From Zero to Future SOC

Mastering the Journey from Project Kickoff to Security Operations Excellence

splunk> a cisco company

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> a CISCO company

Defending The Galaxy, One Log at a Time

Agenda

01 The SOC Journey Begins

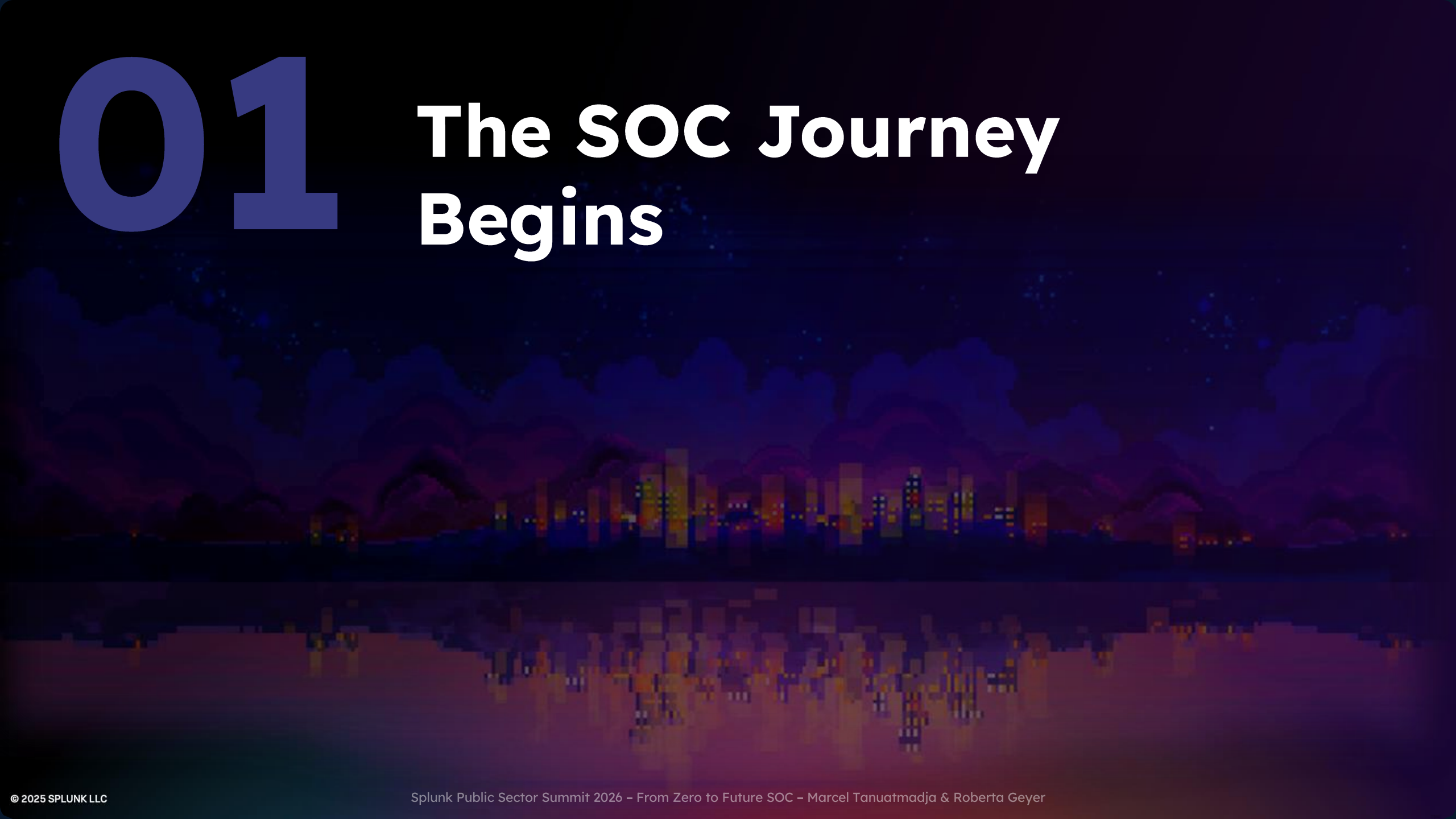
02 SOC Project Kickoff: From Idea to Impact

03 People Make the SOC

04 Anatomy of a Cyberattack and Detection Engineering

05 Powering the Future SOC

01 The SOC Journey Begins



heise online heise+ entdecken

Claude: AI chatbot used for cyberattack on Mexican government

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

Cyber Security News

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.

