Denken wie ein Hacker: Hacker verstehen um Ihr Unternehmen besser zu schützen

mit dem MITRE ATT&CK Framework & Splunk

splunk> turn data into doing™

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Le-Khanh Au

Security Advisor

Alex Pilger

Partner Technical Manager (CISSP,GMON)

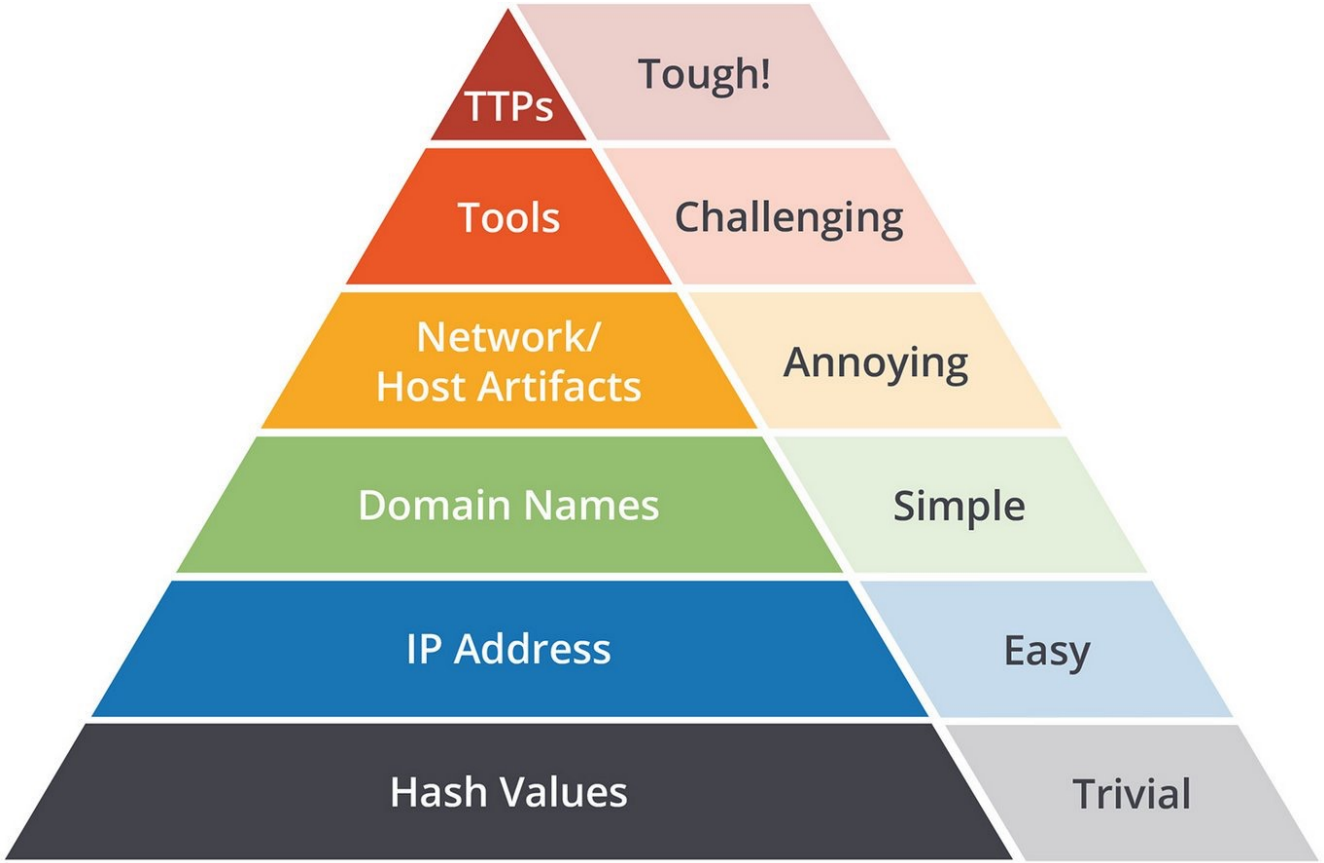
Agenda

