

From Zero to Future SOC

Mastering the Journey from Project Kickoff to Security Operations Excellence



Marcel Tanuatmadja
Roberta Geyer

Forward- looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or 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 or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

Defending The Galaxy, One Log at a Time



Agenda

- 01** The SOC Journey Begins
- 02** SOC Project Kickoff: From Idea to Impact
- 03** People Make the SOC
- 04** Anatomy of a Cyberattack and Detection Engineering
- 05** Powering the Future SOC

01

The SOC Journey Begins



PROMPT: Generate payload for exploit ...



Claude

Hacker Jailbreaks Claude AI to Write Exploit Code Steal Government Data

A hacker exploited Anthropic's Claude AI chatbot over a month-long campaign starting in December 2025, using it to identify vulnerabilities, generate exploit code, and exfiltrate sensitive data from Mexican government agencies. The operation spanned from December 2025 to early January 2026, with the hacker crafting Spanish-language prompts to role-play Claude as an "elite hacker" in a simulated bug bounty program. Claude's outputs included reconnaissance scripts for network scanning, SQL injection exploits, and credential-stuffing automation tailored to outdated government systems.

 heise online [heise+ entdecken](#)

Claude: AI chatbot used for cyberattack on Mexican government

An unknown cybercriminal is using Anthropic's AI chatbot to infiltrate Mexican government networks. This follows a worrying trend.



AI is reshaping the threat landscape

AI-Generated Malware
and Exploits

AI-Augmented
Reconnaissance

AI-Enhanced Social
Engineering

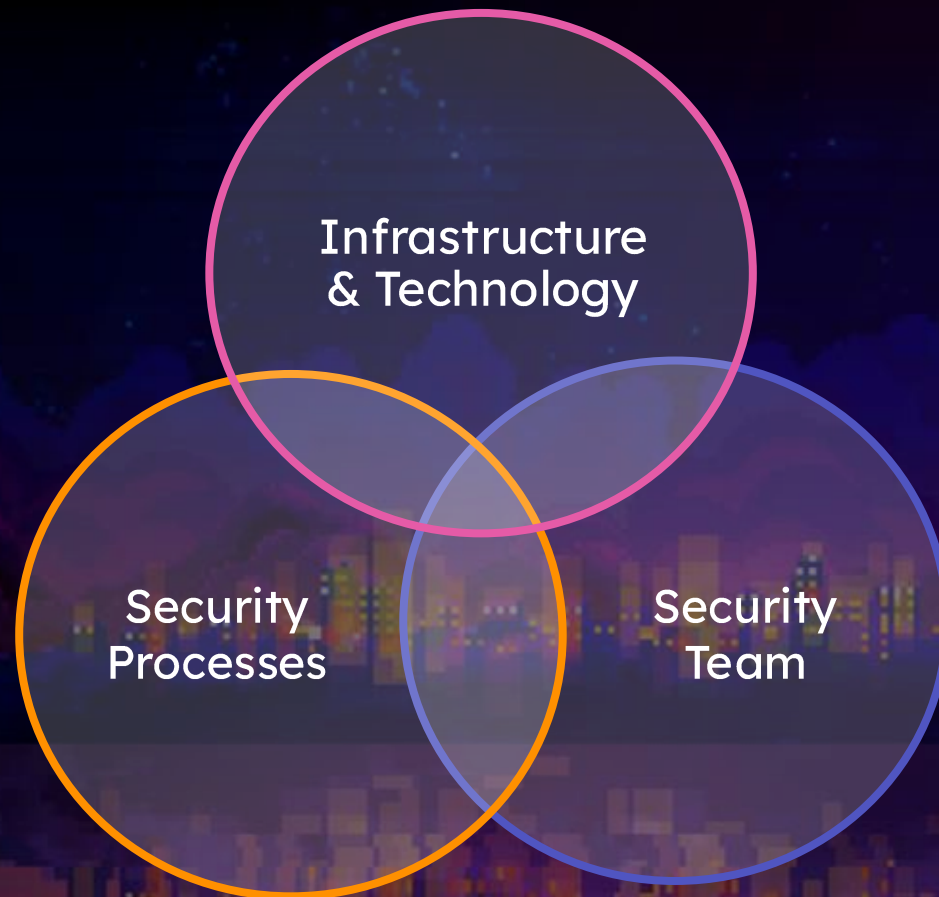
Autonomous Attack
Chains



02

SOC Project Kickoff: From Idea to Impact

The 3 Pillars of SOC



3 equal parts make a **mature security program.**

You need a Security Program



A Charter for Your Security Program

“what?”

Asset Inventory,
Architecture

“from what?”

Vulnerabilities,
Threats.

“if you don’t?”

Impact

“how likely?”

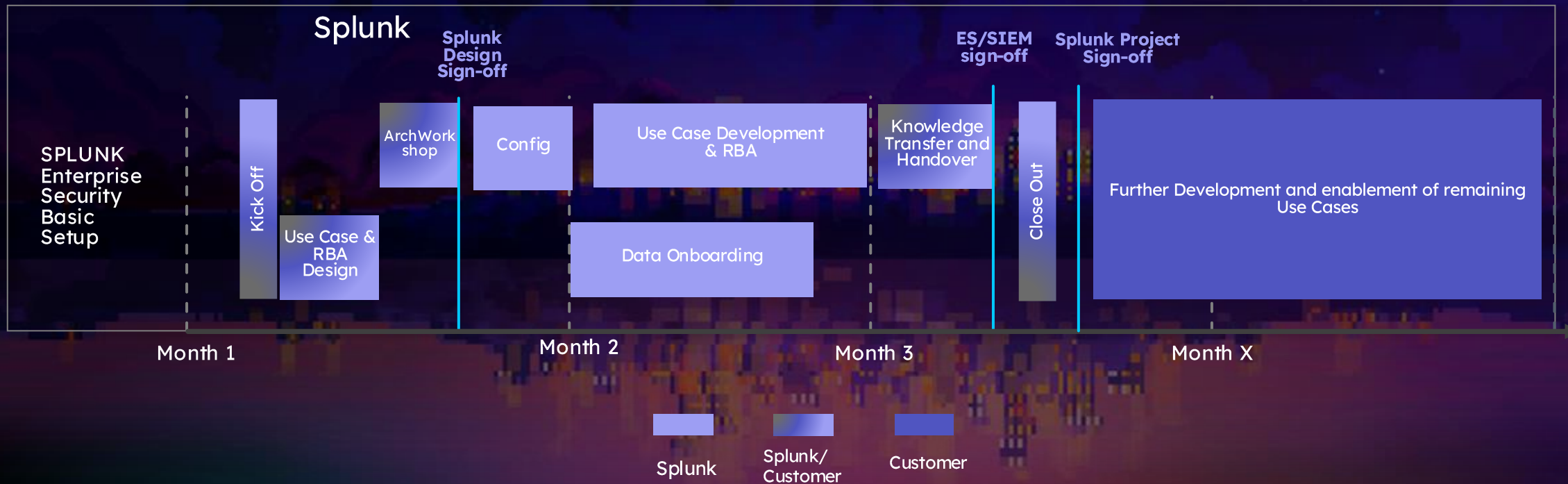
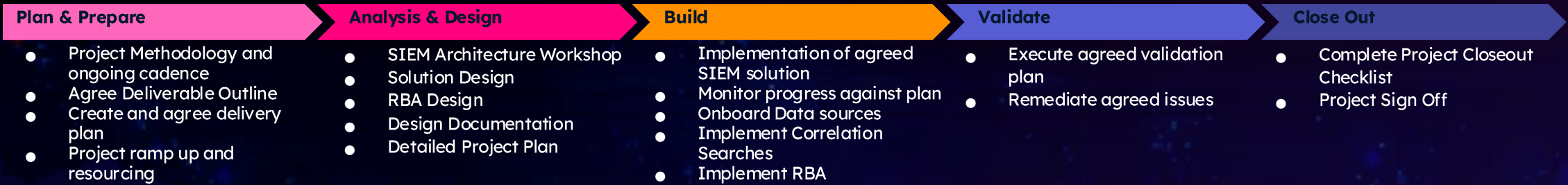
Likelihood

