Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach

Jim Apger | Splunk

Stuart McIntosh | American Family Insurance

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Our Speakers

JIM APGER

Staff Security Architect

Splunk

STUART MCINTOSH

Threat Intel Analyst

American Family Insurance

splunk> .conf18

Framework for this session (Agenda)

- Problem Statement
- High-Level Concepts — Jim
- Production Deployment — Stuart
- Anatomy of a Risk Rule
- Anatomy of a Risk Incident

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions	Plist Modification	Extra Window	Private Keys	System Owner/User	Windows Remote			Standard Application

splunk> .conf18

Problem Statement

Shouldn’t come as a surprise

Is Your SOC A Big Alert Pipeline?

Defining Characteristics

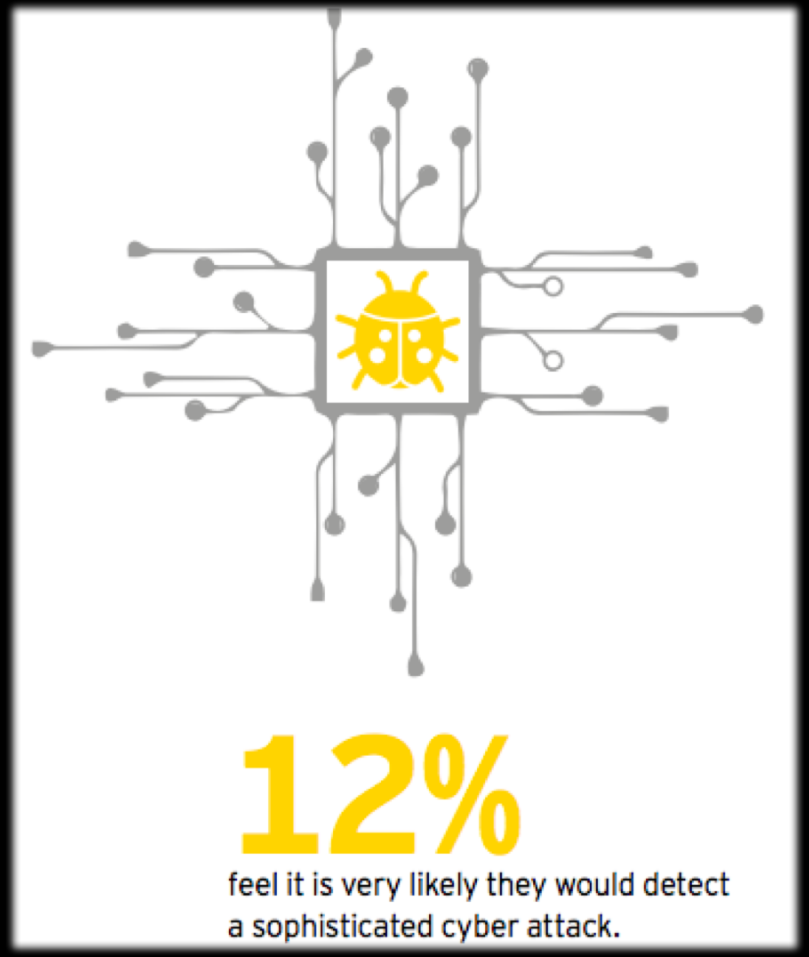
- Incidents based on narrowly defined detections lead to majority noise within the SOC
- Adding more detection mechanisms continue to overburden the SOC Analysts with more alerts
- Whitelisting as a reaction to the above results in a situational numbness (coined by Stuart)

"A perception of the SOC as a big alert pipeline is outdated and does not allow the organization to make use of more active processes such as internal TI generation and threat hunting."

Source: Gartner; How to Plan, Design, Operate and Evolve a SOC; by Anton Chuvakin and Augusto Barros; October 2016

How Big is this Problem?

We Need to Fix That!



Source : EY Global Information Security Survey 2017-2018

High-Level Concepts

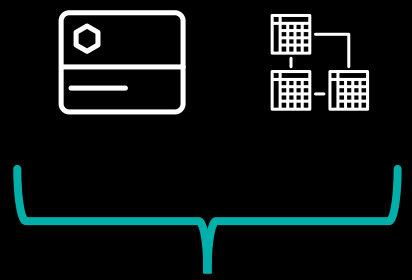
Adding a Level of Abstraction

The Risk Driven Approach

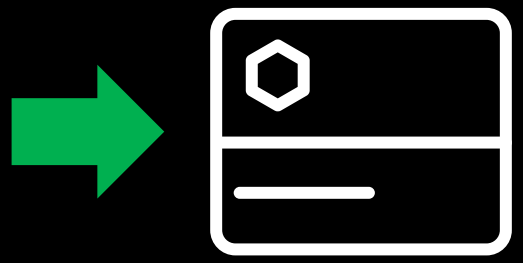
Mindset Shift: Cast a Wide Net

Risk Attribution

Using a Summary Index or ES Risk Index



RiskRule-AnomalousLogin
RiskRule-ThreatIntelIOC
RiskRule-MalwareDetection
RiskRule-IDSRecon
RiskRule-IDSAttack
RiskRule-FirstTimeSeenDomain
RiskRule-LongPowershell
RiskRule-EncryptedPowershell
RiskRule-EndPointAV
RiskRule-#10
.
.
.
.
RiskRule-#150



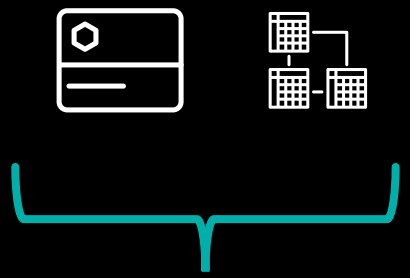
Risk Index

RiskIncidentRule-HighCompositeRiskScore
RiskIncidentRule-Multiple RiskRulesSinglePhase
RiskIncidentRule-MultipleATT&CKPhases
.
.
.
.