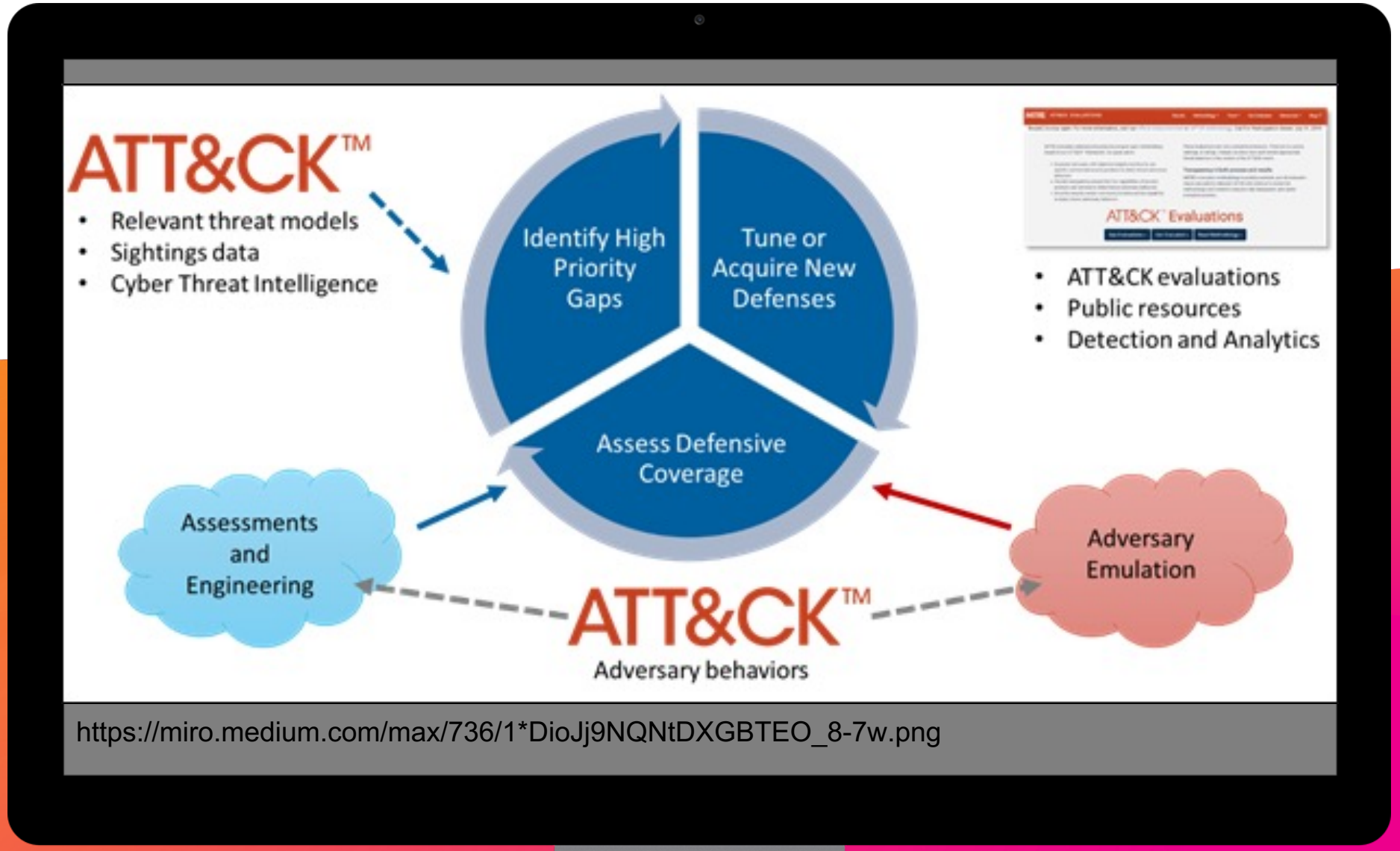
- MITRE Att@ck Framework Explained
- MITRE Att&ck operationalized in Splunk
- MITRE Att@ck beyond Simple Detections
- Wrap Up

MITRE ATT&CK explained

splunk> turn data into doing™

The Pyramid of Pain





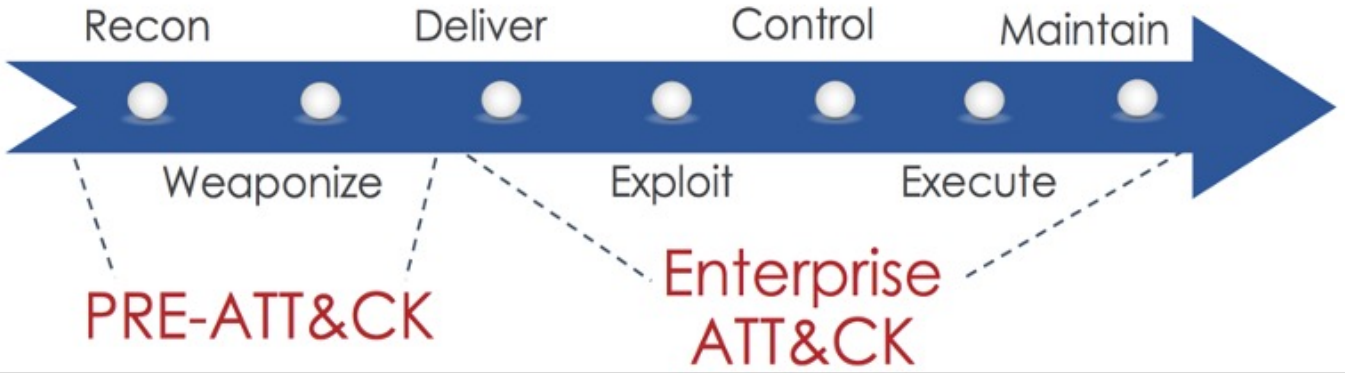
https://miro.medium.com/max/736/1*DioJj9NQNtDXGBTEO_8-7w.png

