A Framework For Developing And Operationalizing Security Use Cases

Ryan Faircloth

"Professional" Security Consultant, 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.

Outline

- Intro
- Motivators/requirements
- Framework/approach
- Goal setting, prioritizing
- Operationalizing
- Example use case
- How to work with us

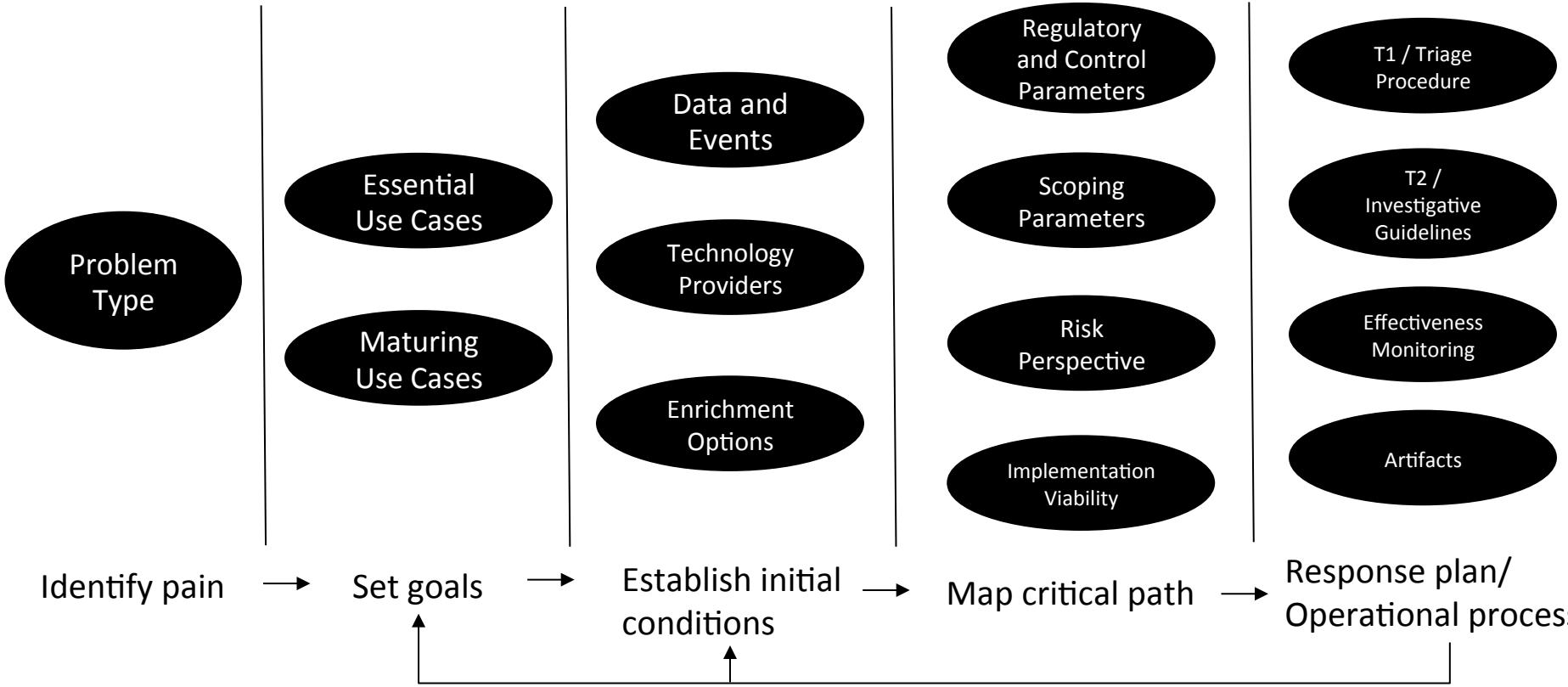
Short Intro

- Splunker 2 years
- Information Security focused “day job” over 5 years
- Doing security work “don’t get hacked” over a decade, if we do get hacked they don’t get anything important

Business Motivators

- Compliance
- Security Visibility
- Peer Adoption
- Process Effectiveness
- Tactical Threat
- Secure Configuration Management
- Special Requests
- Product Adoption

Framework/Approach



Use Case Development

- Communicates progress toward agreed goals
- Holds accountable the teams creating events for analysis
- Justifies the value of work
- Validates the investment in technology?
- Links events of interest to concrete concepts, spend less time explaining why something is important

Everyone Knows Your Goals

- Maybe. Agreeing to the words and the definitions are not the same thing. You say - they heard – but confusion follows
- Stakeholders have different views
- Define the goal and the measurement up front