Risk Driven Alert
Notable Event in ES
Create/Update ticket in External system

Risk Attribution

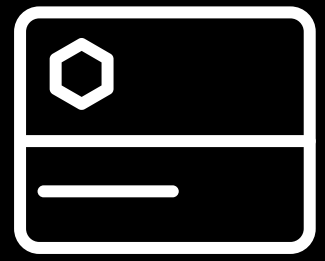
Context Written to the Risk Index



RiskRule-AnomalousLogin
RiskRule-ThreatIntelIOC
RiskRule-MalwareDetection
RiskRule-IDSRecon
RiskRule-IDSAttack
RiskRule-FirstTimeSeenDomain
RiskRule-LongPowershell
RiskRule-EncryptedPowershell
RiskRule-EndPointAV
RiskRule-#10
.
.
.
RiskRule-#150

Include in the Attribution

risk_score
risk_object
risk_object_type
rule_name (search_name)
rule_phase



Risk Index

Risk Attribution

Indicator Search Examples

- Threat Intel
  - Create attributions for matches
  - Dynamic score based on feed, asset/identity, or other context
- IDS/AV
  - Map the IDS vendor categories into ATT&CK/Kill chain phases
  - Dynamic score based on category, asset/identity, or other context
- Behavioral Anomaly attributions (SSE and ESCU)
- Outlier attributions – leveraging ML
- 3rd party Integrations to include their risk attributions, like WHOIS
- **Hint:** A very High Risk Score attribution will trigger an incident via the RiskRule-HighRiskScore rule

Risk Attribution

Indicator Search Example #1

Sets the stage for “testmode” by creating info_sid

```
|inputlookup generic_sysmon_process_launch_logs.csv |addinfo
|search [|inputlookup tools.csv | search discovery_or_attack=attack | eval filename="Image=\"*\\\\" . filename . "\"" | stats values(filename) as search | eval search=mvjoin(search, " OR ")]
|transaction host maxpause=5m
|where eventcount>=4
|fields - _raw closed_txn field_match_sum linecount
|eval risk_object=host, risk_type="system", risk_score=eventcount*5, kill_chain_phase=mvappend(kill_chain_phase,"exploit","install"), search_name="Concentration_of_Hacker_Tools_by_Filename"
|collect index=risk
```

Send the attribution to the Risk index

Direct from Splunk Security Essentials

Concentration of Hacker Tools by Filename (Assistant: Simple Search)

splunk> .conf18

Risk Attribution

Indicator Search Example #1

index=risk search_name=Concentration_of_Hacker_Tools_by_Filename

i	Time	Event
⌄	8/24/16 5:58:59.000 PM	08/24/2016 17:58:59 +0000, info_min_time=1522778400.000, info_max_time=1522867706.000, info_search_time=1522867706.802, Image="C:\\mytools\\console.exe C:\\mytools\\fgdump.exe C:\\mytools\\hping.exe C:\\mytools\\nc.exe", ParentImage="C:\\Windows\\System32\\cmd.exe", duration=190, eventcount=5, orig_host=we8105desk, info_max_time="1522867706.000", info_min_time="1522778400.000", info_search_time="1522867706.802", info_sid="1522867706.223739", kill_chain_phase="exploit install", risk_object=we8105desk, risk_score=25, risk_type=system, search_name=Concentration_of_Hacker_Tools_by_Filename, sha1="4D71EC138CC5921F7074D4413DB7CF52A0A56504 BC8F700316EF635AAF2431A1D3A310D017A2890B C5E19C02A9A1362C67EA87C1E049CE9056425788 DAFDBAEBE3B8D66DBEFA8D86C5DD7E436892759F"

Event Actions

Type	Field	Value	Actions
Selected	host	bots2017	
	search_name	Concentration_of_Hacker_Tools_by_Filename	
	source	/opt/splunk/var/spool/splunk/a293e0cb1dec36c4_events.stash_new	
	sourcetype	stash	
Event	Image	C:\mytools\console.exe C:\mytools\fgdump.exe C:\mytools\hping.exe C:\mytools\nc.exe	
	ParentImage	C:\Windows\System32\cmd.exe	
	duration	190	
	eventcount	5	
	info_max_time	1522867706.000	
		1522867706.000	
	info_min_time	1522778400.000	
		1522778400.000	
	info_search_time	1522867706.802	
		1522867706.802	
	info_sid	1522867706.223739	
	kill_chain_phase	exploit install	
	orig_host	we8105desk	
	risk_object	we8105desk	
	risk_score	25	
	risk_type	system	
	sha1	4D71EC138CC5921F7074D4413DB7CF52A0A56504 BC8F700316EF635AAF2431A1D3A310D017A2890B C5E19C02A9A1362C67EA87C1E049CE9056425788 DAFDBAEBE3B8D66DBEF A8D86C5DD7E436892759F	
Time	_time	2016-08-24T17:58:59.000+00:00	
Default	index	risk	
	linecount	2	

