

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

mit dem MITRE ATT&CK Framework & Splunk

# 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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2021 SPLUNK Inc. All rights reserved.



***Le-Khanh Au***

Security Advisor



**Alex Pilger**

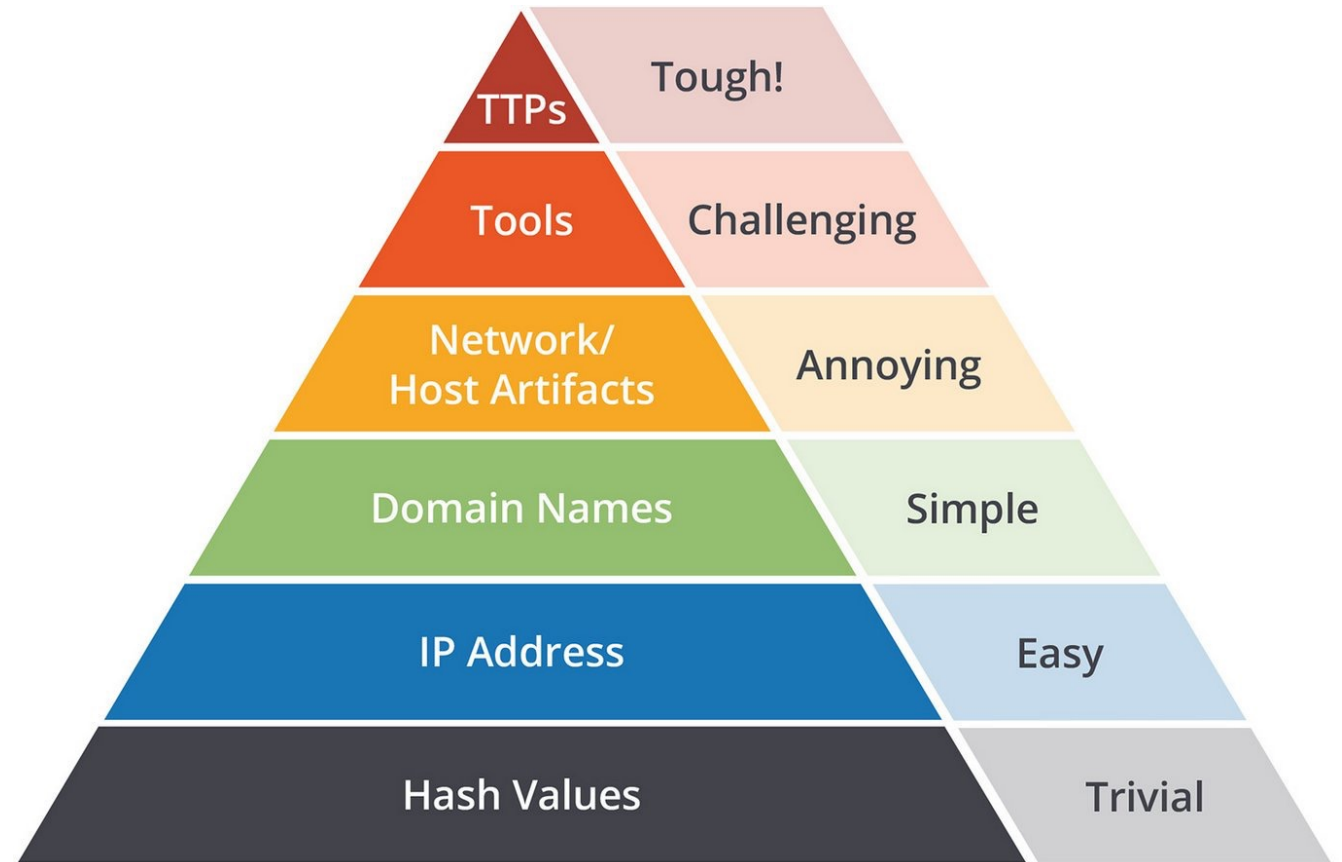
Partner Technical Manager (CISSP,GMON)

