata written at index time using Technology Add-on framework
- Allows Target to specify specific fields to consume in Splunk for consumption in ESM
- Manageable via the deployment server

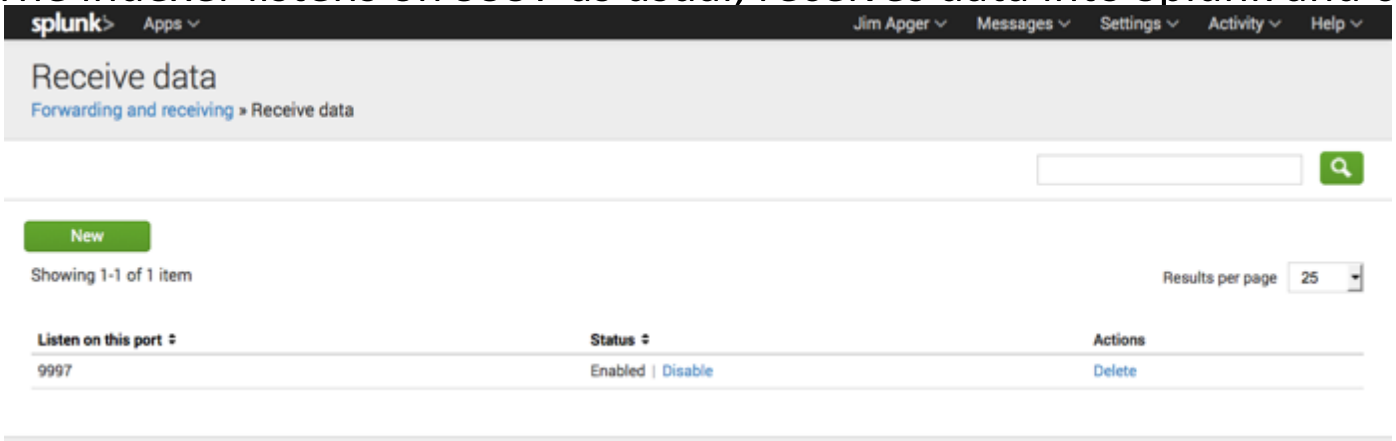
Current Architecture Challenge



Architecture with SplunkSight

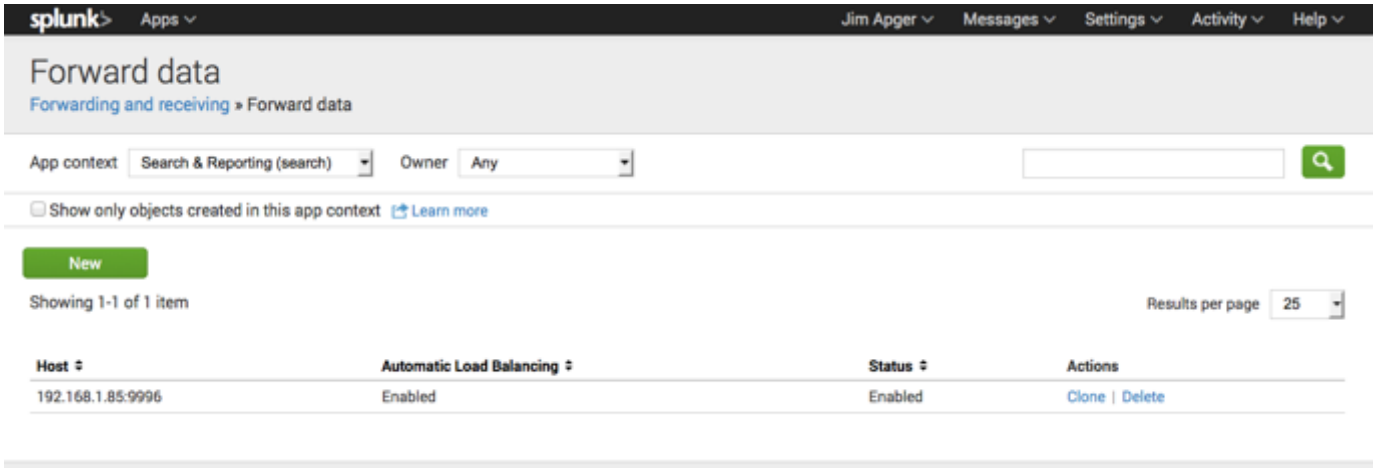
How it Works

- Communication from forwarder
  - We configure the forwarder to send data to the Splunk Indexer, as you have currently deployed Splunk today.
  - For data types requiring transformation at index time (either on a Heavy Forwarder, or on the Indexer) we send either **Cooked** or **Uncooked** data.
  - The indexer listens on 9997 as usual, receives data into Splunk and consumes it.