Risk = Impact × Likelihood

Continuous Monitoring as Security Program



Splunk Best-Practice Delivery Model for SOC Projects



Success Factors and Pitfalls

Proactive project planning

Lock scope & success criteria

Plan realistically

Realistic milestones and project outcome

Stakeholder management

Define Responsibility's and Boundaries

Outcome-driven tracker

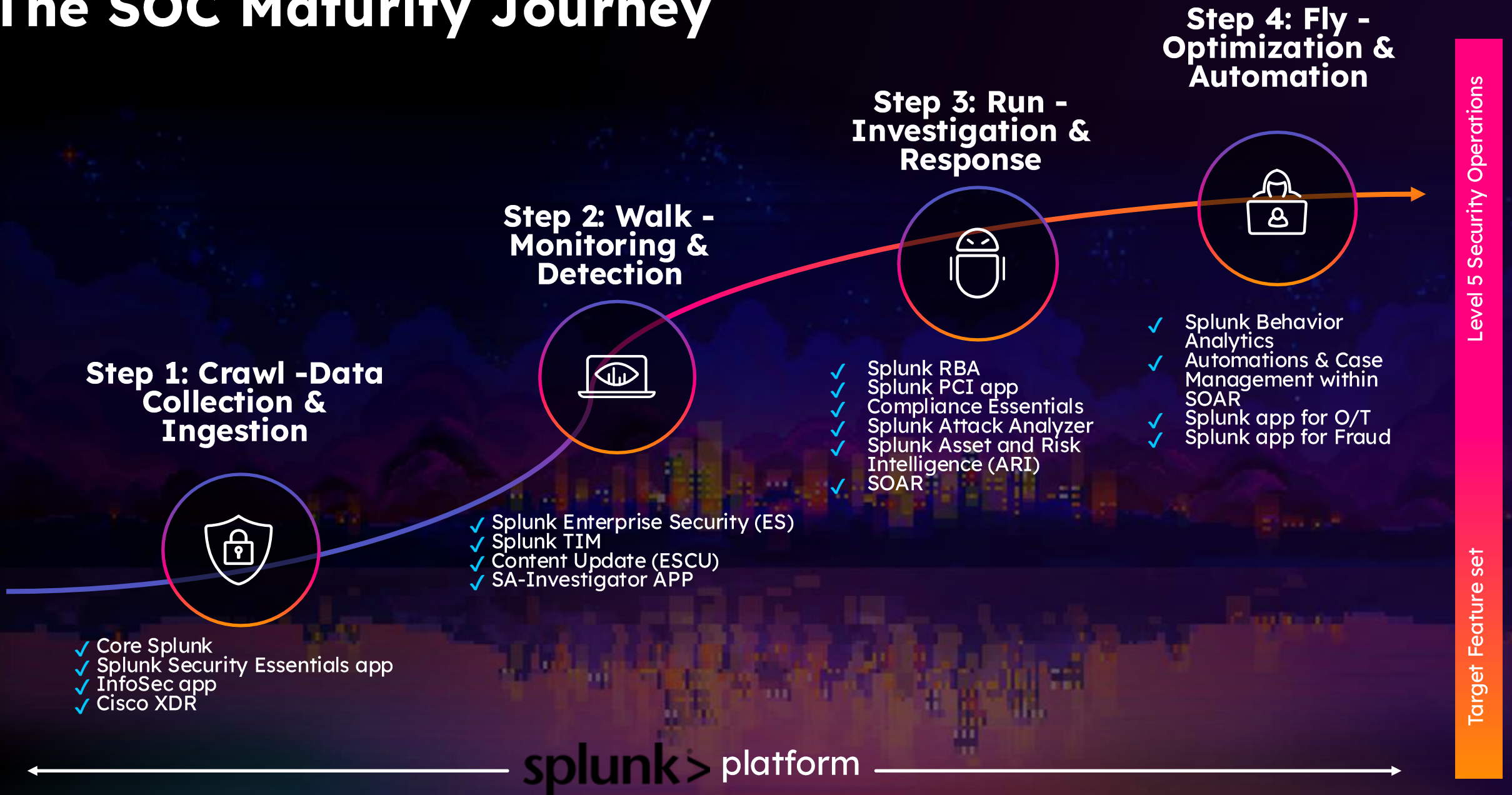
Assign actions, visualize critical path

“A project moves fastest when its manager listens hardest - to the people who build it.”