Example Goal And Measure

- Goal: reduce the risk of loss of data or operational availability due to malware operating in the environment

- Measure Identification of patient zero for new malware strains, allowing analysts to identify opportunities for prevention through the application of enhancements to preventive controls. (trackable)

- Test monitor for infections for signatures where outbreak occurs more than n hours after first encounter

What Are Valid Goals

- Any meaningful measure of progress towards one of the following:
- Organizational high level risk statement
- Compliance with internal or external standard by which the security program is measured or assessed, COBIT, HIPPA-HiTech, PCI, SOX etc
- Increase in the stature of the team within the organization, or increase in the reputation of the organization with its customers, vendors or peers as a competitive advantage
- Reduction in the operational expense or opportunity cost of any current process

Who Are Goal Setters

- Risk frameworks
- The Headlines
- Executive meetings at the golf course
- Keeping up with the Jones Inc.
- Conferences
- Auditors (based on standards, or Google searching)
- Security Concerns

Lets Set Some Goals

- Show progress in the reduction of risk or impact
- RV1-AbuseofAccess — Abuse of access addressed the risk of authorized or entitled access in such a way as to cause harm to the organization
- RV2-Access — Access addressed the risk of unauthorized access in such a way as to cause harm to the organization
- RV3-MaliciousCode — Malicious code addressed the risk of processes used against the organization, these risks include "malware" as well as authorized software used for malicious intent.
- RV4-ScanProbe — Risk of activities that could discover a weakness in the organizations systems, controls, or configuration that could latter be used to harm the organization
- RV5-DenialofService — Risk of denial of service includes such concerns as load based and destructive change to the infrastructure.
- RV6-Misconfiguration — Modification of a system that results in a misconfiguration defined as insecure or unreliable impacting the compliance, security, or availability of the system. Such configuration may increase the likelihood or impact of other adverse events.

Or Maybe These

- In the constantly evolving threat landscape organizations often must set aside strategic plans and react to specific threats. Tactical threat motivations support the urgent on boarding of missing critical data sources
- Problems Types
- PRT05-TacticalThreat-InsiderThreat
- PRT05-TacticalThreat-Ransomeware
- PRT05-TacticalThreat-SpearphishingCampaign

Or These

- Lets be compliant
- SOX
- PCI
- HIPPA
- CORBIT

Recognizing Our Goal Setters

We may not like that external pressures set our priorities, you may not have this problem but this is a fact of life in most organizations working with these pressures to gain momentum will enable more success in the short and long term.

How To Define ”Progress”

- That is a really good question, and it must be asked
- Some solutions can satisfy more than one rubric, many times just one but that’s not bad

- Did we improve the efficiency of the operation by reducing the time required, or improving accuracy
- Did we create new knowledge that can be used to inform our future decisions
- Did we identify an occurrence of an adverse event? Is it working

How To Prioritize Problem Types

- Go through each problem type
- Extract out the essential use cases
- What data and events do you need
- What enrichment options do you have
- Score the rest based on:
  - Adoption phase
  - Severity
  - Fidelity
  - Load factor
  - Etc.
- Map out fastest time to impact
- Define process / teams

Does It Work?