AI is reshaping the threat landscape

AI-Generated Malware and Exploits

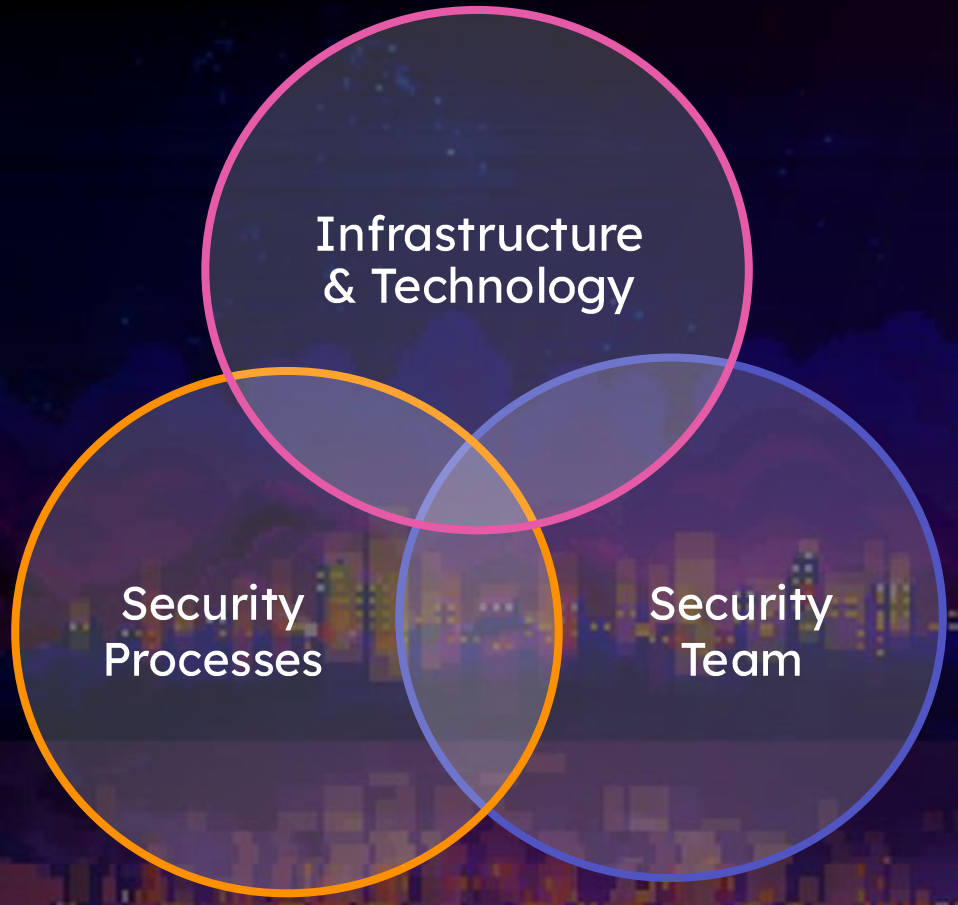
AI-Augmented Reconnaissance

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.**

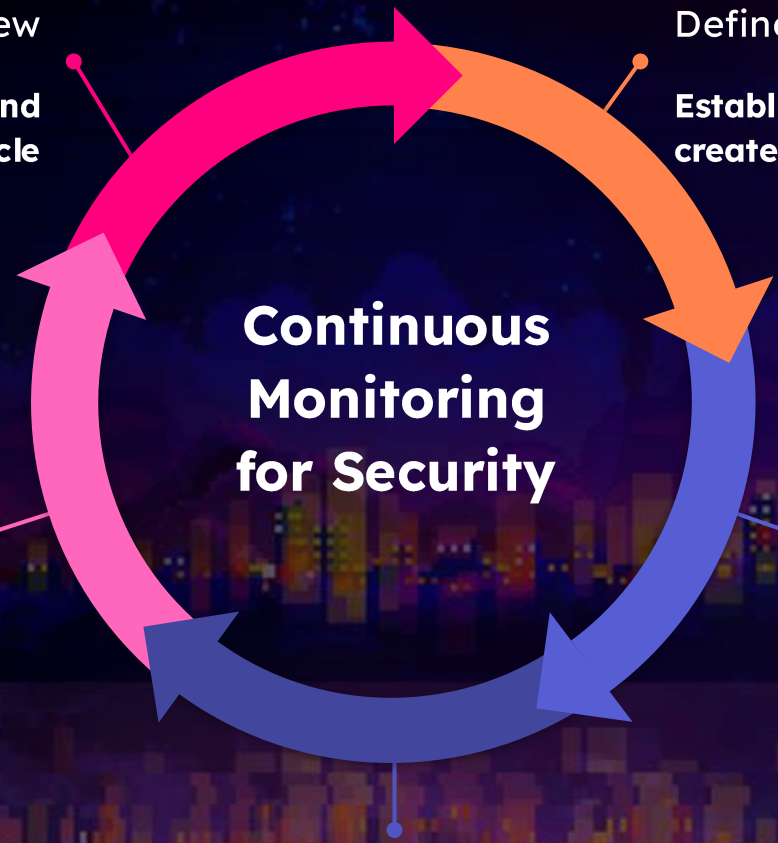
You need a Security Program

A Charter for Your Security Program

“what?”	“from what?”	“if you don’t?”	“how likely?”
Asset Inventory, Architecture	Vulnerabilities, Threats.	Impact	Likelihood

Risk = Impact X Likelihood

Continuous Monitoring as Security Program



Define and Predict

Establish risk, vulnerability, create hypothesis.

Establish and Architect

Establish frequency, determine requirements.

Implement and Collect

Add assets, identities, sources, dashboards, searches and reports