The SOC Maturity Journey



The SOC Maturity Journey



03

People Make the SOC

SOC Roles and Responsibilities



Splunk Learning Paths & Certifications

[Splunk Core Certified User](#)

[Splunk Core Certified Power User](#)

[Splunk Core Certified Advanced Power User](#)

[Splunk Enterprise Certified Admin](#)

[Splunk Enterprise Certified Architect](#)

[Splunk Enterprise Security Certified Admin](#)

[Splunk Certified Cybersecurity Defense Analyst](#)

[Splunk Certified Cybersecurity Defense Engineer](#)

[Splunk SOAR Certified Automation Developer](#)

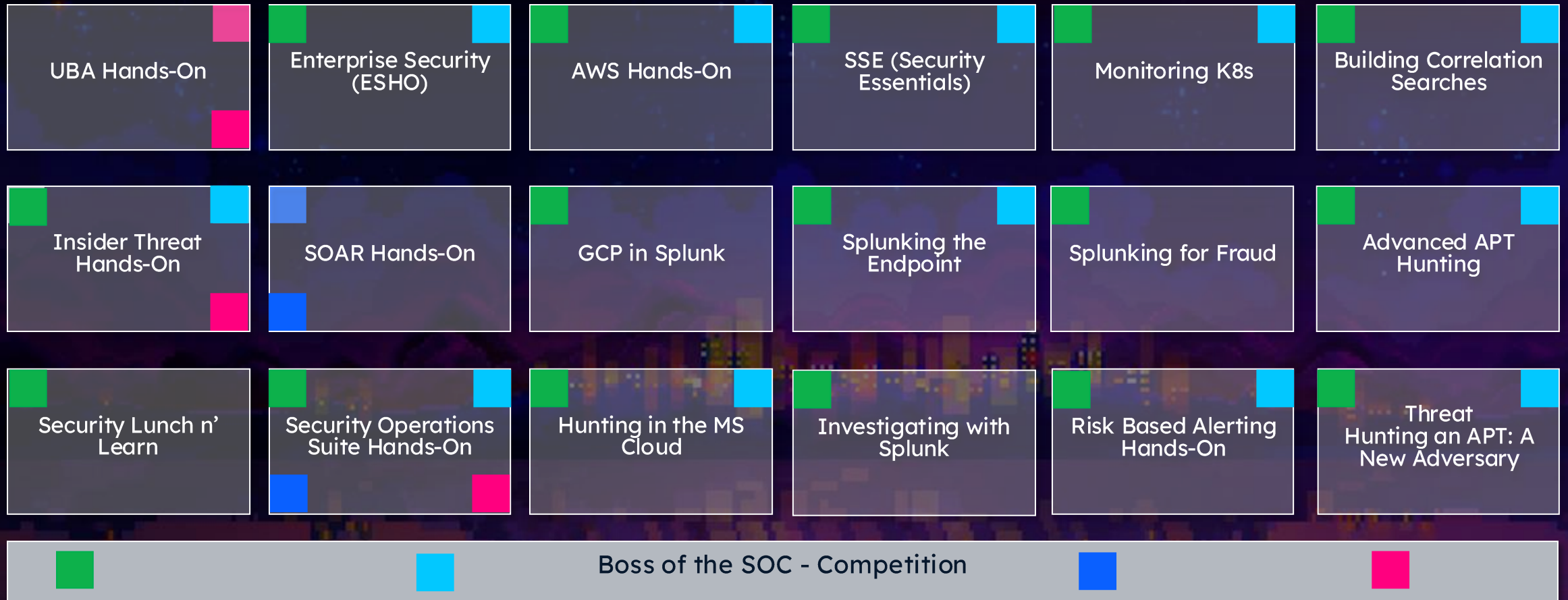


Success paths based on
Splunk product and role

Recommended sequence
of courses



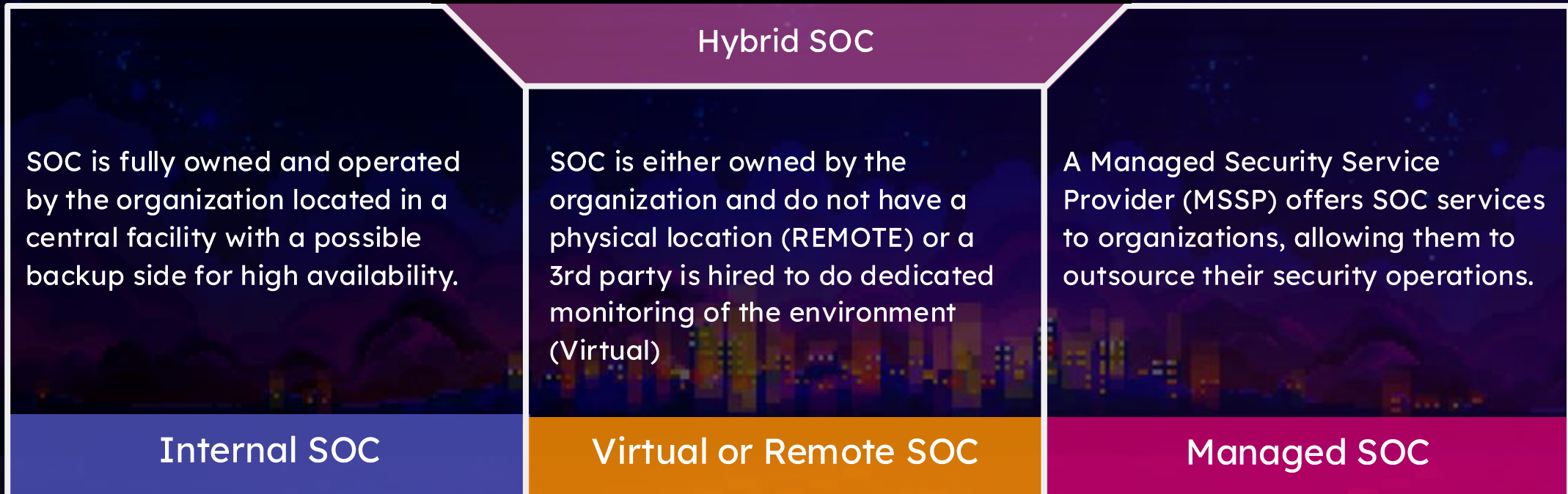
Splunk for Security Workshops



Introductory

Advanced

Different SOC Types



04

Anatomy of a Cyberattack and Detection Engineering

Cyber Kill Chain by Lockheed Martin



Reconnaissance: Attacker gathers info on the target.

Weaponization: Malware is developed or customized.

Delivery: Malware is delivered (e.g. via email or exploit).

Exploitation: Payload is executed on the target.

Installation: Malware installs a backdoor or persistent access.

Command & Control: Remote access is established.

Actions on Objectives: Data theft, destruction, or ransomware.

The earlier an attack is detected in the chain, the easier and cheaper it is to stop.