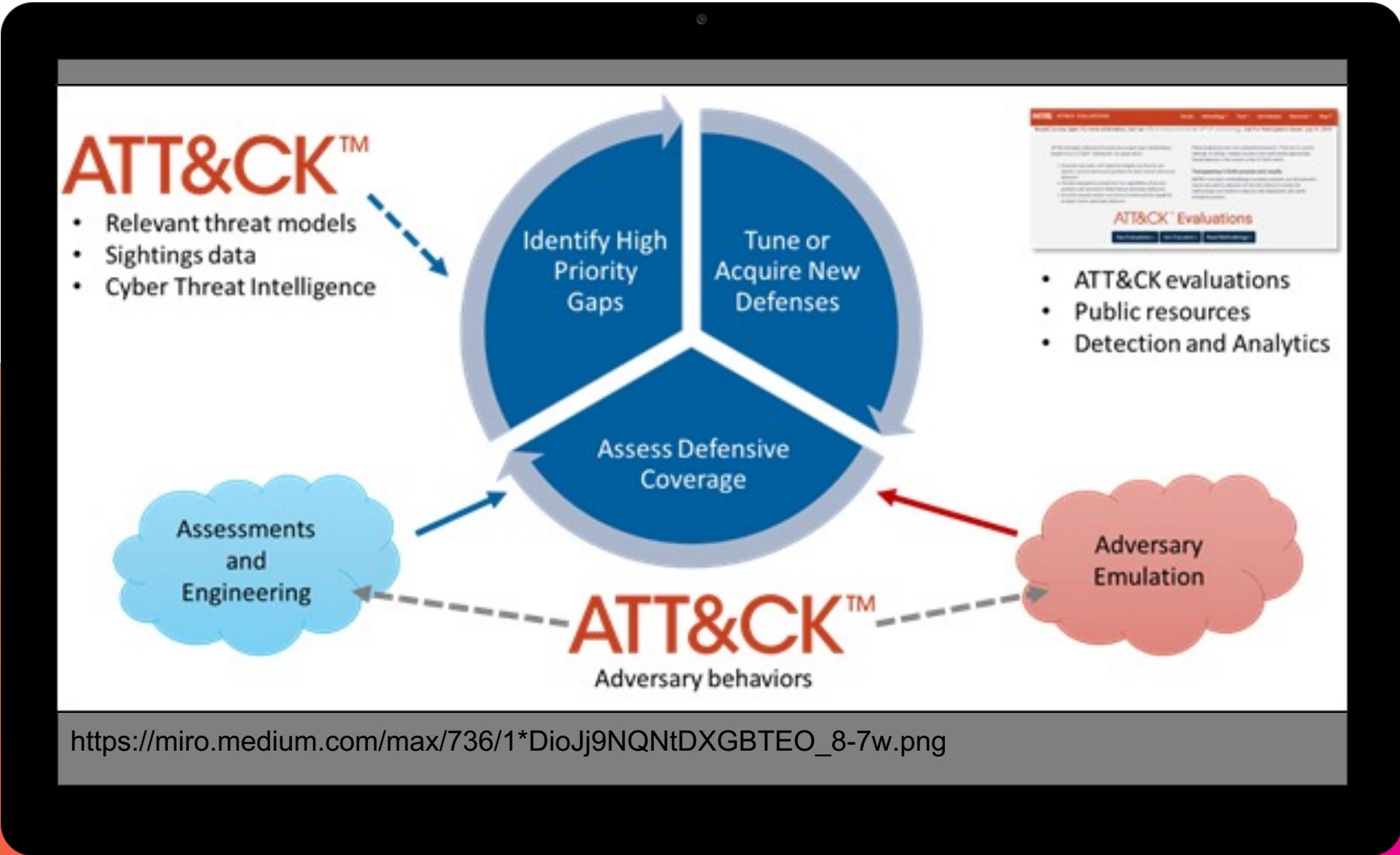
# Agenda

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

# MITRE ATT&CK explained

# The Pyramid of Pain