Introduction to MITRE ATT&CK™

A knowledge base of adversary behavior

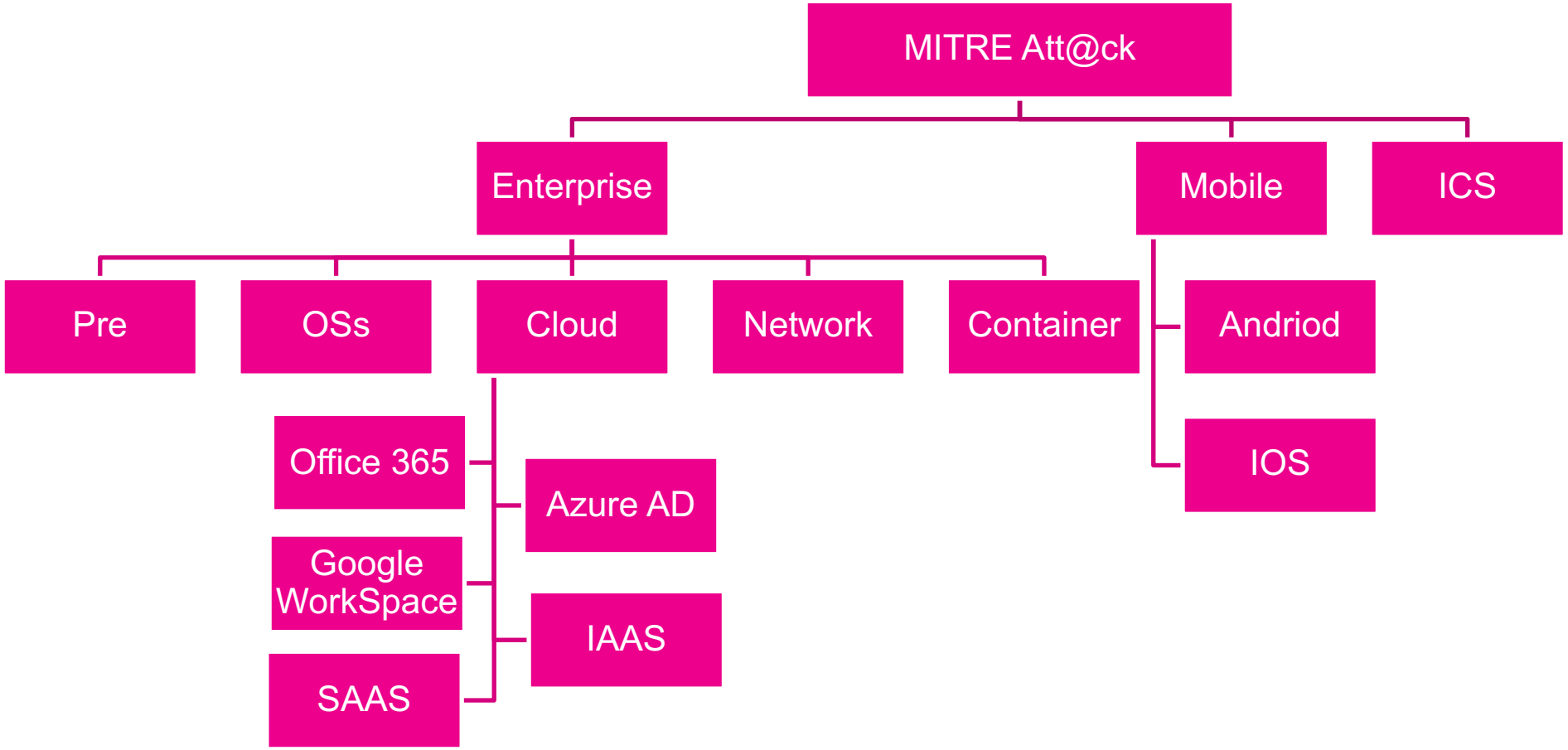
- Based on real-world observations
- Free, open, globally accessible, and community-driven
- A common language