Analyze and Report

View data and results, search based on hypothesis

Respond and Review

Mitigate as needed, review findings and make recommendations for next cycle

Splunk Best-Practice Delivery Model for SOC Projects

Plan & Prepare

- Project Methodology and ongoing cadence
- Agree Deliverable Outline
- Create and agree delivery plan
- Project ramp up and resourcing

Analysis & Design

- SIEM Architecture Workshop
- Solution Design
- RBA Design
- Design Documentation
- Detailed Project Plan

Build

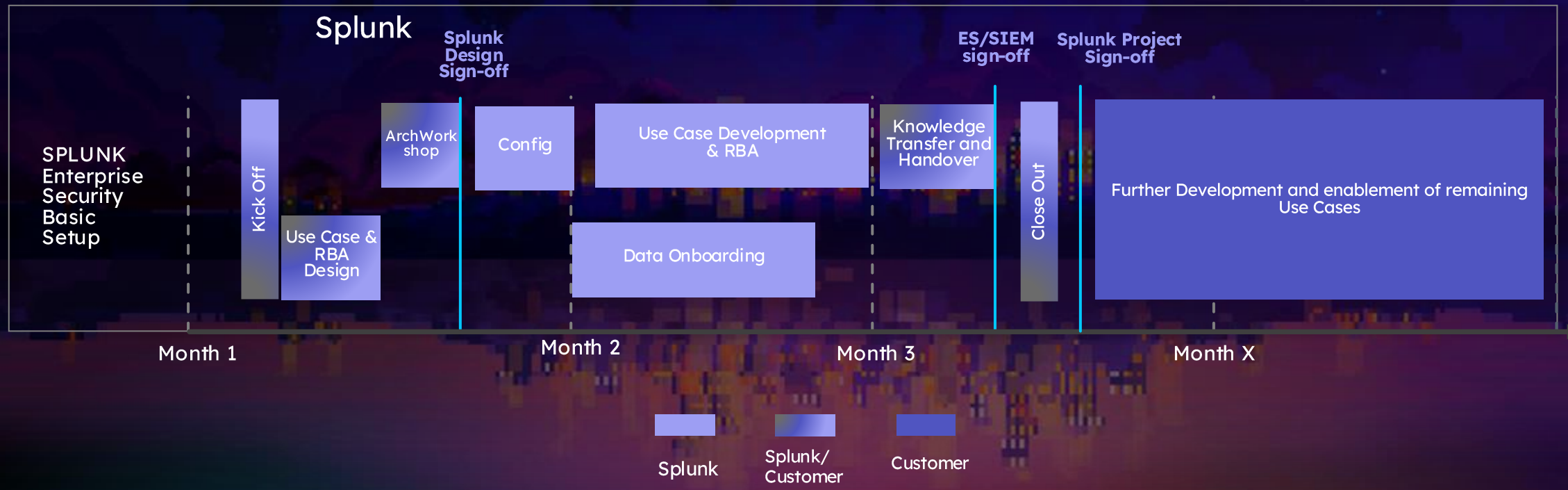
- Implementation of agreed SIEM solution
- Monitor progress against plan
- Onboard Data sources
- Implement Correlation Searches
- Implement RBA