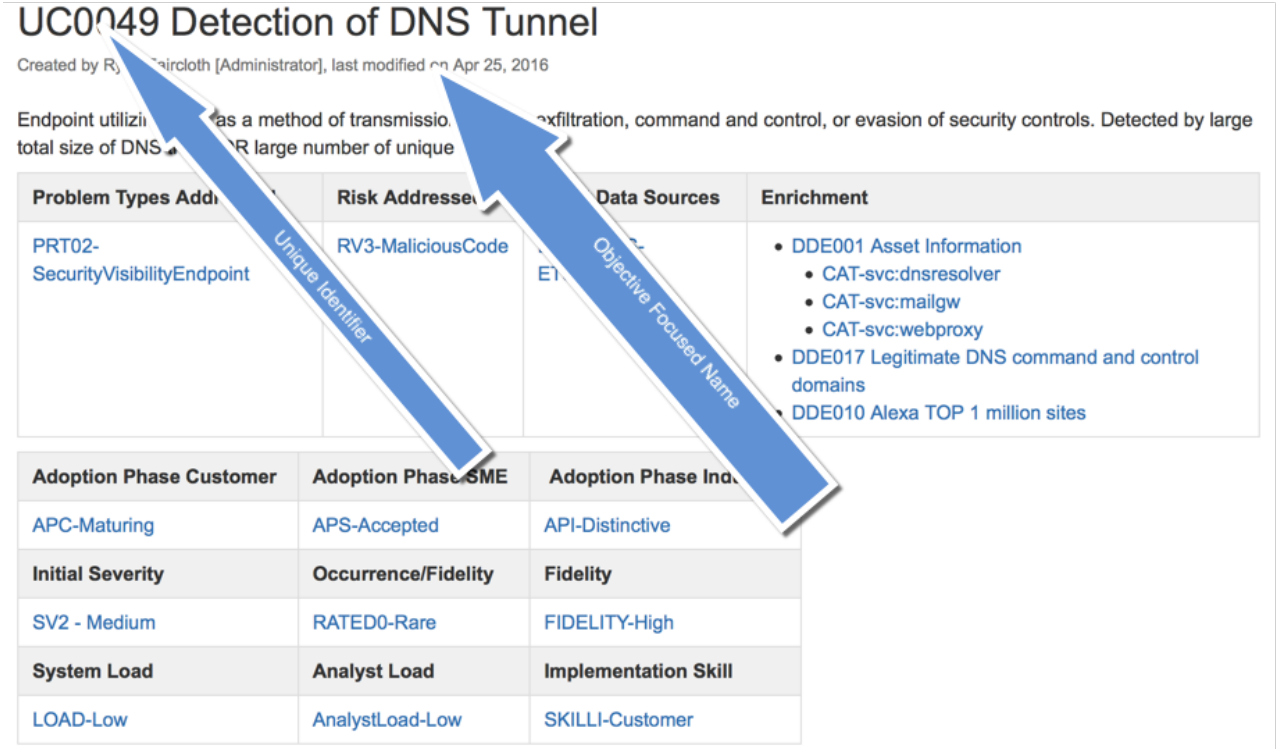
- Does the approach produce results
- October 2015 Documented the first 20 risk mitigation Focused
- October 2016…

110
Use Cases

By The Numbers It Does

Adoption Motivations	Defined use cases	Taxonomy	Consumer Friendly	Extensible	Adoptable	Opposition
• Proactive: • Business Problems • Business Risks • Compliance • Expectations • Reactive: • Technology Driven • Expectations	• Single definition of a use case for multiple audiences	• Structured approach • Defined terms	• Technician Level • Manager Level • Director Level • Executive Level • Sales Engineer Level • Account Manager Level	• Started with use cases for ES • Added use cases for PCI • Structured to embrace ITSI and ITOA	• Code provided for ten use cases • Structured for Content Pack Creation	• Built on the concepts of previous efforts
7	**85**	**20**	**7**	**∞**	**10**	**0**

Define A Use Case – ID + Name



Define A Use Case – Describe What This Will Do

UC0049 Detection of DNS Tunnel

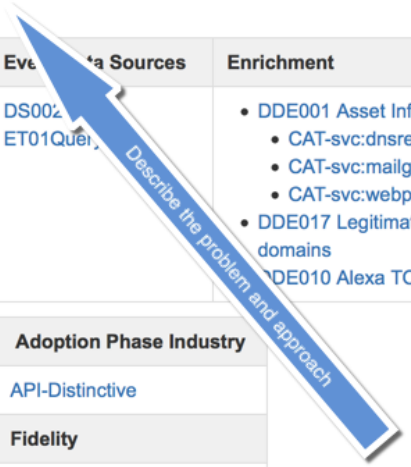
Created by Ryan Faircloth [Administrator], last modified on Apr 25, 2016

Endpoint utilizing DNS as a method of transmission for data exfiltration, command and control, or evasion of security controls. Detected by large total size of DNS traffic OR large number of unique queries.

Problem Types Addressed	Risk Addressed	Eve…ta Sources	Enrichment

PRT02-SecurityVisibilityEndpoint	RV3-MaliciousCode	DS002… ET01Quer…	• DDE001 Asset Information
			  • CAT-svc:dnsresolver
			  • CAT-svc:mailgw
			  • CAT-svc:webproxy
			• DDE017 Legitimate DNS command and control domains
			• …DE010 Alexa TOP 1 million sites

Adoption Phase Customer	Adoption Phase SME	Adoption Phase Industry
APC-Maturing	APS-Accepted	API-Distinctive
Initial Severity	**Occurrence/Fidelity**	**Fidelity**
SV2 - Medium	RATED0-Rare	FIDELITY-High
System Load	**Analyst Load**	**Implementation Skill**
LOAD-Low	AnalystLoad-Low	SKILLI-Customer



Define A Use Case – Attach Business Impact

UC0049 Detection of DNS Tunnel

Created by Ryan Faircloth [Administrator], last modified on Apr 25, 2016

Endpoint utilizing DNS as a method of transmission for data exfiltration, command and control, or evasion of security controls. Detected by large total size of DNS traffic OR large number of unique queries.