Tactics, Techniques and Procedures

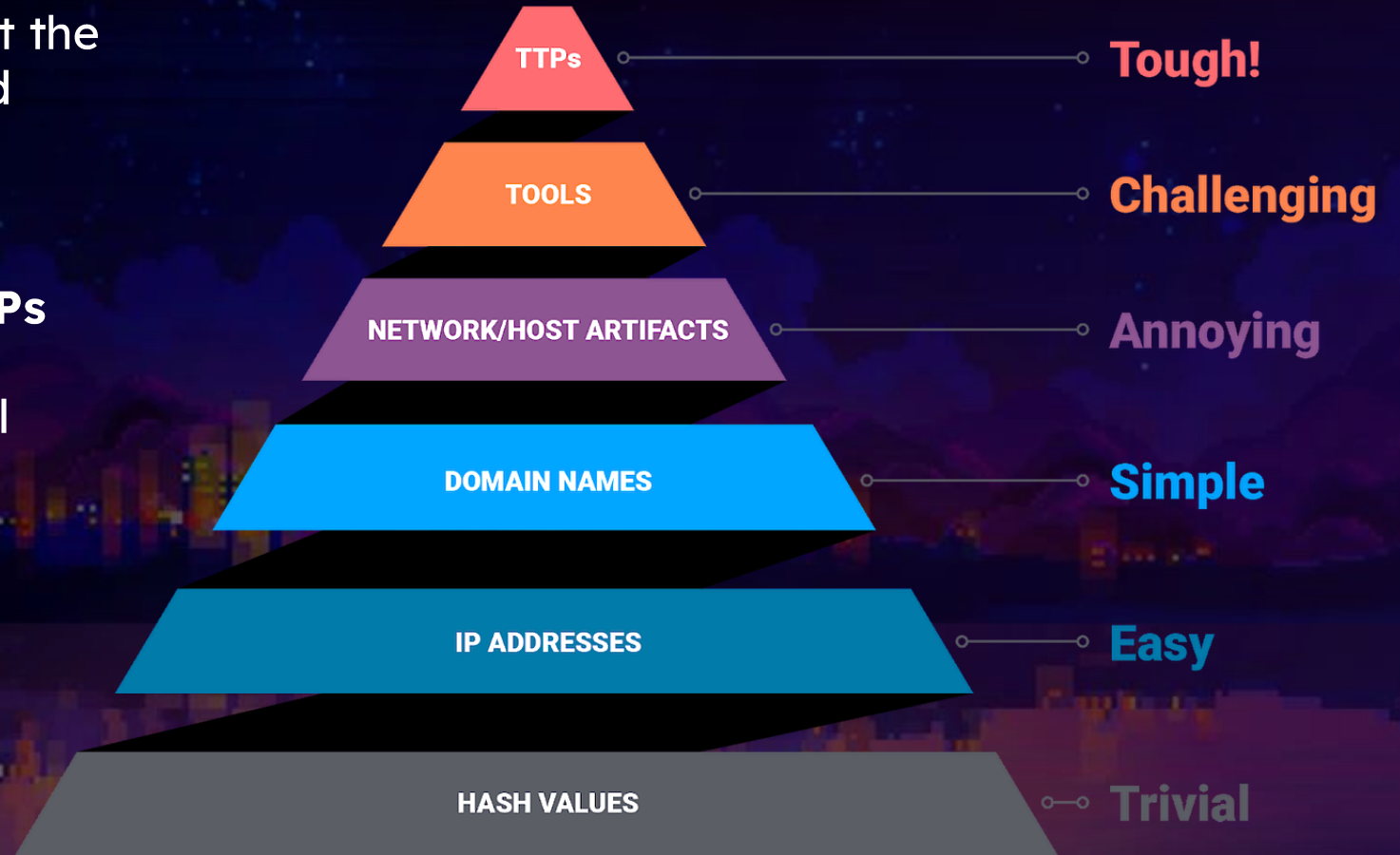
The Pyramid of Pain

Maximize attacker pain: operate at the **top** (TTPs = Tactics Techniques and Procedures)

Layers (low to high): **Hashes** ▯ **IPs** ▯ **Domains** ▯ **Artifacts** ▯ **Tools** ▯ **TTPs**

Low levels = easy to swap, minimal impact

Focus on **behavior/TTP-based** detections and hunting



How to find the right Content

TOP

1. Do a **Risk** assessment – understand your organisations Resiliency needs
2. Engage **Stakeholders** early in the process
3. Identify and prioritize **Use Cases**
4. Identify and prioritize **Data Sources**

DOWN

Leverage MITRE ATT&CK with Splunk Detection Studio

The screenshot displays the Splunk Detection Studio interface, specifically the MITRE ATT&CK matrix and detection coverage/health sections.

MITRE ATT&CK Matrix: A grid of 15 techniques is shown, with 100% coverage for each. Techniques include: Reconnaissance (10 of 10 Techniques (100%)), Resource Development (8 of 8 Techniques (100%)), Gather Victim Identity Information, Acquire Infrastructure, Gather Victim Network Information, Compromise Information, Gather Victim Org Information, Establish Account, Gather Victim Host Information, Compromise Account, Search Open Websites/Domains, Develop Capabilities, Search Victim-Owned Websites, Obtain Capabilities, Active Scanning, Stage Capabilities, Search Open Technical Databases, Acquire Accounts, Search Closed Sources, and Phishing for Information.

Detections Section:

- Detection coverage:** Overall detection technique coverage is 65% (up 5%). A line chart shows coverage over time from January to August.
- Detection health:** Overall detection health is 86% (up 5%). A line chart shows performance over time from January to August.
- Available detections by priority rank:** A donut chart shows the distribution of detection priorities (None, Low, Medium, High).
- Highest priority available detections:** A table lists high-priority detections:

Priority	Name	Actions
High	Endpoint - Potential Automated File Collection - Rule	🔍 🗑️
High	Endpoint - Potential Indicator Removal on Host: Timestamp - Rule	🔍 🗑️
High	ESCU - Any Powershell DownloadFile IF Only - Rule - Rule	🔍 🗑️
High	ESCU - CMD Echo Pipe - Escalation IF Only - Rule - Rule	🔍 🗑️
High	ESCU - Disable Schedule Task IF Only - Rule - Rule	🔍 🗑️
- Deployed detections by health rank:** A donut chart shows the distribution of detection health scores (None, Low, Medium, High).
- Lowest Health Deployed Detections:** A table lists detections with the lowest health scores:

Health	Name	Actions
High	Azure AD Unusual Number of Failed Authentications From Ip	🔍 🗑️
High	Disabling CMD Application	🔍 🗑️
High	Suspicious Reg.exe Process	🔍 🗑️
Medium	Windows Disable Change Password Through Registry	🔍 🗑️
Medium	Windows Modify Registry Default Icon Setting	🔍 🗑️

Impact Section: A grid of 15 impact categories is shown, with 100% coverage for each. Impacts include: Exfiltration Techniques (100%), Impact (15 of 15 Techniques (100%)), Information Over Other Work Medium, Data Destruction, Staged Exfiltration, Firmware Corruption, Unauthorized Transfer, Data Encrypted for Impact, System Size Limits, Service Stop, Over C2 Channel, Inhibit System Recovery, Information Over Alternative Protocol, Defacement, Information Over Physical Medium, Resource Hijacking, Data to Cloud Account, Network Denial of Service, Information Over Web Service, Endpoint Denial of Service, System Shutdown/Reboot, Account Access Removal, Disk Wipe, Data Manipulation, and Financial Theft.