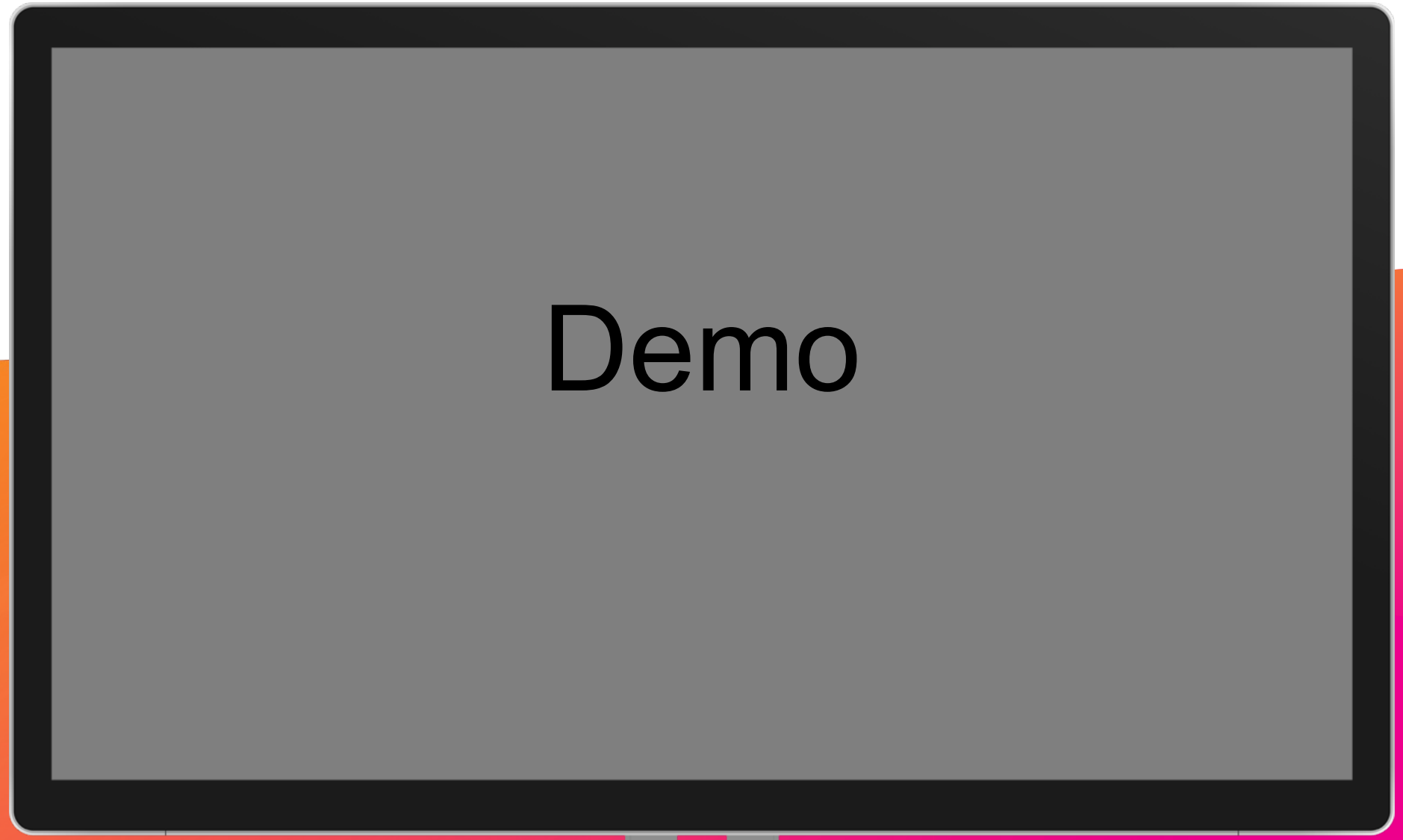
Mobile ATT&CK

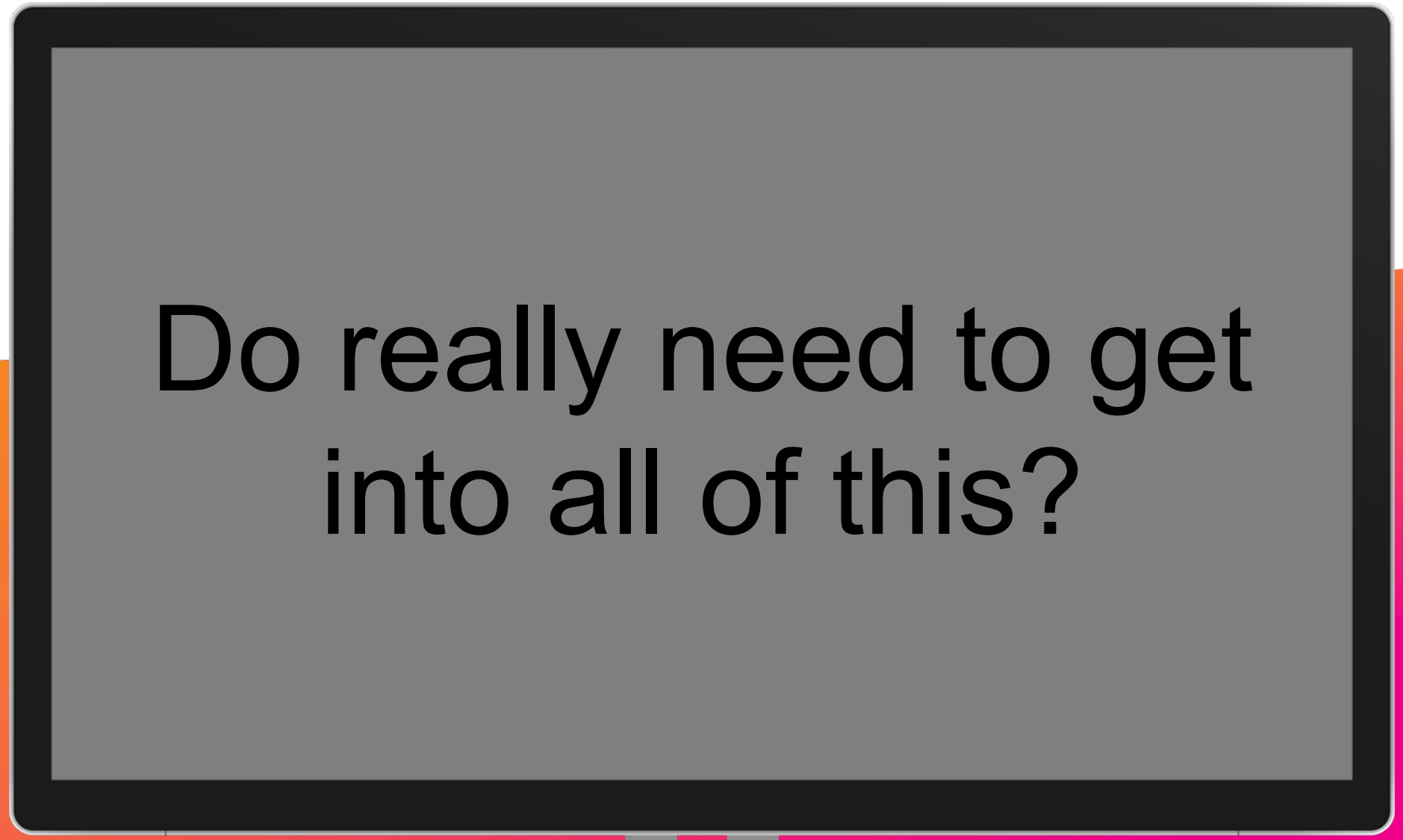


https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

What is in MITRE Att@ck Framework?







MITRE ATT&CK operationalized in Splunk

splunk> turn data into doing™

Adapt MITRE Attack to your Journey

Starter

Situation:
- SOC needed
- No data platform

Splunk Tools:

- Data Source Assessment
- Cloud POV

Data-Driven

Situation:
- SOC needed
- Splunk in place

Splunk Tools:

- Splunk Security Essentials

- Cloud POV

SOC

Situation:
- SOC implemented
- Splunk in place

Splunk Tools:

- Enterprise Security

- Splunk Security Essentials

- Splunk Soar

Data Source Assessment

Network 28 CONFIGURED ITEMS

Work with the network team to identify data source items required to achieve key goals and provide an estimate for the total number of items; an approximation c environment.