How it Works

- Communication from indexer to SplunkSight
  - The Splunk Indexer sends via **outputs.conf**, data to SplunkSight, which lives on a configurable socket on the indexer (we are using 9996 as example)
  - We are sending data using our **TCPOUT** option in our proprietary **S2S protocol**, which allows us to field map, and transform data into CEF Output.



How it Works

- Sending data to Arcsight ESM
  - Defined in splunksight.conf
  - Output is UDP syslog
  - SplunkSight runs as a service and includes a few python processes:
    - Process.py
    - Cefobjectizer.py
    - Daemon.py
    - Utils.py
    - Read-conf.py
    - Splunksightsyslog.py
    - Splunksight.py

Splunksight.conf

```
[daemon]
listen_ip = 0.0.0.0
listen_port = 9996
log_file = /tmp/splunksight.log
pid_file = /tmp/splunksight.pid
log_type = standard

[syslog]
proto = udp
dest_ip = x.x.x.x
dest_port = 514
```

How it Works

- Configuring SplunkSight
  - Requires **WRITE_META = true** for Technology add-ons (**This creates an indexed field**), fields and props configuration.
  - Provide mapping of CIM (Splunk) fields, to CEF (Arcsight) fields i.e. default.csv

Default.csv
#cim,cef
dest,CEF_dest
session_id,CEF_session_id
dest_nt_host,CEF_dest_host
src_ip,src
dest_ip,dst
src_port,spt

Splunk_TA_Windows

Transforms.conf
[Target_Server_Name_as_dest]
SOURCE_KEY = Target_Server_Name
REGEX = ([\\]+)?([^-].*)
WRITE_META = True
FORMAT = dest::"$2”

Fields.conf
[dest]
INDEXED = true

How it Works

- Configuring SplunkSight
  - Enables filtering based on Sourcetypes and indexes. By default, we remove all the _* indexes
  - Can configure whether we send ALL data, or just metadata

Splunksight.conf

[filters]
indexes_to_discard = _internal _introspection _thefishbucket _audit _blocksignature

#sourcetypes_to_discard =sourcetype::syslog
sourcetypes_to_discard =sourcetype::sep::risk