Detection Engineering



Threat Modeling



What threats does the organization care about?

Intellectual or customer data loss, compliance, etc.

Prioritized based on impact

What would the threat look like?

How it would access and exfiltrate confidential data

How would we detect / block the threat?

Required machine data and external context
Searches or visualizations that would detect it

What is the playbook / process for each type of threat?

Severity, response process, roles and responsibilities, how to document, how to remediate, when to escalate or close etc.

What are the most Critical Assets we need to Triage First?

Severity:
Medium

For identities: **user** or **src_user**
For assets: **dest, src, or dvc**

Entity priority	Risk score	Urgency	Status	Actions
high	20	● Medium	In Progress	⋮

Assigned Severity

Assigned Priority	Unknown	Low	Medium	High	Critical
Unknown	Low	Low	Low	Medium	High
Low	Low	Low	Low	Medium	High
Medium	Low	Low	Medium	High	Critical
High	Medium	Medium	Medium	High	Critical
Critical	Medium	Medium	High	Critical	Critical

The Urgency level is set to “Medium” since the entity priority is “high” and the detection severity is “Medium”.

Splunk Threat Research

The screenshot displays the Splunk Threat Research interface. On the left, there's a navigation sidebar with categories like Application, Cloud, Endpoint, Network, Web, Tactics, Collection, Command And Control, Credential Access, Defense Evasion, Discovery, Execution, Exfiltration, Impact, Initial Access, Lateral Movement, and Persistence. The main area shows a 'Detections' table with columns for Name, Data Source, Technique, Type, Analytic Story, and Date. A detailed view on the right shows the detection 'Malicious PowerShell Process - Execution Policy Bypass' with its description, search query, and data source table.

Detections

Name	Data Source	Technique	Type	Analytic Story	Date
Cisco ASA - Core Syslog Message Volume Drop	Cisco ASA Logs	T1562	HUNTING	ArcaneDoor	2025-09-25
Cisco ASA - Logging Disabled via CLI	Cisco ASA Logs	T1562	TTP	Suspicious Cisco Adaptive Security Appliance Activity	2025-09-25
Cisco Secure Firewall - Intrusion Events by Threat Activity	Cisco Secure Firewall Threat Defense Intrusion Event	T1041 T1573.002	ANOMALY	ArcaneDoor, Cisco Secure Firewall Threat Defense Analytics	2025-09-25
Linux Auditd Service Started	Linux Auditd Proctitle	T1569.002	ANOMALY	Compromised Linux Host, Linux Living Off The Land, Linux Persistence Techniques, Linux Privilege Escalation	2025-09-18
Cisco NVM - Curl Execution With Insecure Flags	Cisco Network Visibility Module Flow Data	T1197	ANOMALY	Cisco Network Visibility Module Analytics	2025-09-09
Cisco NVM - MSHTML or MSHTA Network Execution Without URL in CLI	Cisco Network Visibility Module Flow Data	T1218.005 T1059.005	ANOMALY	Cisco Network Visibility Module Analytics	2025-09-09
Cisco NVM - Non-Network Binary Making Network Connection	Cisco Network Visibility Module Flow Data	T1055 T1036	ANOMALY	Cisco Network Visibility Module Analytics	2025-09-09
Cisco NVM - Outbound Connection to Suspicious Port	Cisco Network Visibility Module Flow Data	T1571	ANOMALY	Cisco Network Visibility Module Analytics	2025-09-09
Cisco NVM - Rclone Execution With Network Activity	Cisco Network Visibility Module Flow Data	T1567.002	ANOMALY	Cisco Network Visibility Module Analytics	2025-09-09
Cisco NVM - Rundll32 Abuse of MSHTML.DLL for Payload Download	Cisco Network Visibility Module Flow Data	T1218.005	ANOMALY	Cisco Network Visibility Module Analytics	2025-09-09

Detection: Malicious PowerShell Process - Execution Policy Bypass

Updated Date: 2025-08-22 | ID: 9be56a82-b1cc-4318-87eb-d138afaca39 | Author: Rico Valdez, Mauricio Velazco, Splunk | Type: Anomaly | Product: Splunk Enterprise Security

Description

The following analytic detects PowerShell processes initiated with parameters that bypass the local execution policy for scripts. It leverages data from Endpoint Detection and Response (EDR) agents, focusing on command-line executions containing specific flags like "-ex" or "bypass." This activity is significant because bypassing execution policies is a common tactic used by attackers to run malicious scripts undetected. If confirmed malicious, this could allow an attacker to execute arbitrary code, potentially leading to further system compromise, data exfiltration, or persistent access within the environment.

Search

```
I tstats `security_content_summariesonly` values(Processes.process_id) as process_id, values(Processes.parent_process_id) as parent_process_id, values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where `process_powershell` AND Processes.process="* -ex*" AND Processes.process="* bypass *" by Processes.action Processes.dest Processes.original_file_name Processes.parent_process Processes.parent_process_exec Processes.parent_process_guid Processes.parent_process_id Processes.parent_process_name Processes.parent_process_path Processes.process Processes.process_exec Processes.process_guid Processes.process_hash Processes.process_id Processes.process_integrity_level Processes.process_name Processes.process_path Processes.user Processes.user_id Processes.vendor_product | `drop_dm_object_name` (Processes) | `security_content_ctime` (firstTime) | `security_content_ctime` (lastTime) | `malicious_powershell_process_execution_policy_bypass_filter`
```

Data Source

Name	Platform	Sourcetype	Source
CrowdStrike ProcessRollup2	N/A	'crowdstrike:events:sensor'	'crowdstrike'
Sysmon EventID 1	Windows	'XmlWinEventLog'	'XmlWinEventLog:Microsoft-Windows-Sysmon/Operational'
Windows Event Log Security 4688	Windows	'XmlWinEventLog'	'XmlWinEventLog:Security'