Direct from Splunk Security Essentials

Concentration of Hacker Tools by Filename (Assistant: Simple Search)

splunk> .conf18

Risk Attribution

Results: Indicator Search Example #2

```
|inputlookup Anonymized_Email_Logs.csv |addinfo
|stats count by Sender
|rex field=Sender "\@(?<domain_detected>.*)"
|stats sum(count) as count by domain_detected
|eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND domain_detected!="mycompanylovestheenvironment.com")
|eval list="mozilla"
|`ut_parse_extended(domain_detected, list)`
|foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<<FIELD>>' . "." . ut_tld)]
|fields orig_domain domain_detected ut_domain count
|eval word1=mvappend(domain_detected, ut_domain), word2 = mvappend("mycompany.com", "company.com", "mycompanylovestheenvironment.com")
|lookup ut_levenshtein_lookup word1 word2
|eval ut_levenshtein= min(ut_levenshtein)
|where ut_levenshtein < 3
|fields - domain_detected ut_domain
|rename orig_domain as top_level_domain_in_incoming_email word1 as domain_names_analyzed word2 as company_domains_used count as num_occurrences ut_levenshtein
    as Levenshtein_Similarity_Score
|eval risk_object=top_level_domain_in_incoming_email, risk_object_type="other", risk_score=num_occurrences*5, kill_chain_phase=mvappend(kill_chain_phase,"deliver")
    , search_name="Emails_with_Lookalike_Domains"
|collect index=risk
```

Direct from Splunk Security Essentials

Emails with Lookalike Domains (Assistant: Simple Search)

splunk> .conf18

Risk Attribution

Indicator Search Example #2

index=risk search_name=Concentration_of_Hacker_Tools_by_Filename

i	Time	Event
⌄	8/24/16 5:58:59.000 PM	08/24/2016 17:58:59 +0000, info_min_time=1522778400.000, info_max_time=1522867706.000, info_search_time=1522867706.802, Image="C:\\mytools\\console.exe C:\\mytools\\fgdump.exe C:\\mytools\\hping.exe C:\\mytools\\nc.exe", ParentImage="C:\\Windows\\System32\\cmd.exe", duration=190, eventcount=5, orig_host=we8105desk, info_max_time="1522867706.000", info_min_time="1522778400.000", info_search_time="1522867706.802", info_sid="1522867706.223739", kill_chain_phase="exploit install", risk_object=we8105desk, risk_score=25, risk_type=system, search_name=Concentration_of_Hacker_Tools_by_Filename, sha1="4D71EC138CC5921F7074D4413DB7CF52A0A56504 BC8F700316EF635AAF2431A1D3A310D017A2890B C5E19C02A9A1362C67EA87C1E049CE9056425788 DAFDBAEBE3B8D66DBEFA8D86C5DD7E436892759F"

Event Actions

Type	Field	Value	Actions
Selected	host	bots2017	
	search_name	Concentration_of_Hacker_Tools_by_Filename	
	source	/opt/splunk/var/spool/splunk/a293e0cb1dec36c4_events.stash_new	
	sourcetype	stash	
Event	Image	C:\mytools\console.exe C:\mytools\fgdump.exe C:\mytools\hping.exe C:\mytools\nc.exe	
	ParentImage	C:\Windows\System32\cmd.exe	
	duration	190	
	eventcount	5	
	info_max_time	1522867706.000	
		1522867706.000	
	info_min_time	1522778400.000	
		1522778400.000	
	info_search_time	1522867706.802	
		1522867706.802	
	info_sid	1522867706.223739	
	kill_chain_phase	exploit install	
	orig_host	we8105desk	
	risk_object	we8105desk	
	risk_score	25	
	risk_type	system	
	sha1	4D71EC138CC5921F7074D4413DB7CF52A0A56504 BC8F700316EF635AAF2431A1D3A310D017A2890B C5E19C02A9A1362C67EA87C1E049CE9056425788 DAFDBAEBE3B8D66DBEF A8D86C5DD7E436892759F	
Time	_time	2016-08-24T17:58:59.000+00:00	
Default	index	risk	
	linecount	2	