CEF Output example

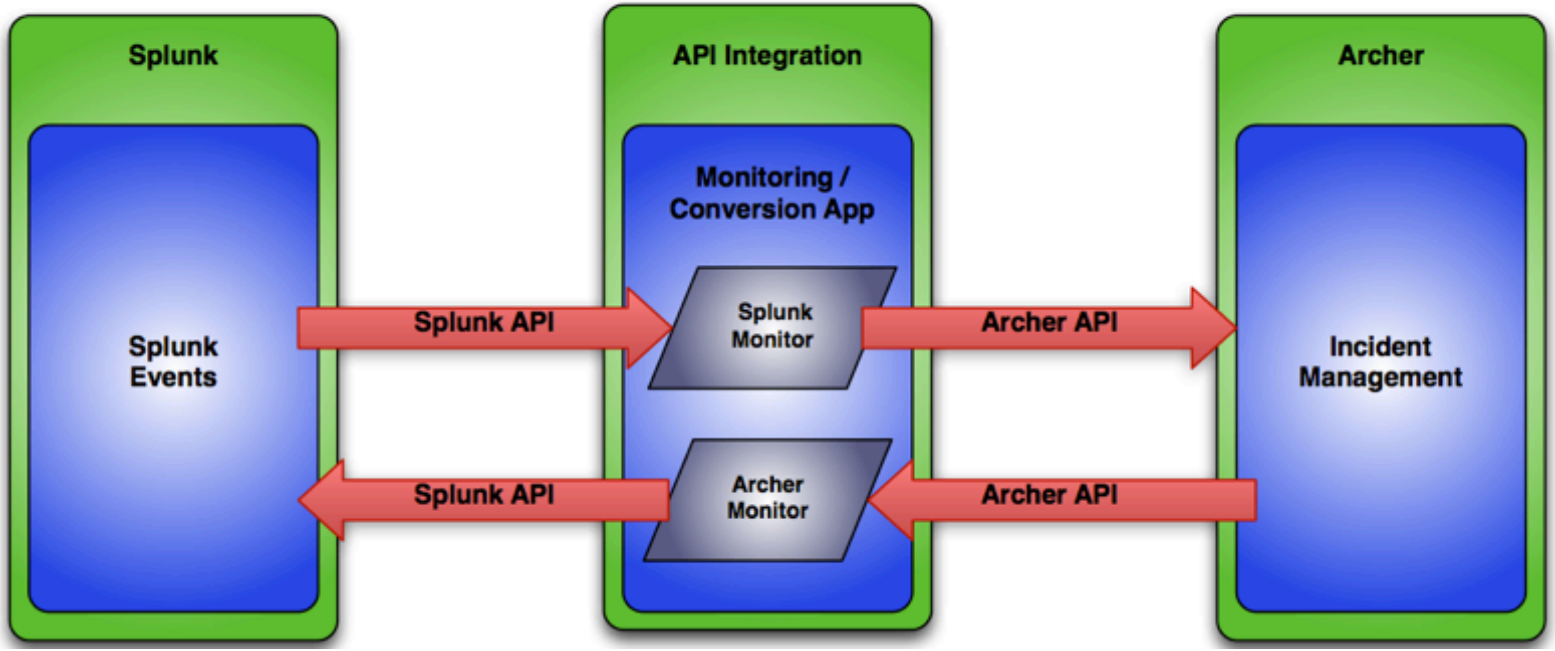
Sep 4 20:30:03 172.16.130.1 CEF: 0|Splunk|sourcetype::bluecoat|1.0|100000|generic event|5|src=10.11.36.20 end=179 fileType=application/x-fcs in=24804 request=http://199.9.251.150/idle/1021363361/6290 xreferrer=- requestMethod=POST suser=- act=TCP_NC_MISS xstatus=200 requestCookies="Flash\"" out=212
Sep 4 20:30:03 172.16.130.1 CEF: 0|Splunk|sourcetype::bluecoat|1.0|100000|generic event|5|
Sep 4 20:30:03 172.16.130.1 CEF: 0|Splunk|sourcetype::bluecoat|1.0|100000|generic event|5|
Sep 4 20:30:03 172.16.130.1 CEF: 0|Splunk|sourcetype::bluecoat|1.0|100000|generic event|5|src=10.44.38.116 end=125 fileType=- in=39 request=tcp://216.219.113.250:443/ xreferrer=- requestMethod=CONNECT suser=- act=TCP_TUNNELED xstatus=200 requestCookies=- out=67

Workflow Example:

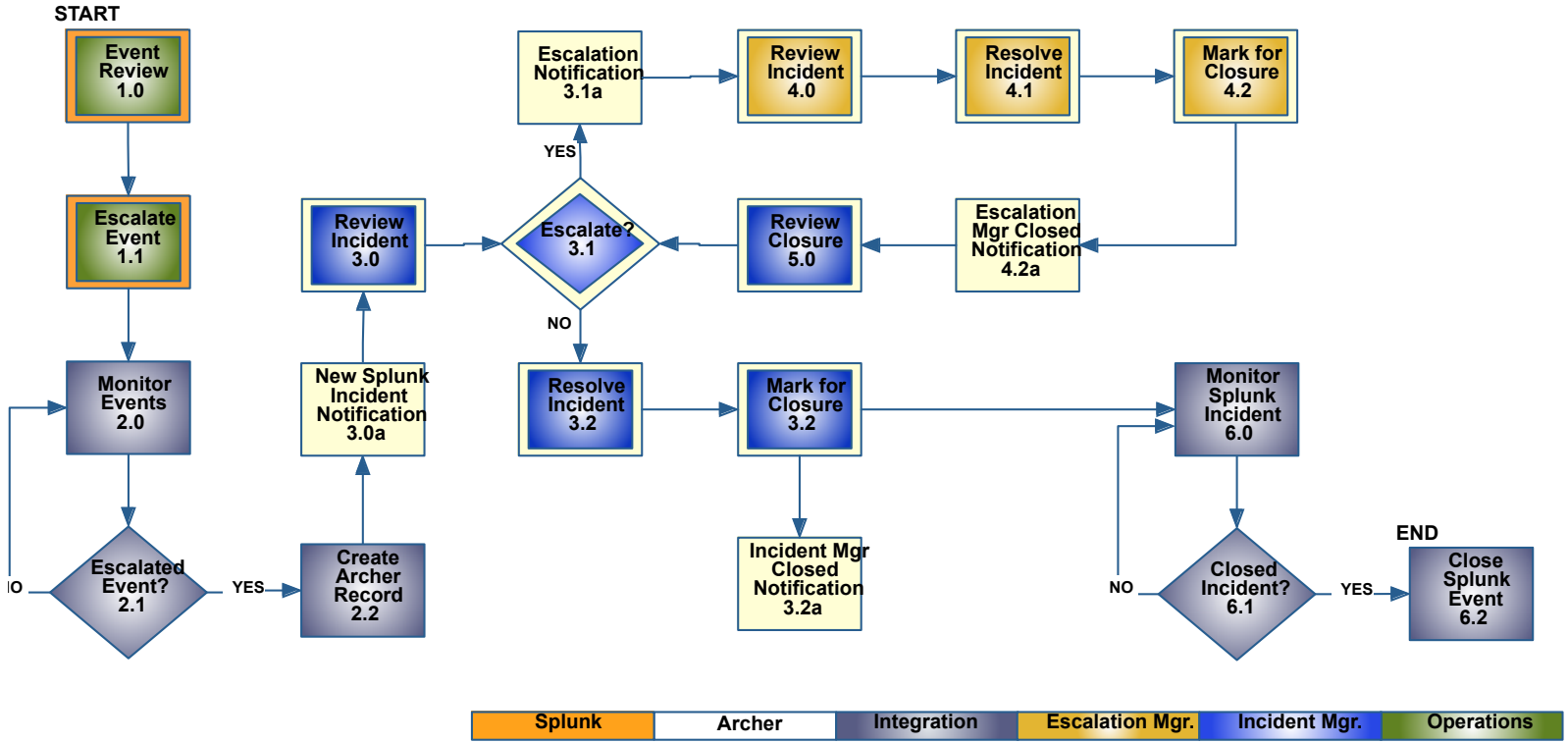
Splunk > Archer

splunk>

Splunk / Archer Integration Overview - v1.0



Splunk / Archer Integration Workflow - v1.0

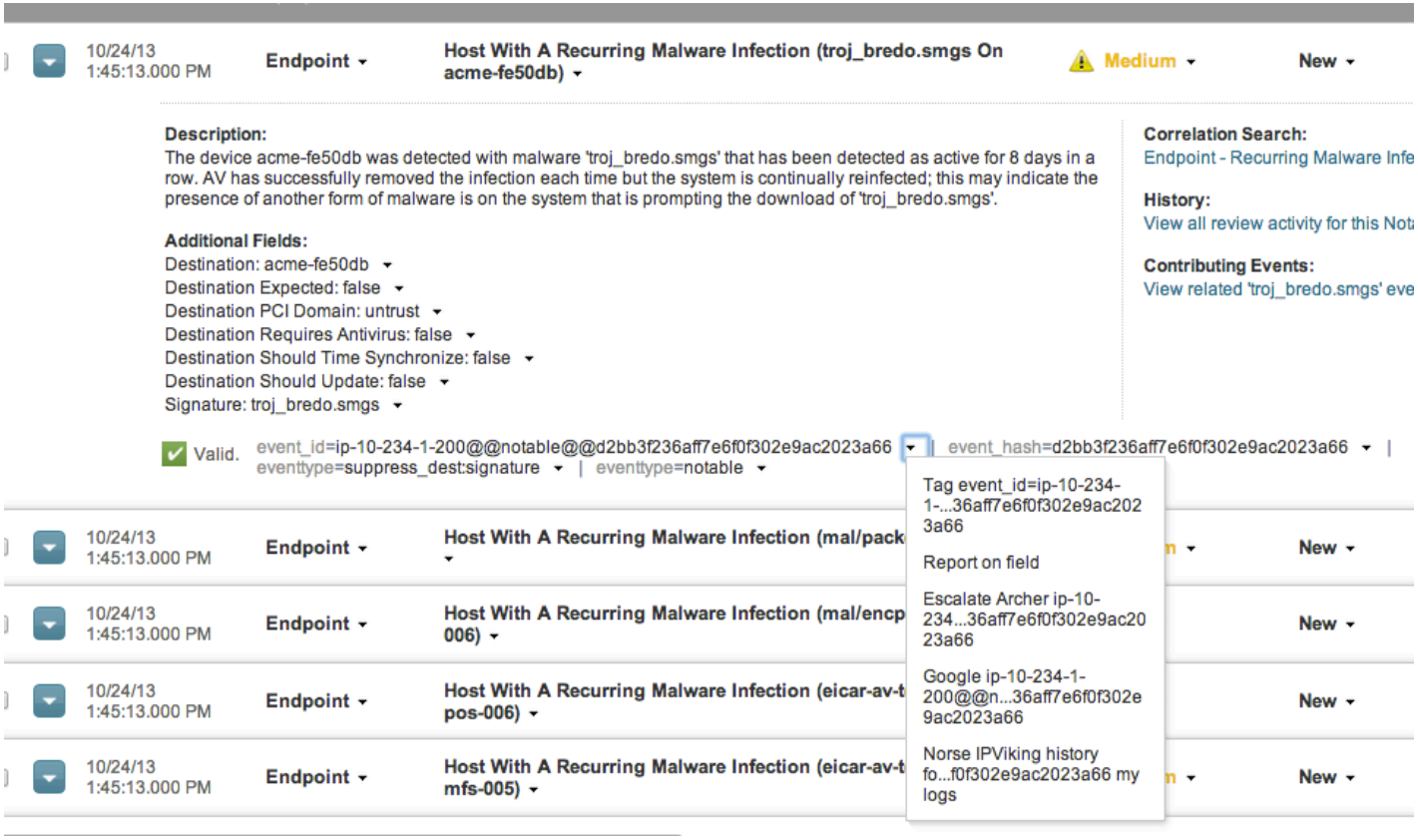


Getting Data to Archer

python REST API interaction with Splunk API for gathering things like asset info, vuln data, etc pulled from the metadata 'Notable Events' correlation framework.