Macros Used

Name	Value
process_powershell	(Processes.process_name=pwsh.exe OR Processes.process_name=powershell.exe OR Processes.process_name=powershell.isc.exe OR Processes.original_file_name=pwsh.dll OR Processes.original_file_name=PowerShell.EXE OR Processes.original_file_name=powershell.isc.EXE)

<https://research.splunk.com/>

Event-Based Detections



Finding-Based Detections

index=risk



Finding-Based Detections

Mission Control Analytics Security content Configure Search

Enterprise Security

Queue ES-00001 ATT&CK tactic threshold exceeded over previous 7 days for system=splunkshrtcompany-1

Overview Response Events Search Automation Intelligence

Overview

ATT&CK tactic threshold exceeded over previous 7 days for system=splunkshrtcompany-1

MITRE ATT&CK map

The highlighted techniques were detected on the entity (in a finding) splunkshrtcompany-1

Detections 4 Detections in selected time range 4 Sub-Techniq... (1) Last 30 days

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
0 of 11 Techniques (0%)	0 of 8 Techniques (0%)	1 of 14 Techniques (7%)	0 of 39 Techniques (0%)	0 of 74 Techniques (0%)	0 of 41 Techniques (0%)	0 of 93 Techniques (0%)	0 of 30 Techniques (0%)	0 of 35 Techniques (0%)	0 of 20 Techniques (0%)	0 of 17 Techniques (0%)	1 of 28 Techniques (4%)	2 of 11 Techniques (18%)	0 of 20 Techniques (0%)

Exploit Public-Facing Application

Application Layer Protocol

Data Compressed

Data Transfer Size Limits

Intermediate findings

Timeline

Entity splunkshrtcompany-1 80 Finding score 490 Intermediate findings count 7

Asset splunkshrtcompany-1 +3 Priority Critical DNS splunkshrtcompany-1 Owner jeremiah wortoski Business unit ecomm Category magento +2 City San Francisco

Timeline Threat topology

Scroll to zoom

90
80
70
50
0

00:00 04:00 08:00 12:00 16:00 20:00 00:00 04:00 08:00 12:00 16:00 20:00

Tue 10 March Wed 11 March Thu 12 March

An unusual volume of outbound network activity ...

An unusual volume of outbound network activity ...

An unusual volume of outbound network activity ...

An unusual volume of outbound network activity ...

Possible Exploitation of Public-Facing Applicatio...

Command and Control via External Communicati...

Command and Control via External Communicati...

Owner lily thomson Status In Progress

Urgency High Sensitivity Unassigned

Disposition Undetermined

Apply changes to included findings

ID ES-00001

Type Investigation

Time Mar 11th, 2026 9:03 AM

Last updated Mar 11th, 2026 9:06 AM

Reference ID 5c3f252a-448a-4c13-b5d0-6a68fc0f62c2

Investigation type default

Description ATT&CK tactic threshold exceeded for an object over the previous 7 days

Notes

Show all

es_soar_integration_user Mar 11, 9:02 AM

ATT&CK tactic threshold exceeded over previous 7 days for...
SOAR Analysis for: splunkshrtcompany-1

Splunk Enterprise Security has detected that system 'splunkshrtcompany-1' generated 490.0 points of risk.

Full statistics and timeline on this user's risk behavior can be found [here](#)

MITRE ATT&CK

Splunk SOAR has aggregated and aligned the following risk rules to ATT&CK Tactics and Techniques.

Initial Access

Exploit Public-Facing Application: T1190

Edit event-based detection

[Back to Content management](#)

Event-based detection

Finding details

Entities

Threat objects

Annotations

Time range

Conditions

Throttling

Adaptive response

1 Event-based detection

* Name ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule

App ES Content Updates

UI dispatch context None

App configured for drill-down search links or email adaptive response actions. If no app is selected, the UI app context is used by default.

* Description The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228 by correlating multiple MITRE ATT&CK tactics detected in risk events. It leverages Splunk's risk data model to calculate the distinct count of MITRE ATT&CK tactics from Log4Shell-related detections. This activity is significant because it indicates a high probability of exploitation if two or more distinct tactics are observed. If confirmed malicious, this activity could lead to initial payload delivery, callback to a malicious server, and post-exploitation activities, potentially resulting in unauthorized access, lateral movement, and further compromise of the affected systems.

Add information on what the detection searches for and the security use case addressed by the detection. For example: Identify excessive number of failed login attempts (likely to detect a brute force attack).

Mode Guided Manual

```
* Search | tstats 'security_content_summariesonly' min(_time) as firstTime max(_time) as lastTime sum(All_Risk.calculated_risk_score) as risk_score, count(All_Risk.calculated_risk_score) as risk_event_count, values(All_Risk.annotations.mitre_attack.mitre_tactic_id) as annotations.mitre_attack.mitre_tactic_id, dc(All_Risk.annotations.mitre_attack.mitre_tactic_id) as mitre_tactic_id_count, values(All_Risk.annotations.mitre_attack.mitre_technique_id) as annotations.mitre_attack.mitre_technique_id, dc(All_Risk.annotations.mitre_attack.mitre_technique_id) as mitre_technique_id_count, values(All_Risk.tag) as tag, values(source) as source, dc(source) as source_count from datamodel=Risk.All_Risk where All_Risk.analyticstories="Log4Shell CVE-2021-44228" All_Risk.risk_object_type="system" by All_Risk.risk_object All_Risk.risk_object_type All_Risk.annotations.mitre_attack.mitre_tactic | 'drop_dm_object_name(All_Risk)' | 'security_content_ctime(firstTime)' | 'security_content_ctime(lastTime)' | where source_count >= 2 | 'log4shell_cve_2021_44228_exploitation_filter'
```

2 Finding details

The following information applies to a finding produced by this detection.

* Title RBA: Log4Shell CVE-2021-44228 Exploitation

Enter optional note...