Configured Item	Total Items	% Indexed	Best Practice Data Sou
Switches	-	100%	*Ethernet and virtual sw*
Routers	-	100%	*cisco_cdr; cisco:asa; cis*
Firewalls (and NextGen Firewalls)	10	100%	*Palo Alto; Cisco; Check*
DDoS Protection	-	100%	*Akamai; Arbor; Netscou*
VPNs	2	100%	*Citrix NetScaler Nitro; C*
Proxy Systems (Web Proxies)	2	100%	*Bluecoat Proxy; Fortine*
Network Access Control (NAC)	-	100%	*Aruba ClearPass; Cisco*
Wireless Access Points	-	100%	*Netgear; Linksys; etc*
LDAP Directory Services	-	100%	*OpenLDAP*
FTP Servers	-	100%	*vsftpd*
DNS	2	100%	*Splunk Stream; BIND; P*
SNMP systems	-	100%	*LogicMonitor; Manage*
Deep Packet Inspection systems	2	100%	*Splunk Stream; PCAP; 2*
DHCP	-	100%	*DHCP Insight; Linux DH*
Loadbalancer	4	100%	*Citrix Netscaler; F5 Big-*
Other	-	100%	
Other	-	100%	
Other	-	100%	

Security Systems 1.011 CONFIGURED ITEMS

Work with the security team to identify data source items required to achieve key goals and provide an estimate for the total number of items; an approximation environment.

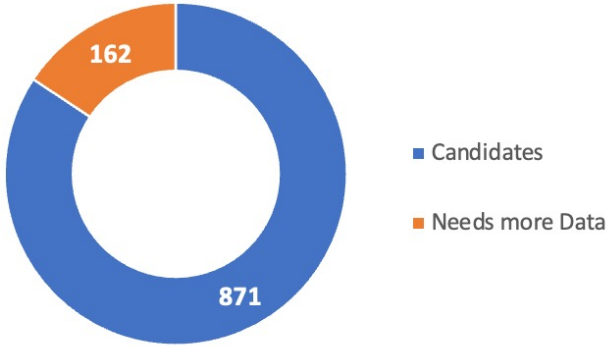
Configured Item	Total Items	% Indexed	Best Practice Data Source Types	% Data Source Typ
Vulnerability Management (VM)	1	100%	*Tripwire IP360; Nessus; OpenVAS; ncircle; Qualys etc*	
Penetration Test Systems/Services	-	100%	*Matasploit logs etc.*	
Network and Security Traffic Analysis	-	100%	*Netflow*	
Intrusion Prevention/Detection Systems (IPS/IDS)	10	100%	*Snort; Bro; Cisco Firepower; TippingPoint IPS; Juniper IDP; McAfee*	
Threat Intelligence Feeds	-	100%	*Anomali; FireEye; BrowdStrike; Threat Lists; Blacklists; etc*	
Automated Malware Anaylsis (Sandbox)	-	100%	*Cisco AMP; FireEye; ChaekPoint SandBlast; Cuckoo; Lastline; etc*	
Source Code Vulnerability Analysis Systems	-	100%	*Logs from OWASP; etc*	
Physical Card Readers	-	100%	*building access systems*	
Block-, Allow-, Watch-Lists	-	100%	*List of prohibited items such as open ports; processes; services*	
User Behavior Analytics (UBA) Systems	-	100%	*Splunk UBA*	
Asset & Identity Lists (from CMDB, AD, LDAP, GRC etc.)	-	100%	*CMDB; Asset Directory; LDAP; IT-GRC Risk assessment*	
Data Loss/Leakage Prevention (DLP)	-	100%	*Microsoft; Clearswift; Digital Guardian; Symantec; McAfee*	
EDR (Endpoint Detection & Response)	1.000	100%	*Tanium; Carbon Black; FireEye HX; CrowdStrike Falcon; Ziften*	
NDR (Network Detection & Response)	-	100%	*Vectra; Darktrace; Extrahop; Lastline*	
WAF (Web Application Firewall)	4	100%	*Imperva; F5; Barracuda; Radware; Citrix Netscaler*	
Other	-	100%		
Other	-	100%		
Other	-	100%		