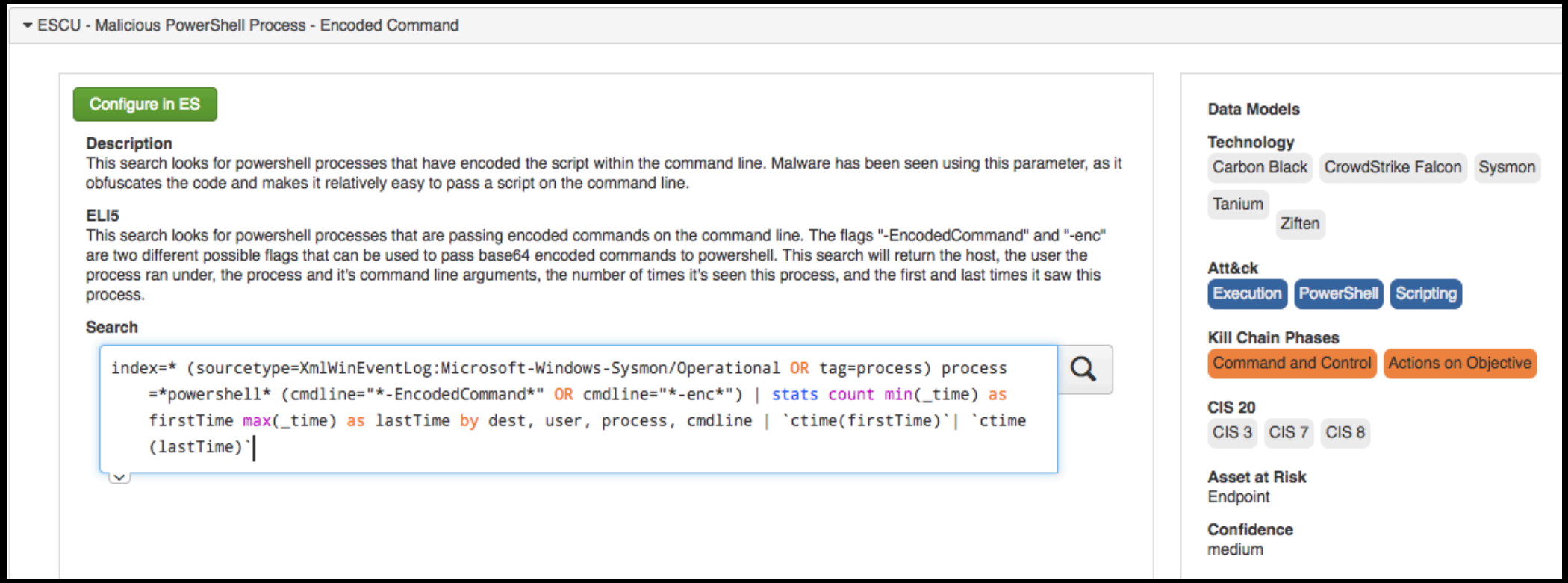
Direct from Splunk Security Essentials

Concentration of Hacker Tools by Filename (Assistant: Simple Search)

splunk> .conf18

Risk Attribution

Indicator Search Example #3



Append to the above search:

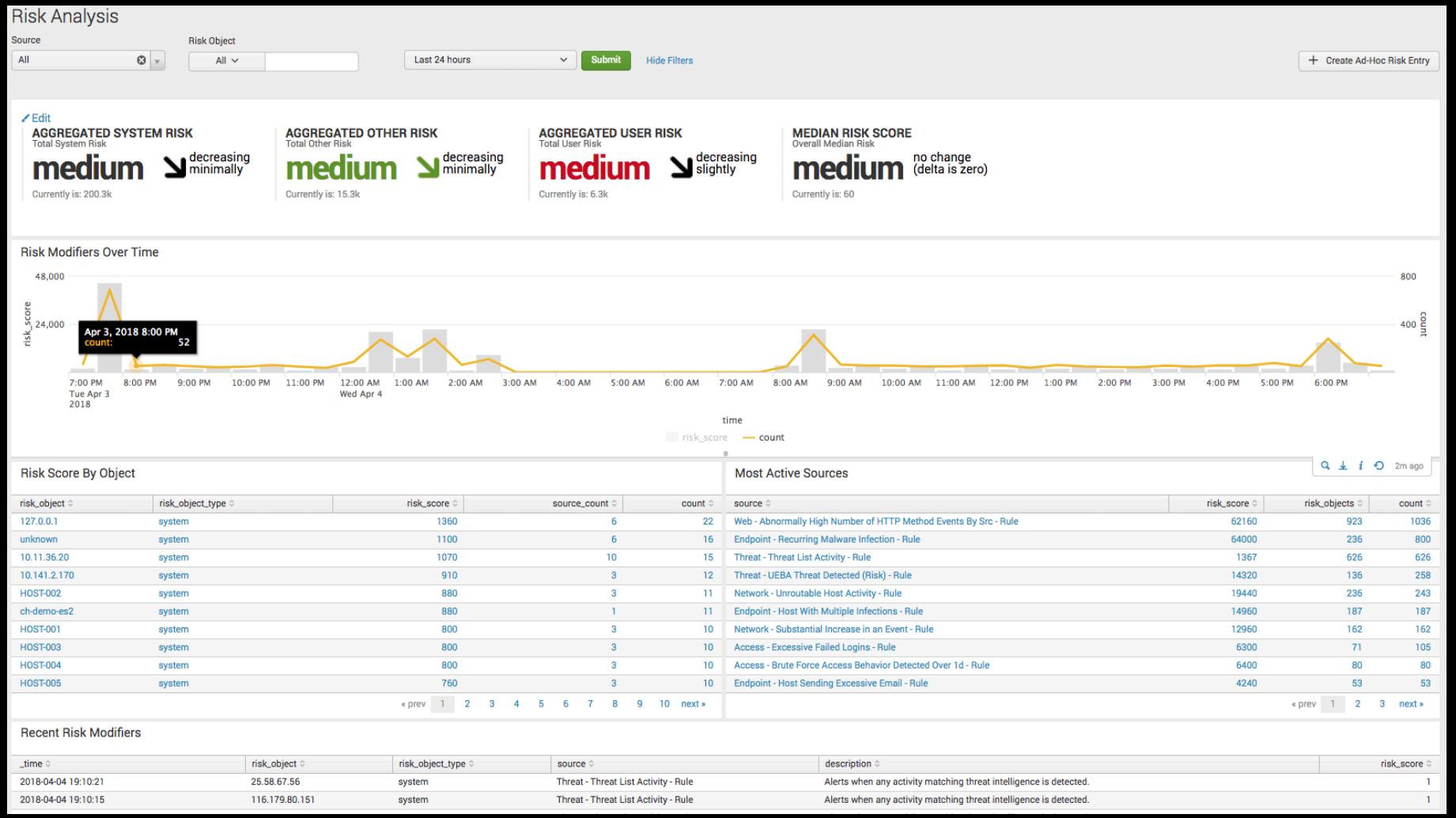
```
|eval risk_object=host,
     risk_object_type="system",
     risk_score=count*5,
     kill_chain_phase=mvappend("CC","ActOnObjective"),
     search_name="Malicious PowerShell Process - Encoded Command"
|collect index=risk
```