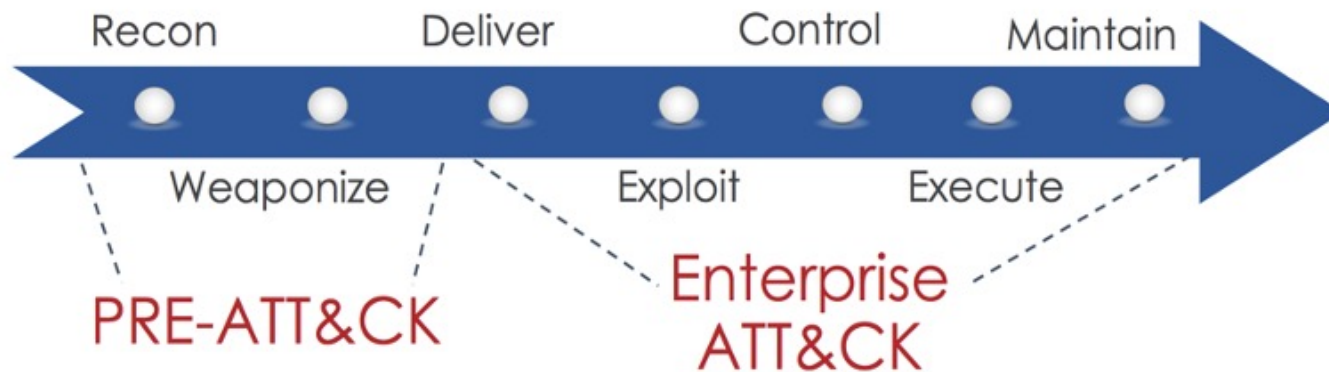




## Introduction to MITRE ATT&CK™

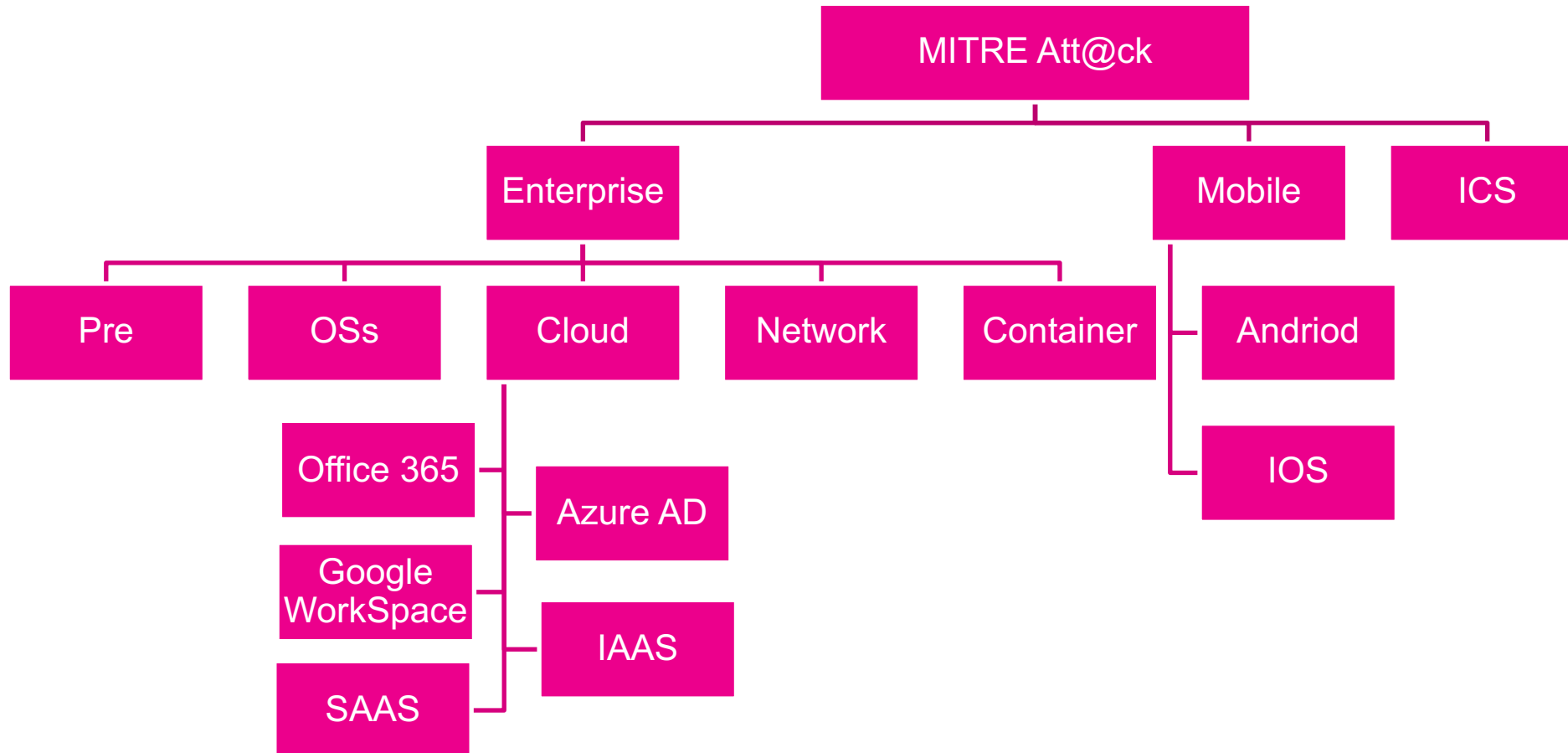
### A knowledge base of adversary behavior