Validate

- Execute agreed validation plan
- Remediate agreed issues

Close Out

- Complete Project Closeout Checklist
- Project Sign Off



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

Step 1: Crawl -Data Collection & Ingestion

- ✓ Prevention Focused
- ✓ Firewall and Endpoint Security
- ✓ Manual Remediation
- ✓ Standard use case focused

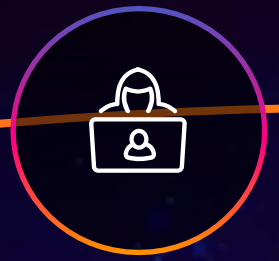
Step 2: Walk - Monitoring & Detection

- ✓ Log aggregation and retention
- ✓ Enhancing with Threat Intelligence
- ✓ Custom use cases
- ✓ Custom dashboards

Step 3: Run - Investigation & Response

- ✓ Alert Prioritization
- ✓ Threat hunting
- ✓ Custom reporting
- ✓ Needing faster responses
- ✓ Deeper analysis and context

Step 4: Fly - Optimization & Automation



- ✓ Behavioral analytics
- ✓ User Anomalies
- ✓ Expanding use cases
- ✓ Adversarial Simulation
- ✓ Insider Threat detections

Level 5 Security Operations

Target Feature set

splunk> platform

The SOC Maturity Journey

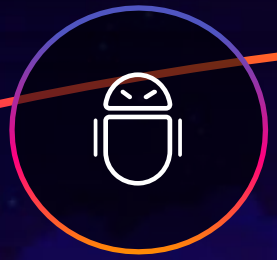
Step 1: Crawl -Data Collection & Ingestion

- ✓ Core Splunk
- ✓ Splunk Security Essentials app
- ✓ InfoSec app
- ✓ Cisco XDR

Step 2: Walk - Monitoring & Detection

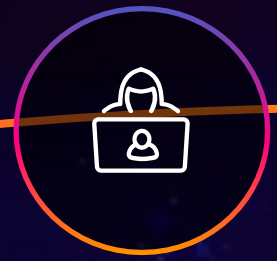
- ✓ Splunk Enterprise Security (ES)
- ✓ Splunk TIM
- ✓ Content Update (ESCU)
- ✓ SA-Investigator APP

Step 3: Run - Investigation & Response



- ✓ Splunk RBA
- ✓ Splunk PCI app
- ✓ Compliance Essentials
- ✓ Splunk Attack Analyzer
- ✓ Splunk Asset and Risk Intelligence (ARI)
- ✓ SOAR