Direct from ES Content Updates
Malicious PowerShell

splunk> .conf18

Risk Attribution

Risk/Behavior Based View Across the Org

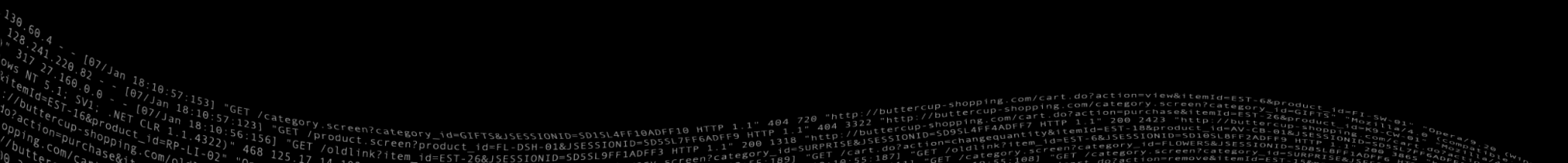


splunk> .conf18

Risk Driven Alerting Examples

Create a Risk Driven Alert by directly querying the risk index for:

- Static risk threshold crossed
  - Great for single high risk rules
  - Detect low and slow
- Multiple phases/techniques observed
- Detect an anomalous score move within a peer group (asset/identity)
- Sequence or combination of attributions or phases



Risk Driven Alert

Multiple Phases Example

New Search

```
index=risk | rex mode=sed field=kill_chain_phase "s/\n/,/g"|makemv delim="," kill_chain_phase
|stats sum(risk_score) as risk_score_aggregate
    values(search_name) as search_name
    values(risk_object_type) as risk_objects_type
    values(kill_chain_phase) as kill_chain_phase
    by risk_object
|where mvcount(kill_chain_phase)>=3 AND mvcount(search_name)>=2
```

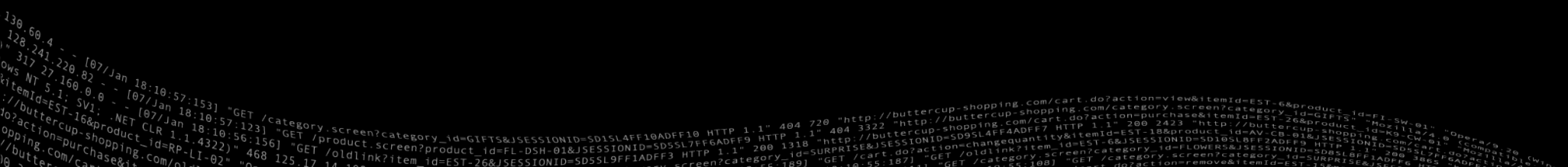
We are looking for any object with risk attributions spanning more than 2 kill chain phases and more than 1 risk rule.

✓ 25 events (before 4/5/18 12:59:59.000 PM) No Event Sampling

Events | Patterns | Statistics (1) | Visualization

20 Per Page | Format | Preview

risk_object	risk_score_aggregate	search_name	risk_objects_type	kill_chain_phase
we8105desk	275	Concentration_of_Hacker_Tools_by_Filename Short_Lived_Admin_Accounts	system	ActOnObjective CC exploit install



splunk> .conf18

Production Deployment

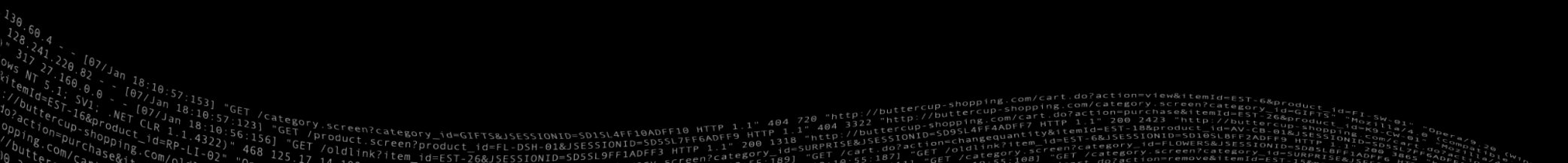
American Family Insurance

splunk> .conf18

Environment Overview

What we are working with

- Organization
  - 25,000 Endpoints
  - 20,000 Users
  - 4 SOC Analysts
  - 4 Threat Intel Focused Employees
- Data Sources
  - Network IDS
  - Host IDS
  - Antivirus
  - Email
  - Web Proxy
  - Firewall
  - Vulnerability Scanning
  - Active Directory
  - VPN

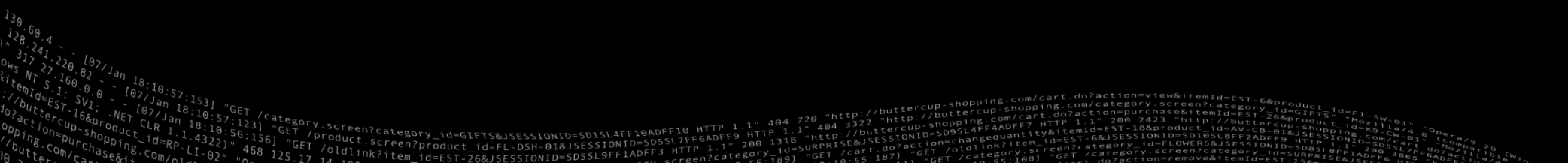


splunk> .conf18

Why Now?