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



<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?



# Demo

Do really need to get  
into all of this?

# MITRE ATT&CK operationalized in Splunk

splunk<sup>®</sup> > turn data into doing<sup>™</sup>

# 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 Source Types
Switches	-	100%	Ethernet and virtual sw
Routers	-	100%	cisco_cdr; cisco:asa; cisc
Firewalls (and NextGen Firewalls)	10	100%	Palo Alto; Cisco; Check
DDoS Protection	-	100%	Akamai; Arbor; Netsco
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; Z
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

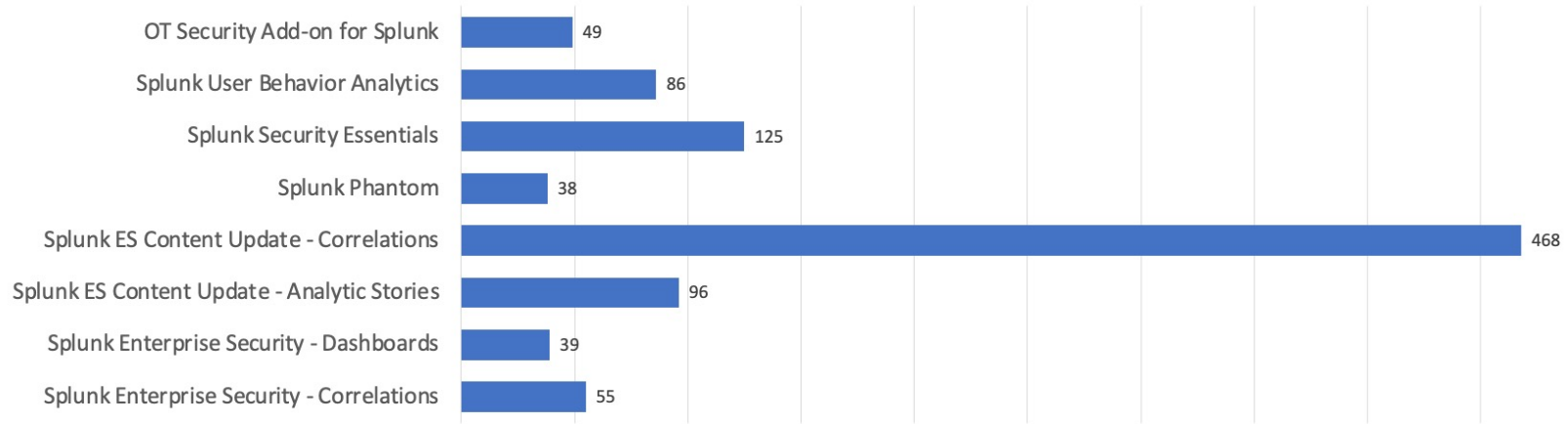
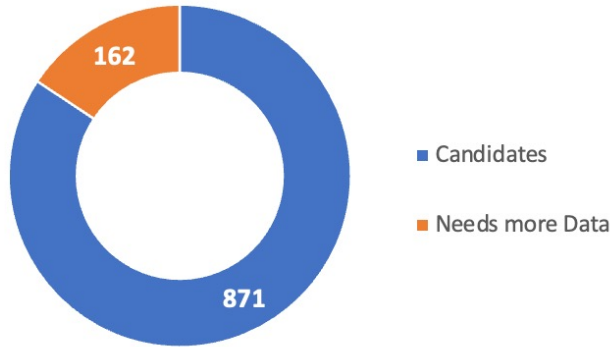
Work with the security team to identify data source items required to achieve key goals and provide an estimate for the total number of items; an approximation environment.