Status On Clone

Save as new version

Details

Type	Event-based detection
ID	9be30d80-3a39-4df9-9102-64a467b24eac
Cloned from	--
Title	ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
Description	The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228 by correlating multiple MITRE ATT&CK tactics detected in risk events. It leverages Splunk's risk...
Author	--
Automation rule	--

Versions 8

12/9/24, 10:46 PM
Version created by Splunk

4.2 4.1

10/18/24, 10:24 PM
Version created from 4.1

4.2 4.1

10/18/24, 10:24 PM
Version created from 4.1

4.1

10/18/24, 10:07 PM
Version created by Splunk

4.1

10/18/24, 10:07 PM

Edit event-based detection

[Back to Content management](#)

App	Event-based detection	Version
ES Content Updates	ESCU - Log4Shell CVE-2021...	4.1

```

1 action.correlationsearch.annotations: {"analytic_story": ["CISA AA22-320A", "Log4Shell CVE-2021-44228 Exploitation - Rule"]}
2 action.correlationsearch.enabled: 1
3 action.correlationsearch.label: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
4 action.correlationsearch.metadata: {"detection_id": "9be30d80-3a39-4df9-9102-64a467b24eac", "description": "This is used to add a new backfill to the backlog."}
5 action.detection_backfill_add_a_backfill_to_the_backlog.description: This is used to add a new backfill to the backlog.
6 action.detection_backfill_add_a_backfill_to_the_backlog.label: Detection: Add a backfill to the backlog.
7 action.detection_backfill_add_a_backfill_to_the_backlog.param._cam: {"technology": [{"vendor": "Splunk"}]}
8 action.detection_backfill_run_the_next_backfill.label: Detection: Run the next backfill
9 action.detection_backfill_run_the_next_backfill.param._cam: {"technology": [{"product": "Detection Backfill"}]}
10 action.detection_backfill_run_the_next_backfill.param.trigger: 0
11 action.email.footer.text: If you believe you've received this email in error, please see your Splunk account page at https://splunk.com/privacy.
12
13 splunk>
14 action.email.pdf.header_left:
15 action.email.pdf.header_right:
16 action.escu: 0
17 action.escu.analytic_story: ["CISA AA22-320A", "Log4Shell CVE-2021-44228"]
18 action.escu.confidence: high
19 action.escu.creation_date: 2024-05-26
20 action.escu.data_models: ["Risk"]
21 action.escu.elid: The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228.
22 action.escu.enabled: 1
23 action.escu.full_search_name: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
24 action.escu.how_to_implement: To implement this correlation search a user needs to enable all detection rules in the detection rule set.
25 action.escu.known_false_positives: There are no known false positive for this search, but it could be affected by false positives from other searches.
26 action.escu.mappings: {"cis20": ["CIS 10"], "kill_chain_phases": ["Command and Control", "Deliver Payload"]}
27 action.escu.modification_date: 2024-05-26
28 action.escu.product: ["Splunk Enterprise", "Splunk Enterprise Security", "Splunk Cloud"]
29 action.escu.providing_technologies: null
30 action.escu.search_type: detection
31 action.notable: 1
32 action.notable.param.entities: [{"risk_object_field": "N/A", "risk_object_type": "N/A", "risk_object_value": ""}]
33 action.notable.param.drilldown_searches: []
34 action.notable.param.nes_fields: user,dest
35 action.notable.param.rule_description: The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228.
36 action.notable.param.rule_title: RBA: Log4Shell CVE-2021-44228 Exploitation
37 action.notable.param.security_domain: endpoint
38 action.notable.param.severity: high
39 action.risk.param.risk: []
40 action.send_notable_to_mc_alert_action: 1

```

Event-based detection	Version
ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule	4.2

```

1 action.correlationsearch.annotations: {"analytic_story": ["CISA AA22-320A", "Log4Shell CVE-2021-44228 Exploitation - Rule"]}
2 action.correlationsearch.enabled: 1
3 action.correlationsearch.label: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
4 action.correlationsearch.metadata: {"detection_id": "9be30d80-3a39-4df9-9102-64a467b24eac", "description": "This is used to add a new backfill to the backlog."}
5 action.detection_backfill_add_a_backfill_to_the_backlog.description: This is used to add a new backfill to the backlog.
6 action.detection_backfill_add_a_backfill_to_the_backlog.label: Detection: Add a backfill to the backlog.
7 action.detection_backfill_add_a_backfill_to_the_backlog.param._cam: {"technology": [{"vendor": "Splunk"}]}
8 action.detection_backfill_run_the_next_backfill.label: Detection: Run the next backfill
9 action.detection_backfill_run_the_next_backfill.param._cam: {"technology": [{"product": "Detection Backfill"}]}
10 action.detection_backfill_run_the_next_backfill.param.trigger: 0
11 action.email.footer.text: If you believe you've received this email in error, please see your Splunk account page at https://splunk.com/privacy.
12
13 splunk>
14 action.email.pdf.header_left:
15 action.email.pdf.header_right:
16 action.escu: 0
17 action.escu.analytic_story: ["CISA AA22-320A", "Log4Shell CVE-2021-44228"]
18 action.escu.confidence: high
19 action.escu.creation_date: 2024-05-26
20 action.escu.data_models: ["Risk"]
21 action.escu.elid: The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228.
22 action.escu.enabled: 1
23 action.escu.full_search_name: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
24 action.escu.how_to_implement: To implement this correlation search a user needs to enable all detection rules in the detection rule set.
25 action.escu.known_false_positives: There are no known false positive for this search, but it could be affected by false positives from other searches.
26 action.escu.mappings: {"cis20": ["CIS 10"], "kill_chain_phases": ["Command and Control", "Deliver Payload"]}
27 action.escu.modification_date: 2024-05-26
28 action.escu.product: ["Splunk Enterprise", "Splunk Enterprise Security", "Splunk Cloud"]
29 action.escu.providing_technologies: null
30 action.escu.search_type: detection
31 action.notable: 1
32 action.notable.param.entities: [{"risk_object_field": "N/A", "risk_object_type": "N/A", "risk_object_value": ""}]
33 action.notable.param.drilldown_searches: []
34 action.notable.param.nes_fields: user,dest
35 action.notable.param.rule_description: The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228.
36 action.notable.param.rule_title: RBA: Log4Shell CVE-2021-44228 Exploitation
37 action.notable.param.security_domain: endpoint
38 action.notable.param.severity: high
39 action.risk.param.risk: []
40 action.send_notable_to_mc_alert_action: 1

```

Details

Type	Event-based detection
ID	9be30d80-3a39-4df9-9102-64a467b24eac
Cloned from	--
Title	ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
Description	The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228 by correlating multiple MITRE ATT&CK tactics detected in risk events. It leverages Splunk's risk...
Author	--
Automation rule	--

Versions 8

- Version created by Splunk
- 4.2 10/18/24, 10:24 PM
Version created from 4.1
- 4.2 10/18/24, 10:24 PM
Version created from 4.1
- 4.1 10/18/24, 10:07 PM
Version created by Splunk
- 4.1 10/18/24, 10:07 PM
Version created by Splunk

Detection Testing and Validation

The **Splunk Attack Range** is an open-source project maintained by the Splunk Threat Research Team. It builds instrumented cloud (AWS, Azure) and local environments (Virtualbox), simulates attacks, and forwards the data into a Splunk instance. This environment can then be used to develop and test the effectiveness of detections.