The conditions that lead to risk based

- Traditional detection to alert plateau
  - New detections meant more alerts on an already taxed staff
  - Whitelist everything leading to a numbness
- Pentest with 1 alert
  - Large motivator
  - Thought we rocked at security, found out we don’t



Initial Success

Big wins for reducing alert fatigue

Expiration Based Whitelisting

Developed whitelists for each notable with automatic expirations

Allows False Positive signatures to catch up

Prevents re-investigating in known good

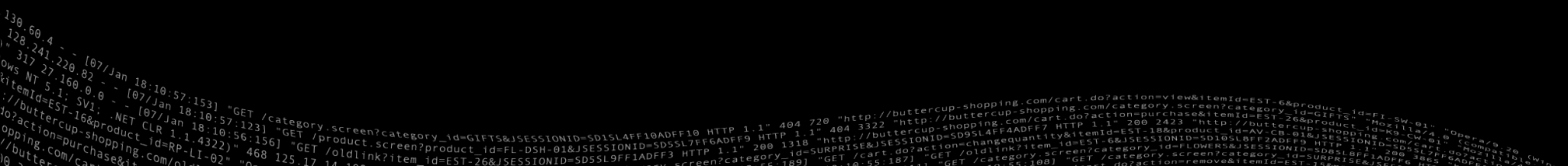
60% reduction in the volume of notables/alerts

Phishing Prevention

Custom email behavior monitoring for proactive identification of potential phishes

Paired with improved controls and script to remove emails from mailboxes

Reduced click-rate of phishing from 40% to <5% with no user training



Anatomy of a Risk Rule

American Family Insurance

splunk> .conf18

Risk Attribution

Components of Risk Attribution

Once an attack behavior is identified it is important to identify the objects involved and assign the risk. This is macro driven to allow ease of support and allow quicker adjustments.

The components of assigning risk are:

- Identify Risk Modifiers
- Establish Risk Score
  - Leverages risk modifiers, confidence in the behavior and impact of the behavior
- Identify Attack Phase of the Behavior

```
| eval rule_impact="Low"
| eval rule_confidence="Low"
| eval rule_phases="initial_access"
| eval rule_name="Potential New Sender Phish - Email"

| `risk_modifier_user(dest_user)`
| `risk_score(rule_impact,rule_confidence,risk_modifier_count)`

| eval risk_object_type="user"
| `risk_attribution(dest_user,risk_object_type,risk_score,rule_phases,rule_name)`
```

splunk> .conf18

Risk Attribution

Risk Modifiers

Risk Modifiers are aspects to a user or system that makes them more critical in the environment. These only apply to internal objects and the sum total from a user and system is then used in the scoring.

Users – Service Account, Privileged Account, Executive, Watchlist*

* populated by integration with other outside processes like terminations

Systems – Privileged System, Critical System, Critical Vulnerabilities

Risk Attribution

Risk Scoring

Risk Scores use the risk modifier count as well as a confidence and impact ratings

Confidence – the fidelity of a true positive with an attack behavior

- Low – less confident, multiple false positives mixed in
- Medium – Some false positives may occur but not regularly
- High – All results are true positive for a specific attack behavior

Impact – how much will this behavior impact the environment

- Info, Low, Medium, High, Critical

Risk Attribution

Pulling it all together

Here comes math…

Low 30%
Medium 60%
High 100%

(Impact * Confidence) * ((Modifiers * .25) + 1) = Net Risk Score

Info 20
Low 40
Medium 60
High 80
Critical 100

0 – N
(Privileged user and system would be 2)