Configured Item	Total Items	% Indexed	Best Practice Data Source Types	% Data Source Ty
Vulnerability Management (VM)	1	100%	Tripwire IP360; Nessus; OpenVAS; ncircle; Qualys etc	
Penetration Test Systems/Services	-	100%	Metasploit 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 Analysis (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%		

### 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 Respoi	Advanced Threat Detection   Se	67%
Yes	Splunk Security Essentials	Concentration of Discovery Tools by Filename			Endpoint Detection and Respoi	Advanced Threat Detection   Se	50%
Yes	Splunk Security Essentials	Concentration of Discovery Tools by SHA1 Hash			Endpoint Detection and Respoi	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 - Rule	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 Security Essentials Apps

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

SPLUNK



## Splunk Security Essentials



49 ratings



Splunk Cloud



Splunk Built

MITRE ATT&K Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Drive-by Compromise	Workload and Scripting Abuse	Account Manipulation	Abuse Elevation Control Mechanisms	Abuse Elevation Control Mechanisms	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmarks Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Browser Inclusion/Access	Active: 0 Available: 0 Needs Data: 1 Total: 1	Service Discovery	Remote Services	Data Staged	Dynamic Resolution
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Accessibility Features	Application Shim/mimic	Trust Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Encrypted Channel
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Change Default File Association	Identity Authentication Process	File and Directory Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Skiffing	Network Service Scanning	Taint Shared Content	Data from Local System	Ingress Tool Transfer
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Network Share Discovery	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Application Access Token	Network Skiffing		Data from Removable Media	Non-Application Layer Protocol
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal Web Session Cookie	Password Policy Discovery		Email Collection	Non-Standard Port
		Implant Container Image	Valid Accounts	Impair Defenses	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Input Capture	Protocol Tunneling
		Office Application Startup		Indicator Removal on Host	Two-Factor Authentication Interception	Permission Groups Discovery		Man in the Browser	Proxy
		Pre-OS Boot		Indirect Command Execution	Unsecured Credentials	Process Discovery		Man-in-the-Middle	Remote Access Software
		Scheduled Task/Job		Masquerading		Query Registry		Screen Capture	Traffic Signaling
		Server Software Component		Modify Authentication Process		Remote System Discovery		Video Capture	Web Service