Step 4: Fly - Optimization & Automation



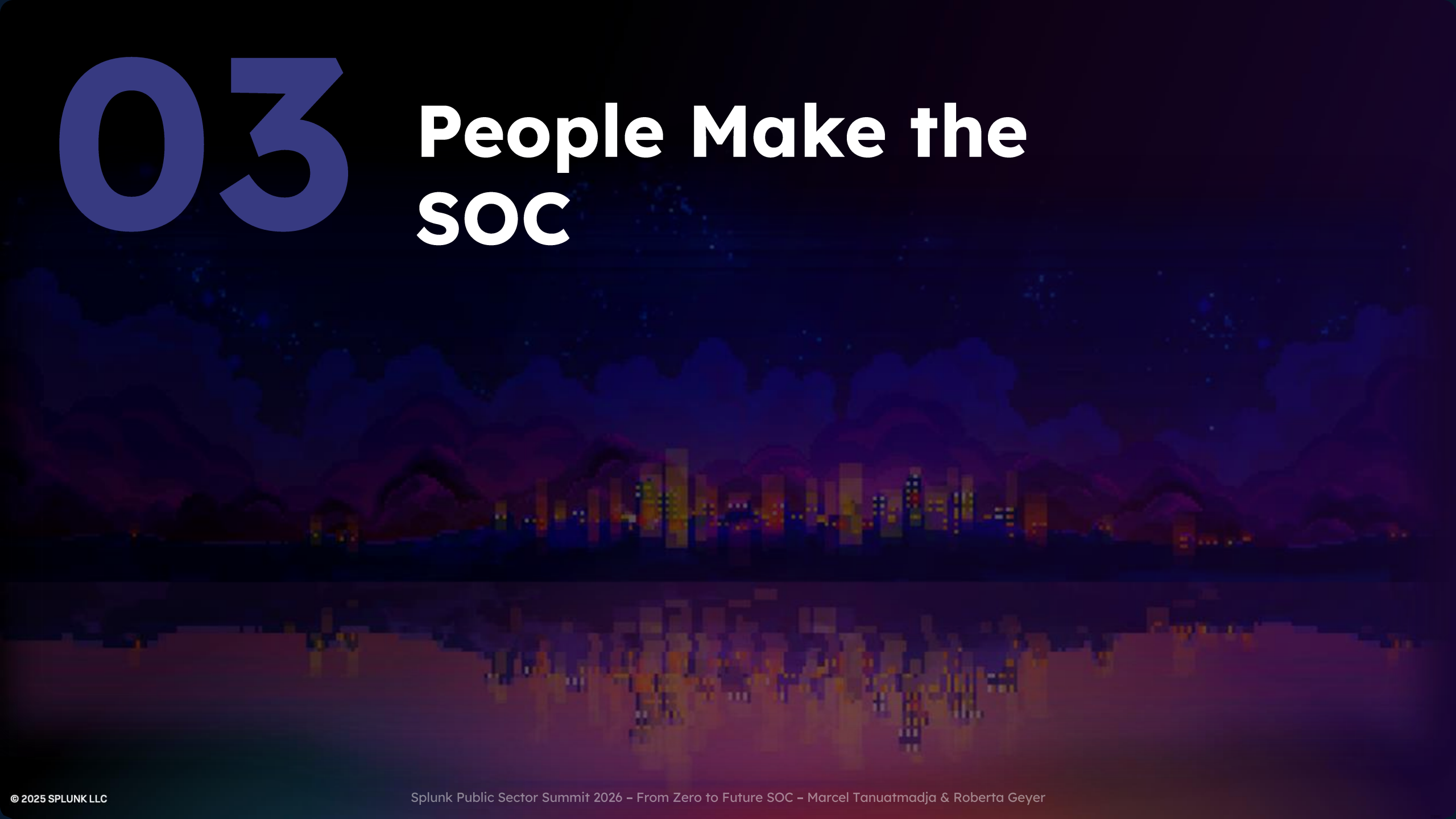
- ✓ Splunk Behavior Analytics
- ✓ Automations & Case Management within SOAR
- ✓ Splunk app for O/T
- ✓ Splunk app for Fraud

Level 5 Security Operations

Target Feature set

splunk> platform

03 People Make the SOC

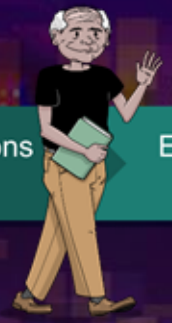


SOC Roles and Responsabilities

Security Tools

Analyst

Investigate Notable Events → Research and identify indicators → Follow Runbooks → Identify True/False positive events



Engineer

Create and test detections (Notables) → Evaluate and ingest sources of Threat Intelligence → Improve Detection Performance

Architect

Choose and Implement security tools and solutions → Work with admins to get data, assets and identities into the SIEM → Improve security operations performance

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

UBA Hands-On	Enterprise Security (ESHO)	AWS Hands-On	SSE (Security Essentials)	Monitoring K8s	Building Correlation Searches
Insider Threat Hands-On	SOAR Hands-On	GCP in Splunk	Splunking the Endpoint	Splunking for Fraud	Advanced APT Hunting
Security Lunch n' Learn	Security Operations Suite Hands-On	Hunting in the MS Cloud	Investigating with Splunk	Risk Based Alerting Hands-On	Threat Hunting an APT: A New Adversary