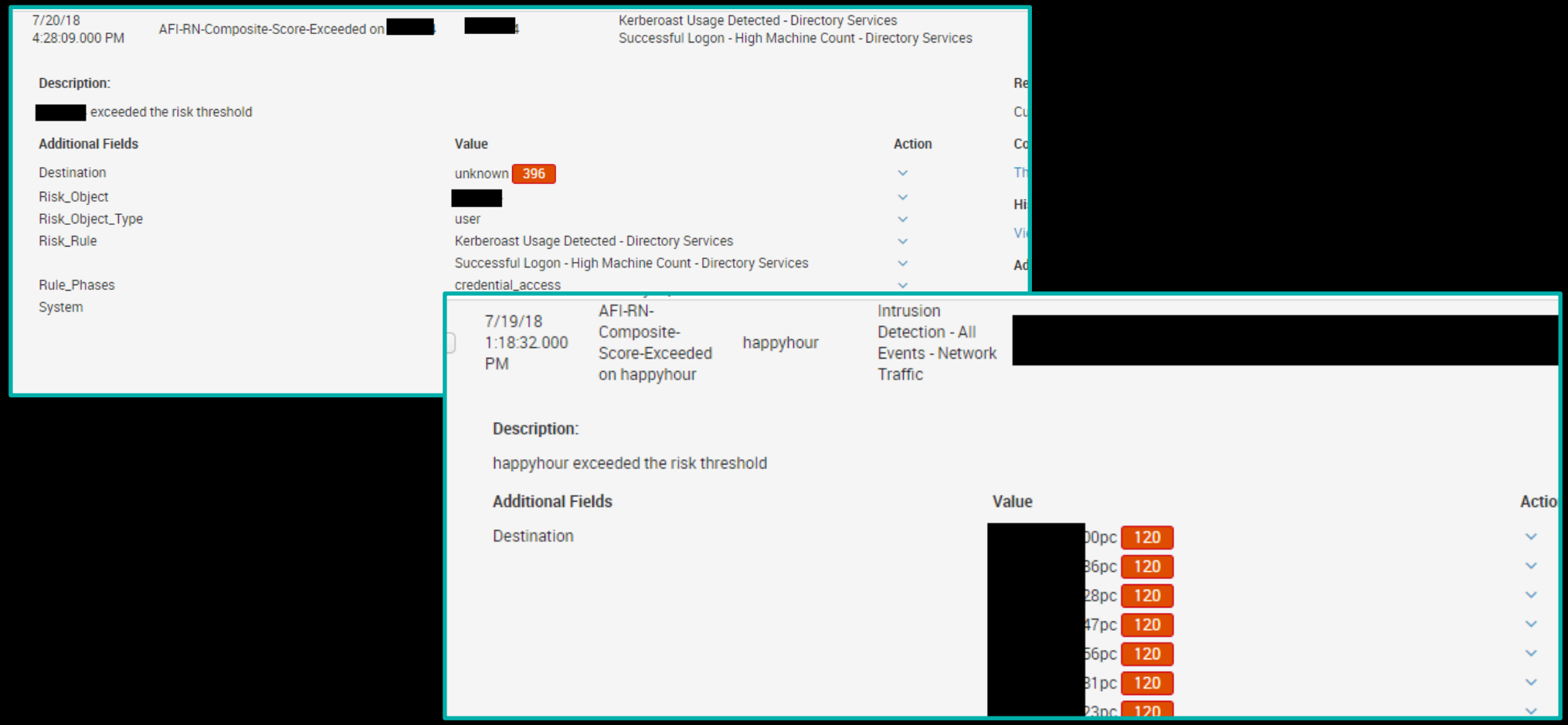
Anatomy of a Risk Incident

American Family Insurance

splunk> .conf18

Anatomy of an Incident

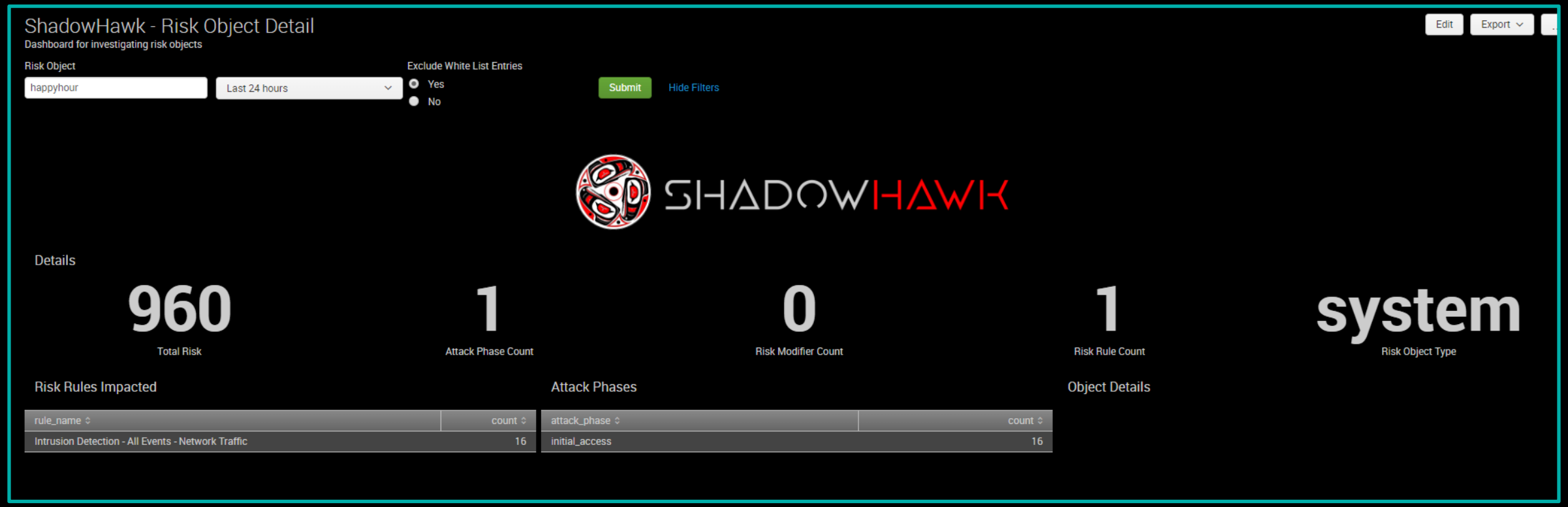
Risk Notables



splunk> .conf18

Anatomy of an Incident

Risk Object Detail



Anatomy of an Incident

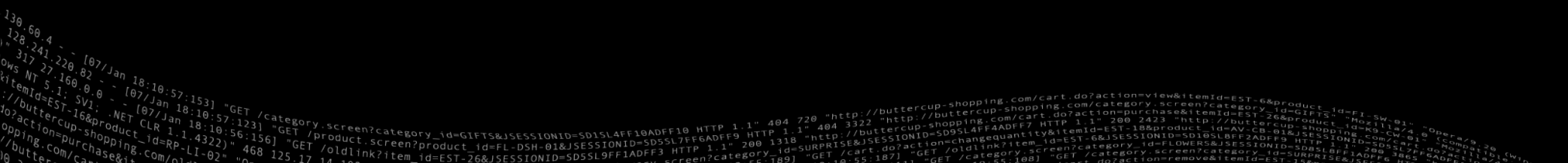
Risk Object Detail

Type	Field	Value	Actions
Selected	host	splunk-sec	
	source	Threat - AFI-RR-IntrusionDetection-AllEvents-NetworkTraffic - Rule	
	sourcetype	stash	
Event	attack_phase	initial_access	
	category	OS Attack	
	dest_system	[redacted]5pc	
	direction	inbound	
	info_max_time	1532023200.000	
	info_min_time	1532019600.000	
	info_search_time	1532024054.631	
	process	SYSTEM	
	risk_modifier_count	0	
	risk_object	happyhour	
	risk_object_type	system	
	risk_score	60	
	rule_confidence	High	
	rule_impact	Medium	
	rule_name	Intrusion Detection - All Events - Network Traffic	
	rule_phases	initial_access	
	search_name	Threat - AFI-RR-IntrusionDetection-AllEvents-NetworkTraffic - Rule	
		Intrusion Detection - All Events - Network Traffic	
	search_now	1532023800.000	
	signature	OS Attack: Microsoft SMB MS17-010 Disclosure Attempt	
	src_system	happyhour	

Lessons Learned

What happened along the journey

- Mindshift
  - Hard to not want to search every 5 minutes
  - Easier for those not in a SOC to make the jump mentally
- Leadership Support
  - Need the time to focus and develop
  - Identify the key business drivers to help them buy in

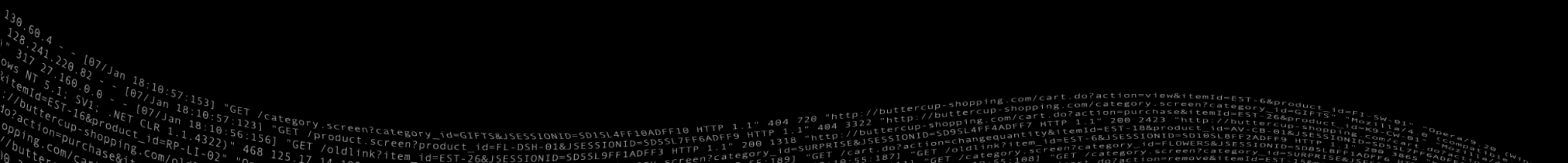


Lessons Learned

What happened along the journey

- What to do with a Risk Notable
  - Need details but everything is summarized
  - How to jump to detail efficiently and accurately
- Fits all SOCs, even small
  - Allows you to prioritize and alert more effectively
  - Reduced noise means more time for other efforts

Towards the end of the effort we realized we made an automated SOC analyst and built that first level decision making into it



What's Next

How to continue maturing this approach

- Pre-Alert and Post-Alert Automation
  - Enabling system isolation if concerned
  - Automatic Packet captures
  - Downgrading user access
- Previous Notables as Enrichment
  - Adjust urgency by sources, modifiers, and score
  - Determine to alert based on other notables
  - Tagging based on behavior patterns and changes to risk
- Ability vs. Capacity
  - Continued Iteration on Ability to detect threats with SOC Capacity to respond

High-Level Takeaways