The common set of fields in the correlationsearches.conf specification would be passed to archer, driven by the **rule_id**

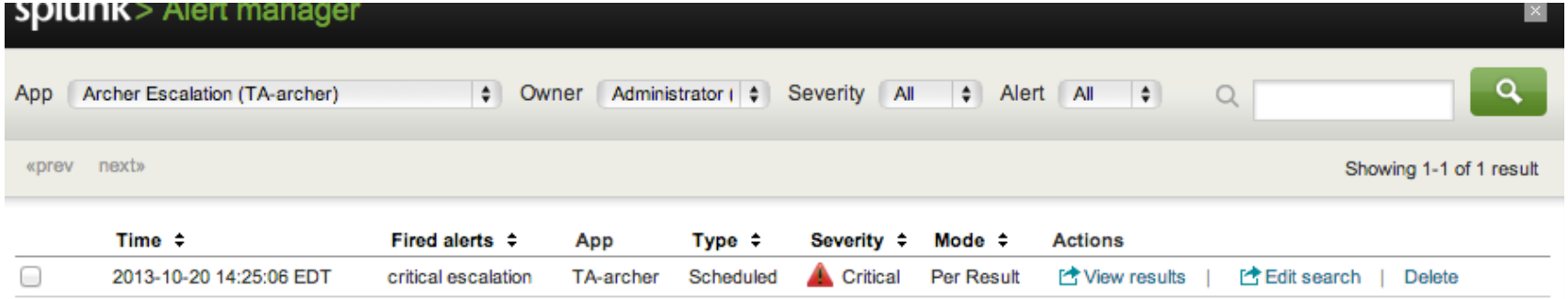
security_domain
severity
rule_name
description
rule_title
rule_description
drilldown_name
drilldown_search
default_status
default_owner