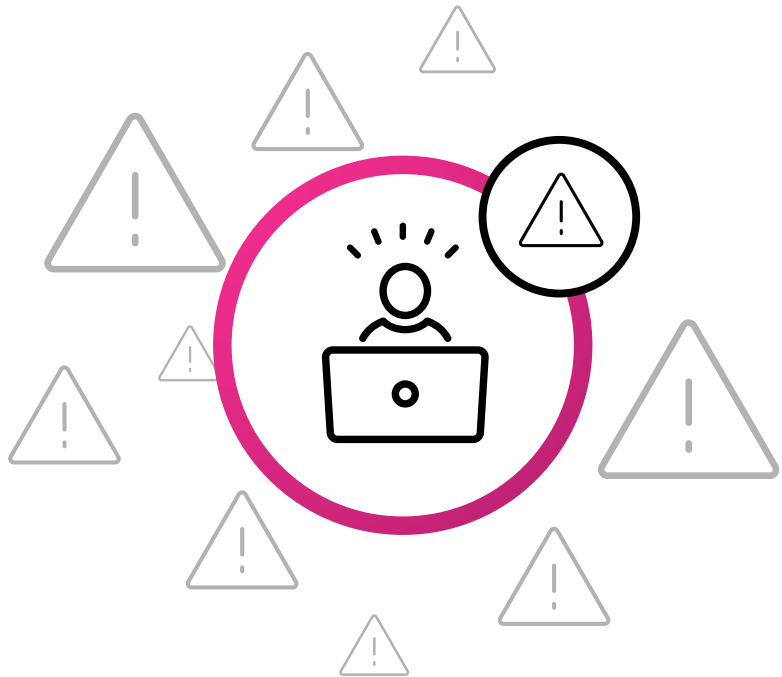


# SSE in Action

# MITRE ATT&CK beyond simple detections

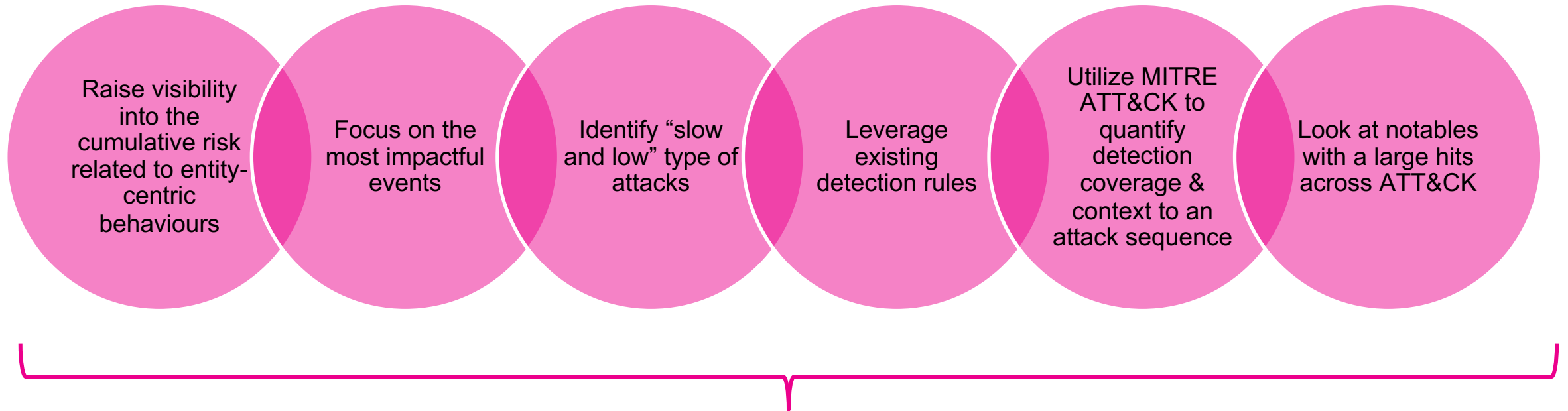
# Alert Volumes Are Overwhelming SOCs

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



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

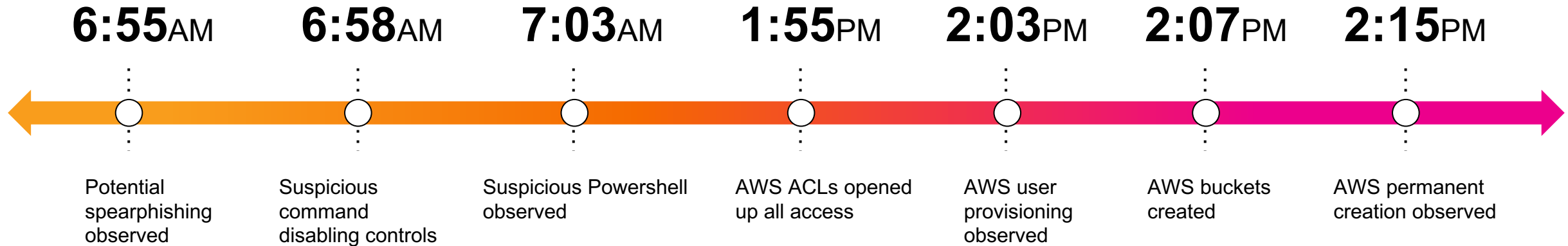