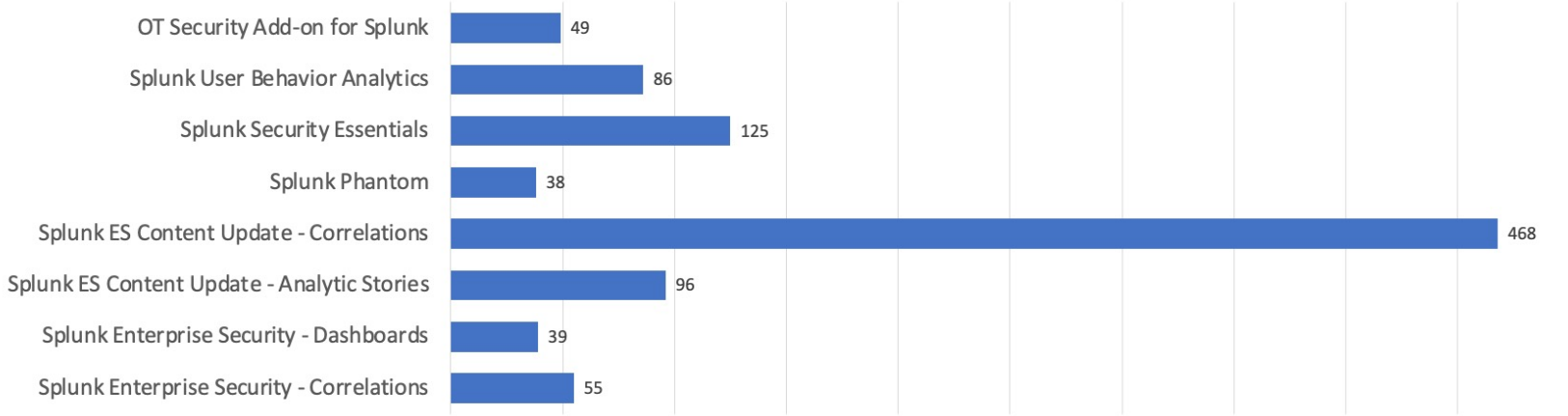
splunk> turn data into doing

Security Content Candidates

Export

Min. Data Indexed 20%





Candidate?	Source	Title	Description	Datamodel	Data Source	High-Level Use Case	Data Source Coverage
Yes	Splunk Security Essentials	Access to In-scope Resources	Visibility into who is accessing in-scope resources is key to your		Web Proxy	Compliance	60%
Yes	Splunk Security Essentials	Access to In-Scope Unencrypted Resources	Unencrypted communications leaves you vulnerable to a data l		Web Proxy	Compliance	60%
Yes	Splunk Security Essentials	Concentration of Attacker Tools by Filename			Endpoint Detection and Respor	Advanced Threat Detection | Se	67%
Yes	Splunk Security Essentials	Concentration of Discovery Tools by Filename			Endpoint Detection and Respor	Advanced Threat Detection | Se	50%
Yes	Splunk Security Essentials	Concentration of Discovery Tools by SHA1 Hash			Endpoint Detection and Respor	Advanced Threat Detection | Se	100%
Yes	Splunk Security Essentials	Short Lived Admin Accounts			Windows Security	Advanced Threat Detection	75%
Yes	Splunk ES Content Update - Correlations	ESCU - Recursive Delete of Directory In Batch CMD - Rule	This search is to detect a suspic	Endpoint			35%
Yes	Splunk ES Content Update - Correlations	ESCU - Disable AMSI Through Registry - Rule	this search is to identify modifi	Endpoint			100%
Yes	Splunk ES Content Update - Correlations	ESCU - Disable ETW Through Registry - Rule	this search is to identify modifi	Endpoint			100%
Yes	Splunk ES Content Update - Correlations	ESCU - Allow File And Printing Sharing In Firewall - Rule	This search is to detect a suspic	Endpoint			100%
Yes	Splunk ES Content Update - Correlations	ESCU - Excessive Usage Of SC Service Utility - Rule	This search is to detect a suspicious excessive usage of sc.exe in		sysmon		50%
Yes	Splunk ES Content Update - Correlations	ESCU - Detect Traffic Mirroring - Rule	Adversaries may leverage traffic mirroring in order to automate		cisco_networks		50%
Yes	Splunk ES Content Update - Correlations	ESCU - Detect Software Download To Network Device - Rul	Adversaries may abuse netboot	Network_Traffic			38%
Yes	Splunk ES Content Update - Correlations	ESCU - Detect Rogue DHCP Server - Rule	By enabling DHCP Snooping as a Layer 2 Security measure on th		cisco_networks		67%
Yes	Splunk Security Essentials	User Logged into In-Scope System They Should Not Have	Follow your GDPR requirement and action your data mapping		Windows Security | Authentica	Insider Threat | Compliance	67%
Yes	Splunk Security Essentials	Basic Malware Outbreak	Looks for the same malware occurring on multiple systems in a		Anti-Virus or Anti-Malware	Security Monitoring	44%
Yes	Splunk Security Essentials	Basic Scanning	Looks for hosts that reach out to more than 500 hosts or more		Network Communication	Security Monitoring	44%