Problem Types Addressed	Risk Addressed	Event Data Sources	Enrichment

PRT02-SecurityVisibilityEndpoint	RV3-MaliciousCode	DS002DNS-ET01Query	• DDE001 Asset Information
			  • CAT-svc:dnsresolver
			  • CAT-svc:mailgw
			  • CAT-svc:webproxy
			• DDE017 Legitimate DNS command and control domains
			• DDE010 Alexa TOP 1 million sites

Highlight Recognized Pain

Adoption Phase Customer	Adoption Phase SME	Adoption Phase Industry
APC-Maturing	APS-Accepted	API-Distinctive
Initial Severity	**Occurrence/Fidelity**	**Fidelity**
SV2 - Medium	RATED0-Rare	FIDELITY-High
System Load	**Analyst Load**	**Implementation Skill**
LOAD-Low	AnalystLoad-Low	SKILLI-Customer

Define A Use Case
What Is Required Data Is Enrichment

UC0049 Detection of DNS Tunnel

Created by Ryan Faircloth [Administrator], last modified on Apr 25, 2016

Identify Data Sources and Enrichment

Endpoint utilizing DNS as a method of transmission for data exfiltration, co... Detected by large total size of DNS traffic OR large number of unique queries.

Problem Types Addressed	Risk Addressed	Event Data Sources	Enrichment

PRT02-SecurityVisibilityEndpoint	RV3-MaliciousCode	DS002DNS-ET01Query	• DDE001 Asset Information
			  • CAT-svc:dnsresolver
			  • CAT-svc:mailgw
			  • CAT-svc:webproxy
			• DDE017 Legitimate DNS command and control domains
			• DDE010 Alexa TOP 1 million sites

Adoption Phase Customer	Adoption Phase SME	Adoption Phase Industry
APC-Maturing	APS-Accepted	API-Distinctive
Initial Severity	**Occurrence/Fidelity**	**Fidelity**
SV2 - Medium	RATED0-Rare	FIDELITY-High
System Load	**Analyst Load**	**Implementation Skill**
LOAD-Low	AnalystLoad-Low	SKILLI-Customer

Define A Use Case – Qualify The Use Case

UC0049 Detection of DNS Tunnel

Created by Ryan Faircloth [Administrator], last modified on Apr 25, 2016

Endpoint utilizing DNS as a method of transmission for data exfiltration, command and control, or evasion of security controls. Detected by large total size of DNS traffic OR large number of unique queries.

Problem Types Addressed	Risk Addressed	Event Data Sources	Enrichment

PRT02-SecurityVisibilityEndpoint	RV3-MaliciousCode	DS002DNS-ET01Query	• DDE001 Asset Information
			  • CAT-svc:dnsresolver
			  • CAT-svc:mailgw
			  • CAT-svc:webproxy
			• DDE017 Legitimate DNS command and control domains
			• DDE010 Alexa TOP 1 million sites

Adoption Phase Customer	Adoption Phase SME	Adoption Phase Industry
APC-Maturing	APS-Accepted	API-Distinctive
Initial Severity	**Occurrence/Fidelity**	**Fidelity**
SV2 - Medium	RATED0-Rare	FIDELITY-High
System Load	**Analyst Load**	**Implementation Skill**
LOAD-Low	AnalystLoad-Low	SKILLI-Customer

Provide Qualitative and Quantitative attributes

Example – Malware - Basics

- From here we start to walk through 3 levels of use cases and how to structure the concepts and scope. Monitoring can have depth and breadth
- Level Essentials monitor alerts from detections systems for things to fix/things to know
- Level Maturing monitor indicators of malware not identified by preventive systems
- Level Mature use level 1 and level 2 data to identify related malware activity not picked up by detective systems

Malware – Level 1 Use Cases
Keep An Eye On AV

- UC0028 Endpoint Multiple infections over short time (Narrative and Use Case Center)
  Multiple infections detected on the same endpoint in a short period of time could indicate the presence of a undetected loader malware component (apt).
- UC0030 Endpoint uncleaned malware detection (Narrative and Use Case Center)
  Endpoint with malware detection where anti malware product attempted to and was unable to clean, remove or quarantine.
  Problem Types Addressed Risk Addressed Event Data Sources Enrichment

Malware – Level Essentials
When The AV Misses

- UC0020 Attempted communication through external firewall not explicitly granted (Narrative and Use Case Center)
  Any attempted communication through the firewall not previously granted by ingress/egress policies could indicate either a misconfiguration (causing systems behind the firewall to be vulnerable) or malicious actions (bypassing the firewall).