# What if we want to...



## Risk Based Alerting (RBA)

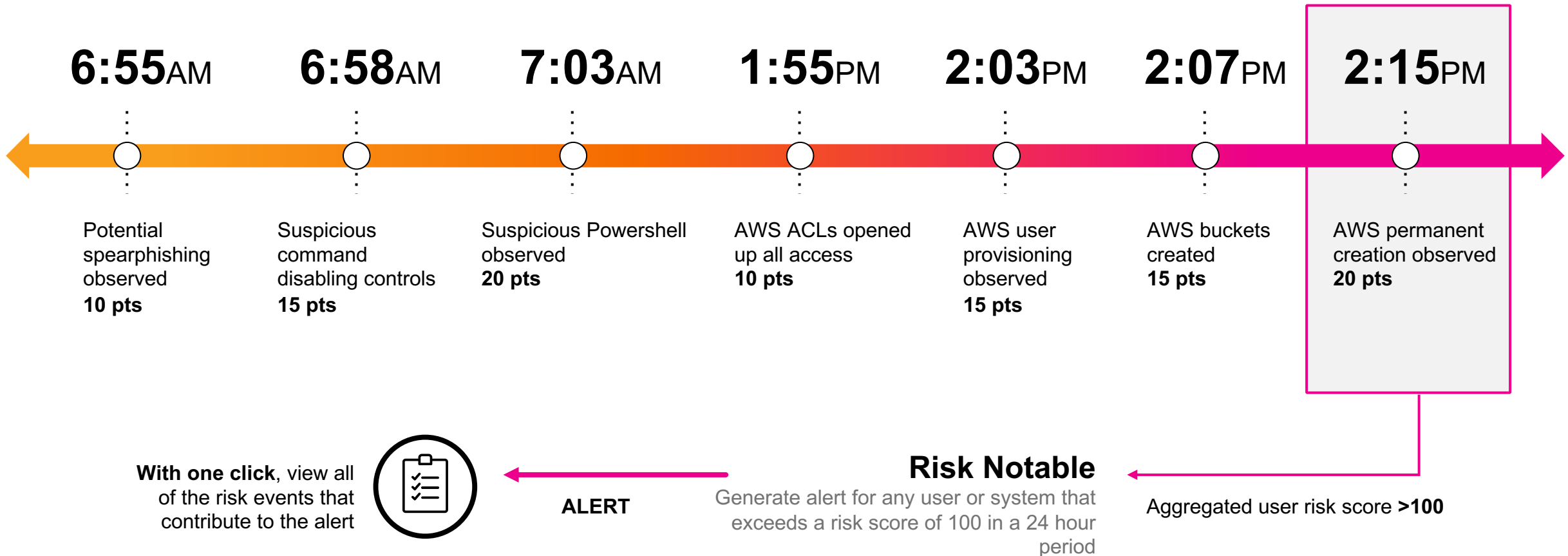
# How Does This Look in Practice?

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



# Risk Based Alerting in Action

# Today's Take Aways

Mitre Att@ck Framework is extremely 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 continuously

# Q&A

splunk > turn data into doing™

# Thank You

splunk® > turn data into doing™