splunk> turn data into doing

Splunk Security Essentials Apps

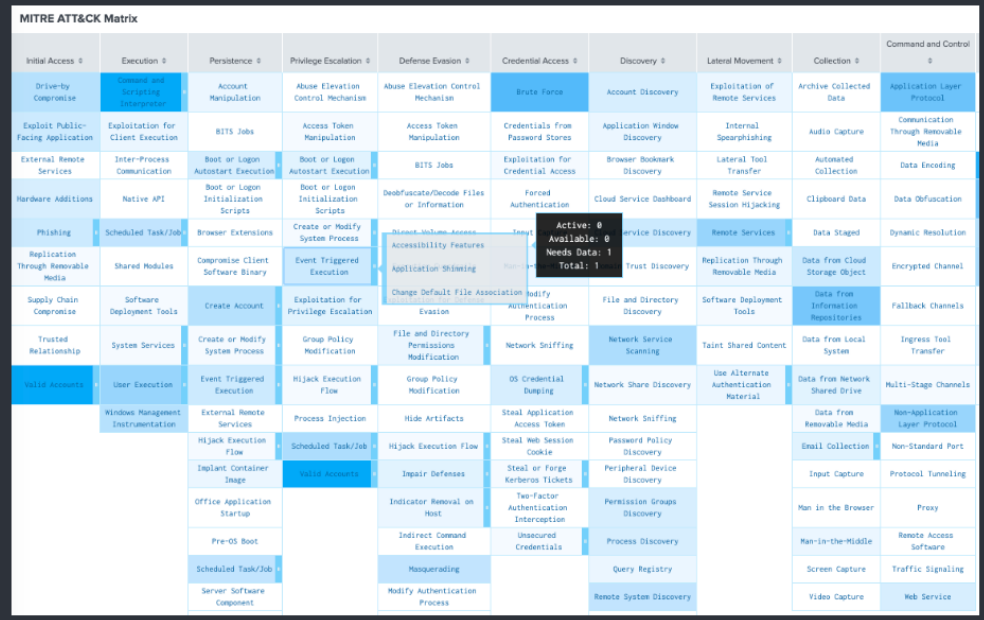
https://splunkbase.splunk.com/app/3435/

SPLUNK

Splunk Security Essentials

49 ratings

Splunk Cloud Splunk Built



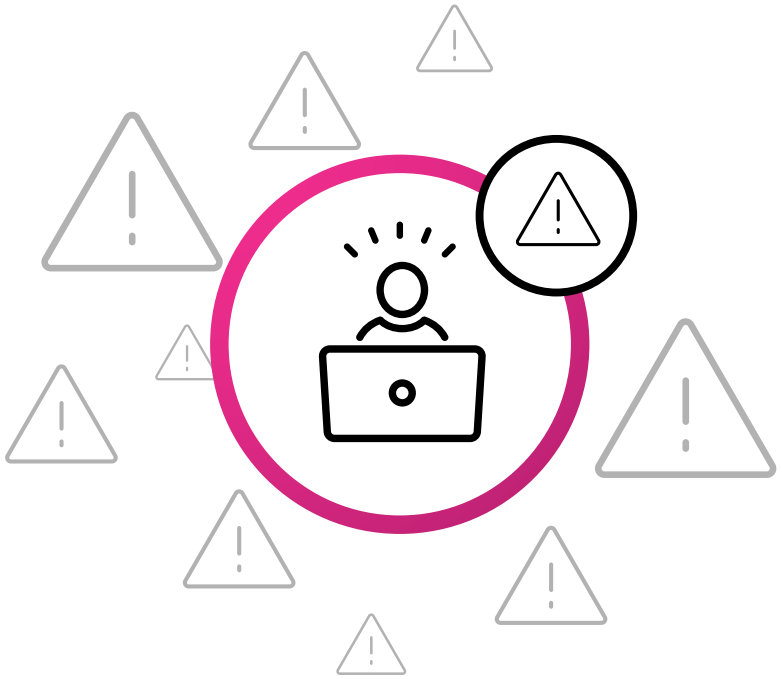
SSE in Action

MITRE ATT&CK beyond simple detections

splunk> turn data into doing™

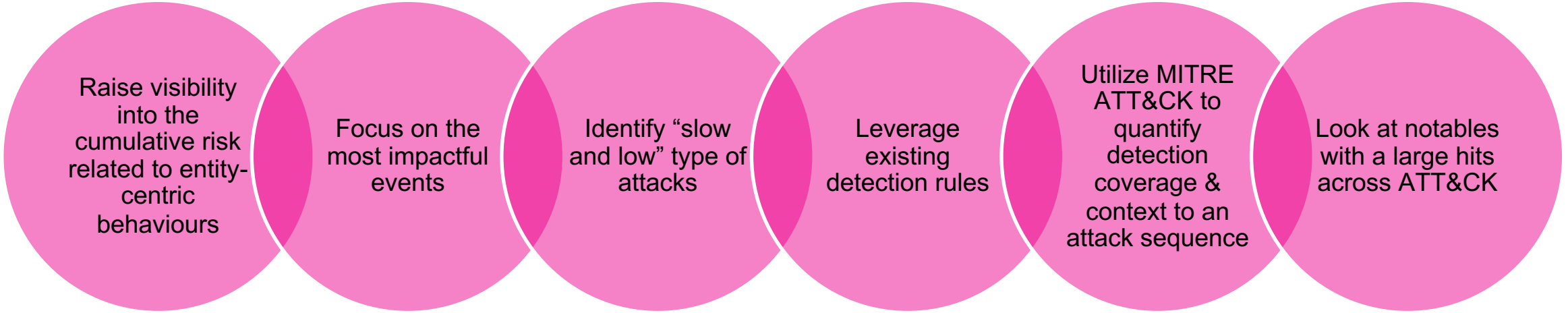
Alert Volumes Are Overwhelming SOCs

Over 40% of orgs receive 10,000+ alerts per day; experience 50%+ false positives



- Abandoned alerts
- Suppressed alerts
- Slow detection / response
- Analyst burnout

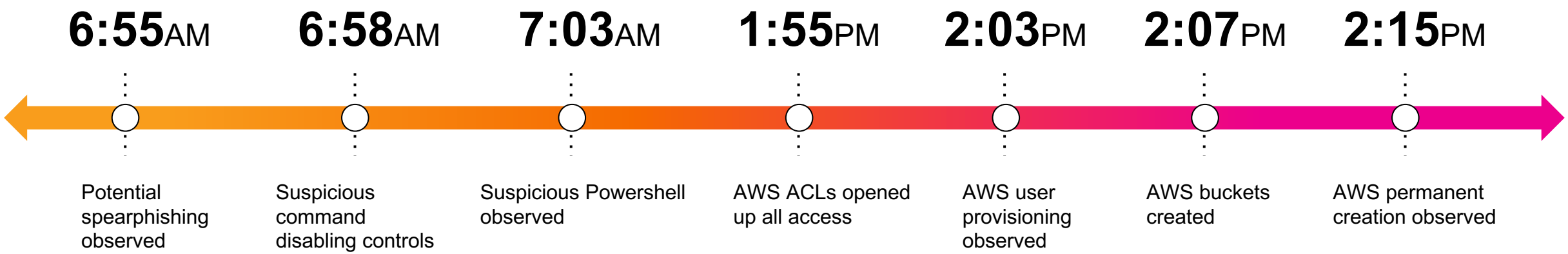
What if we want to…



Risk Based Alerting (RBA)