Malware – Level Essentials
If Its Not Encrypted Listen To Your IDS

- UC0074 Network Intrusion Internal Network (Narrative and Use Case Center)
  IDS/IPS detecting or blocking an attack based on a known signature.

Malware – Level Essentials
Smarter Malware Uses Your Proxy

- UC0047 Communication with newly seen domain (Narrative and Use Case Center)
  Newly seen domain's may indicated interaction with risky or malicious servers. Identification of new domains via web proxy logs without other IOCs allows the analyst/threat hunter to explore the relevant data and potentially identify weaknesses
- UC0081 Communication with unestablished domain (Narrative and Use Case Center)
  Egress communication with a newly seen, newly registered, or registration date unknown domain may indicate the presence of malicious code. Assets communicating with external services excluding Alexa TOP 1M whose reputation score exceeds acceptable norms will be flagged

Malware – Level Mature
Your AV Is Talked Listen

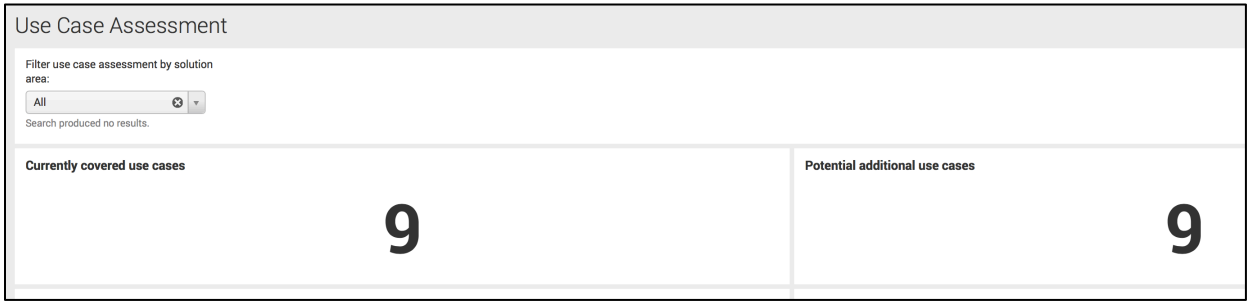
- UC0025 Endpoint Multiple devices in 48 hours in the same site (Narrative and Use Case Center)
  Multiple infected devices in the same site could indicate a successful watering hole attack. Monitor for more than 5% of the hosts in a site.
- UC0026 Endpoint Multiple devices in 48 hours in the same subnet (Narrative and Use Case Center)
  Multiple infected devices in the same subnet could indicate lateral movement of an adversary or a possible worm. Monitor for more than 5% of the host addresses on a subnet as it is not readily possible to know how many hosts are active on a subnet.
- UC0027 Endpoint Multiple devices in 48 hours owned by users in the same organizational unit (Narrative and Use Case Center)
  Multiple infected devices in the same organizational unit could indicate a successful spear phishing attack. Monitor for more than 5% of the hosts in an organizational unit.
- UC0029 Endpoint new malware detected by signature (Narrative and Use Case Center)
  When a new malware variant is detect by endpoint antivirus technology it is possible the configuration or capability of other controls are deficient. Review the sequence of events leading to the infection to determine if additional preventive measures can be put in place.

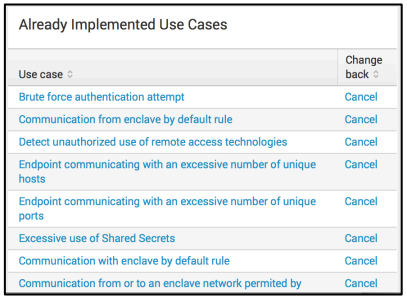
Threats – Level Mature
They Are Everywhere

- UCESS053 Threat Activity Detected Review all log sources with src and dest, IP, fqdn and email addresses for potential match on trusted threat source

How To Work With Us

- Splunk-led workshop – 3-day agenda – contact PS
  - Good for project managers, biz analyst, tech analyst/architect, sec analyst, test lead, exec sponsors, exec stakeholders / deputies, compliance analysts, internal assessors / auditors
- Splunk-led assessment – contact sales and/or PS
  - UCA tool developed by Ryan Faircloth (PS) and Erick Mechler (sales)





What Now?

Related breakout sessions and activities…

THANK YOU

splunk>