Getting Data to Archer

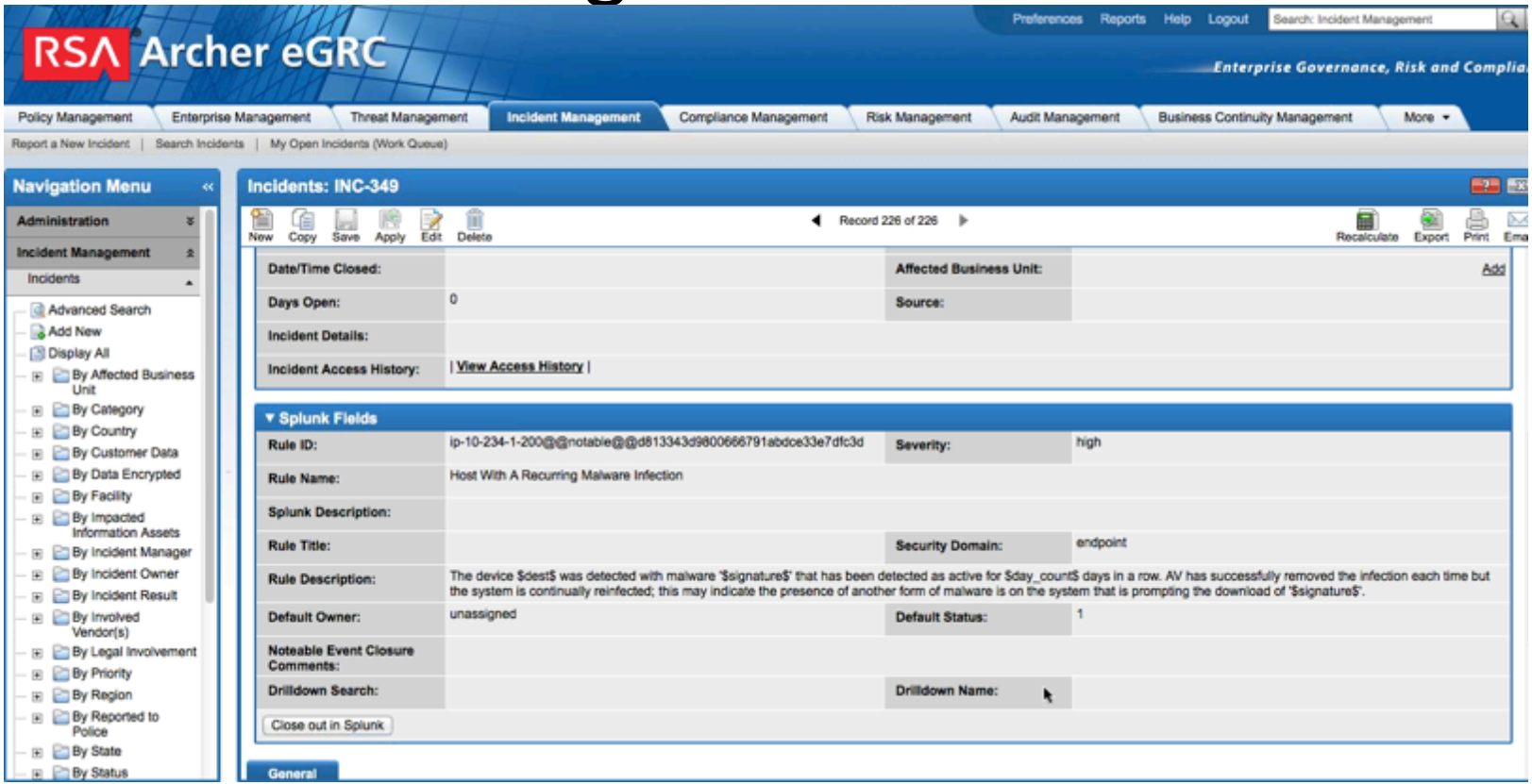


Getting Data to Archer

- Archer fields mapped to Splunk Notable Events field in python SOAP script
- Splunk generates metadata events, and ‘Archer’ command, sends it to Archer via custom search in Enterprise Security.
- Workflow action to escalate a Notable Event to Archer directly
- Automated Splunk Search of the 'Notable Events' Macro every few minutes based on rule_id, event_id and urgency (for alerting if desired)



Getting Data to Archer



Closing a Notable Event from Archer

Archer dashboard object or action to close a 'Notable Event'. We use the ‘search’ REST endpoint to allow a REST call, to change a status or close a status.

This hander takes some **input and writes a properly formatted line of CSV to incident_review.csv**. incident_review.csv's header contains the following fields:

time
rule_id
Owner
Urgency
Status
Comment
user