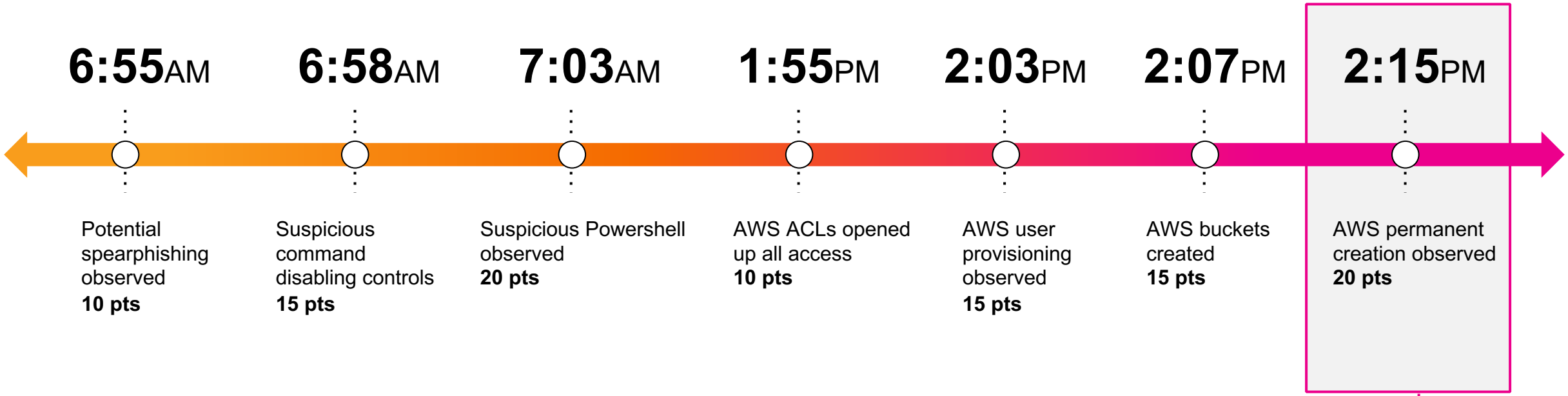
How Does This Look in Practice?

Traditionally, the events below would be considered too noisy and would be abandoned

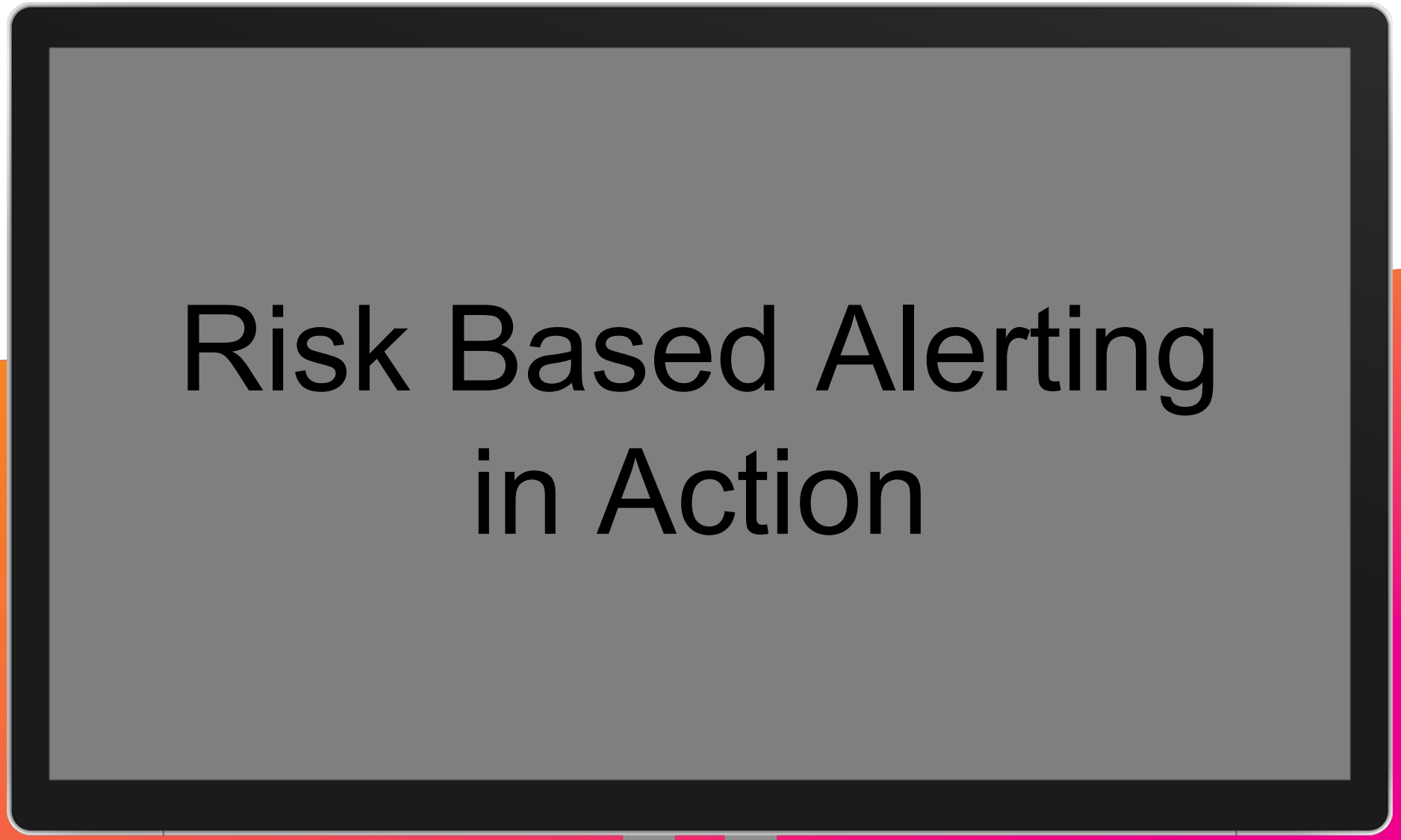


How Does This Look in Practice?

With risk-based alerting, these events become context that informs high-fidelity alerts



splunk> turn data into doing



Today’s Take Aways

Mitre Att@ck Framework is extremly usefull tool to understand your cybersecurity threads

Splunk products and tools make it easy to leverage the Mitre Att@ck Framework in your environment

Mitre Att@ck Framework + Splunk can be your key to improve security posture continuosly

Q&A

splunk> turn data into doing™

Thank You

splunk> turn data into doing™