1. An approach does exist that may provide relief from alert fatigue but it requires commitment from the Security group and support from Leadership

2. It's possible, even for a small SOC, to make a soft transition to this approach

3. Risk scoring becomes extremely important and will require ongoing maintenance but scales the overall effort more effectively

4. Aligning the MITRE ATT&CK matrix and techniques with this approach provides a means for quantifying your security posture and for justifying new data sources.

Q&A

Jim Apger | Splunk

Stuart McIntosh | American Family Insurance

Thank You

Don't forget to rate this session in the .conf18 mobile app

Other Related Approaches

splunk> .conf2017

The Art of Detection

Using Splunk Enterprise Security

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

September 27, 2017 | Washington, DC

Microsoft | TechNet

Search

Securing Office 365

Official blog of the Office 365 Security team

Defending Office 365 with Graph Analytics

Rate this article

Matt Swann - MSFT March 13, 2017

Share 9 232 in 0 0

In Office 365, we are continually improving the detection and response systems that safeguard your data. We gather many terabytes of telemetry from our service infrastructure each day and apply real-time and batch analytics to rapidly detect unauthorized access.

The same engineers who design and operate the Office 365 service also analyze and act on the output of our intrusion detection system. The context we have about the design of Office 365 allows us to build highly-sensitive detections while differentiating between legitimate service behavior and suspicious activity.

As we have scaled up our telemetry and analysis infrastructure, we have also innovated in how we interact with the results of our detection system. One recent development is the use of graphs for correlation and visualization.

Prior to our graph approach, we represented detection results as a set of tickets in a queue for manual review. We found that it was difficult to group related activity together, and occasional bursts of benign activity would overwhelm the system with irrelevant results.

Representing detection results as graphs has enabled us to

- evaluate intrusion detection results in context with related activity,
- incorporate lower-fidelity indicators without overwhelming us with benign results, and
- determine with greater fidelity when datacenter activity is likely to represent an intrusion.

Representing activity as graphs

splunk> .conf18