https://github.com/splunk/attack_range

Detection Studio

Powered by SnapAttack

- Streamline detection creation workflows
- Evaluate detection health
- Expand versioning and detection-as-code

The screenshot displays the Splunk Security content dashboard for 'Security content' under 'Detections'. The interface includes a left sidebar with filters for Quick filters, Detection KPIs, Recommended, Priority, Confidence, Impact, Compatibility, Performance, Detection Config, Deployed State, Finding Type, Data, Modeled Data, and Un-Modeled Data. The main content area features a 'Detections' search bar and three key metrics: Overall detection technique coverage (65% ↑ 5%), Highest priority detections (72), and Lowest health detections (28). Below these metrics is a table of detection rules with columns for Name, Priority, Impact, Compatibility, Performance, Deployed State, and Actions. The table lists various rules such as 'ESCU - Any...', 'ESCU - CMD Echo Pipe - Eastern...', 'ESCU - Detect RClone Command-Line Usage IF Only - Rule - Rule', 'ESCU - Disable Schedule Task IF Only - Rule - Rule', 'ESCU - Registry Keys Used For Persistence IF Only - Rule - Rule', 'ESCU - Windows Sensitive Registry Hive Dump Via CommandLine IF Only - Rule - Rule', 'ESCU - ICACLS Grant Command - Rule', 'ESCU - Network Discovery Using Route Windows App - Rule', 'ESCU - PowerShell Get LocalGroup Discovery - Rule', 'Cisco Network Interface Modifications', and 'Cisco Secure Firewall - Static Tundra Smart Install Abuse'. The right sidebar shows details for the selected rule 'ESCU - ICACLS Grant Command - Rule', including its description, priority (High), and detection logic.

05

Powering the Future SOC

What defines a Future-Ready SOC?



Agentic and automated



Unified and integrated



Analyst-centric and intuitive

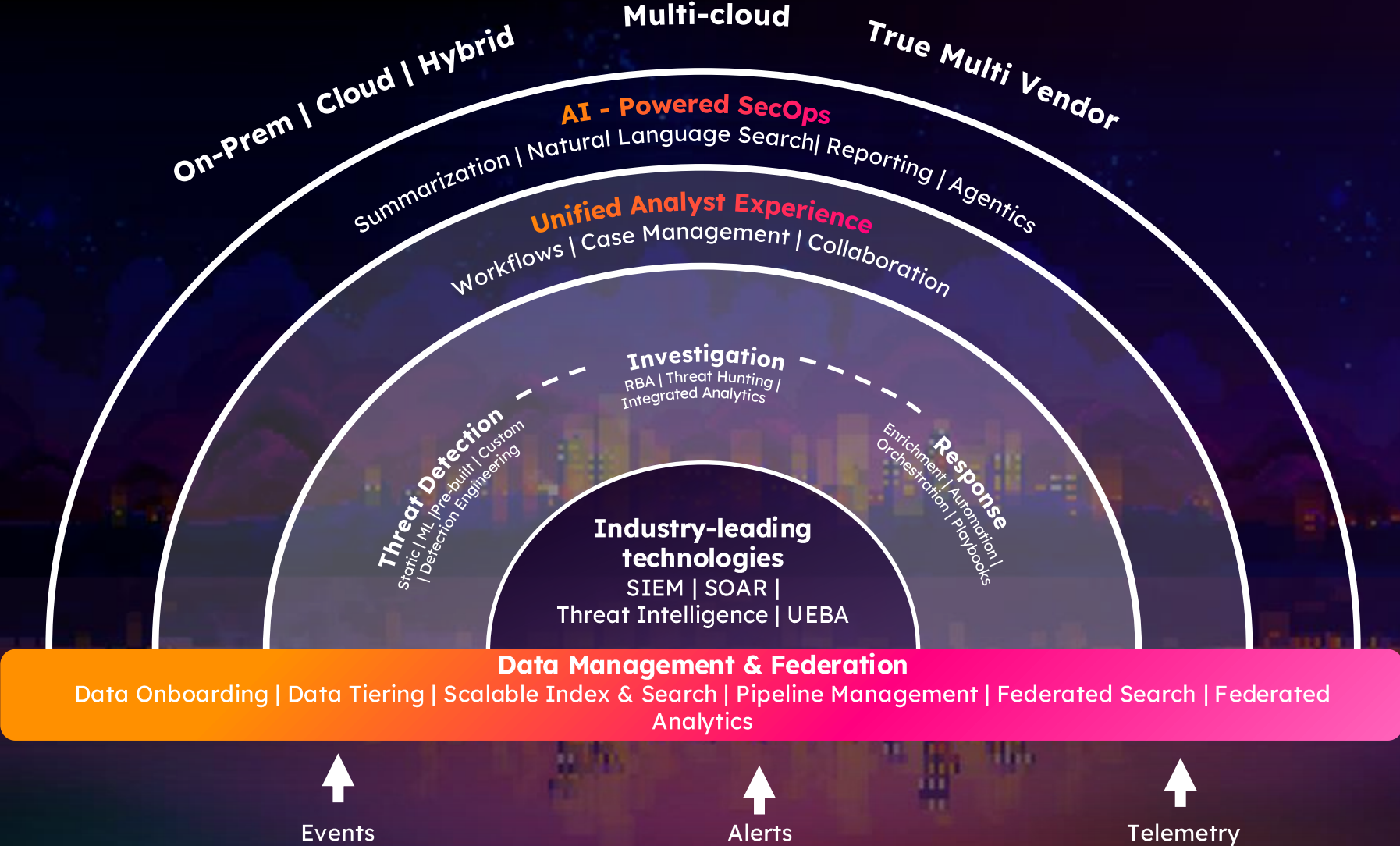


Context-driven and riskbased



Resilient and scalable

Unified TDIR in an AI-Powered SOC Platform



Do more with less.

ES 8 delivers the unified TDIR platform

Better Signal to Noise

- Cut through alert fatigue with Risk-based alerting
- MITRE-mapped detections from Splunk Threat Research Team
- Native Findings grouping

Richer Context

- Real-time threat intelligence alongside alerts „in the moment“
- Tune without breaking production
- AI-Powered Finding explanations and Investigation Reports

Faster Decision

- Built-in Response Plans that streamline investigations and automation
- Unified SOAR for automated enrichment and remediation actions



The SOC Has Changed. Has Yours?

Thank You!

Contact Us

Marcel Tanuatmadja

mtanuatm@cisco.com

Roberta Geyer

robertag@cisco.com