Boss of the SOC - Competition

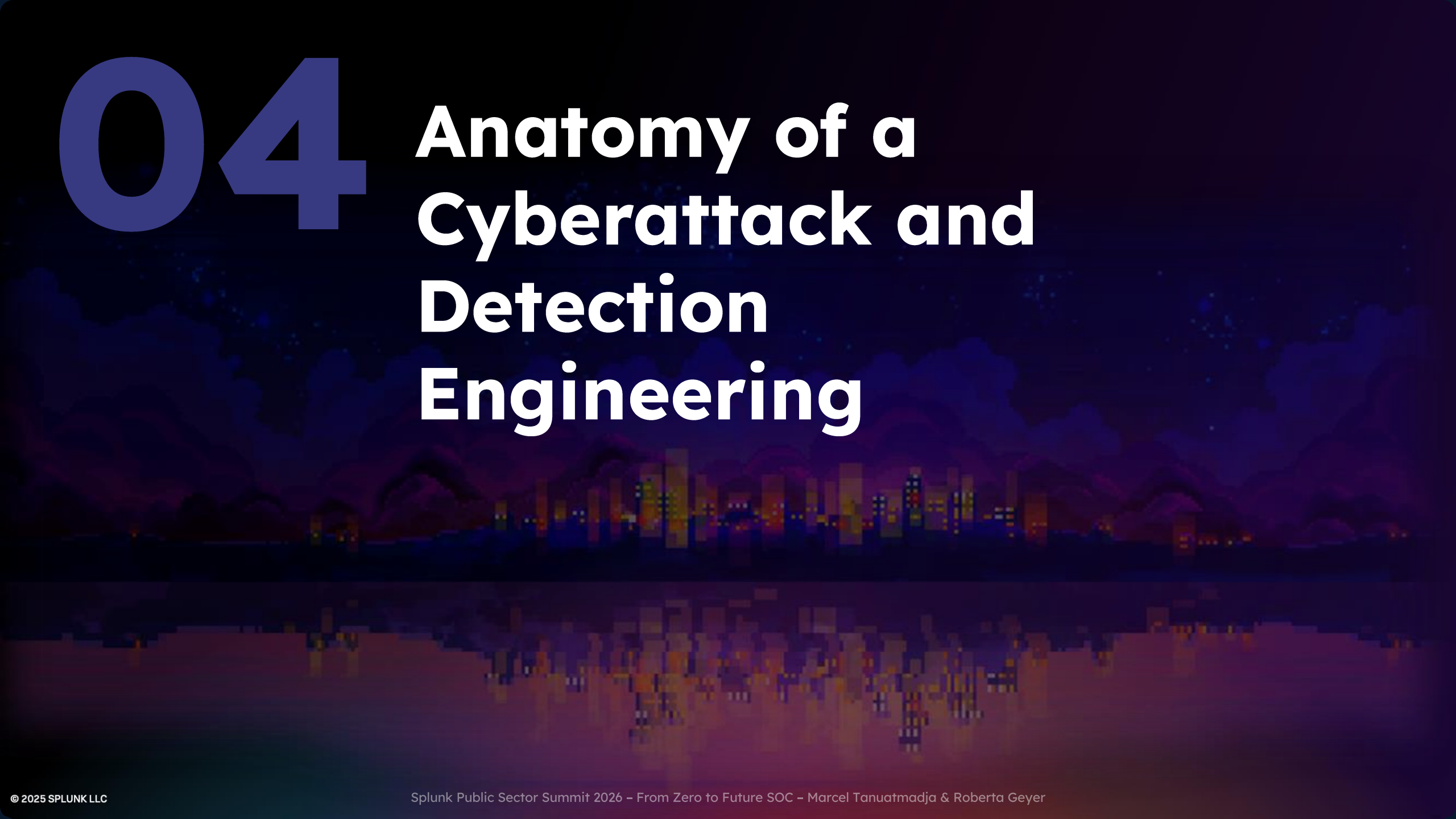
Splunk Enterprise/Cloud | Enterprise Security | SOAR | UBA

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.

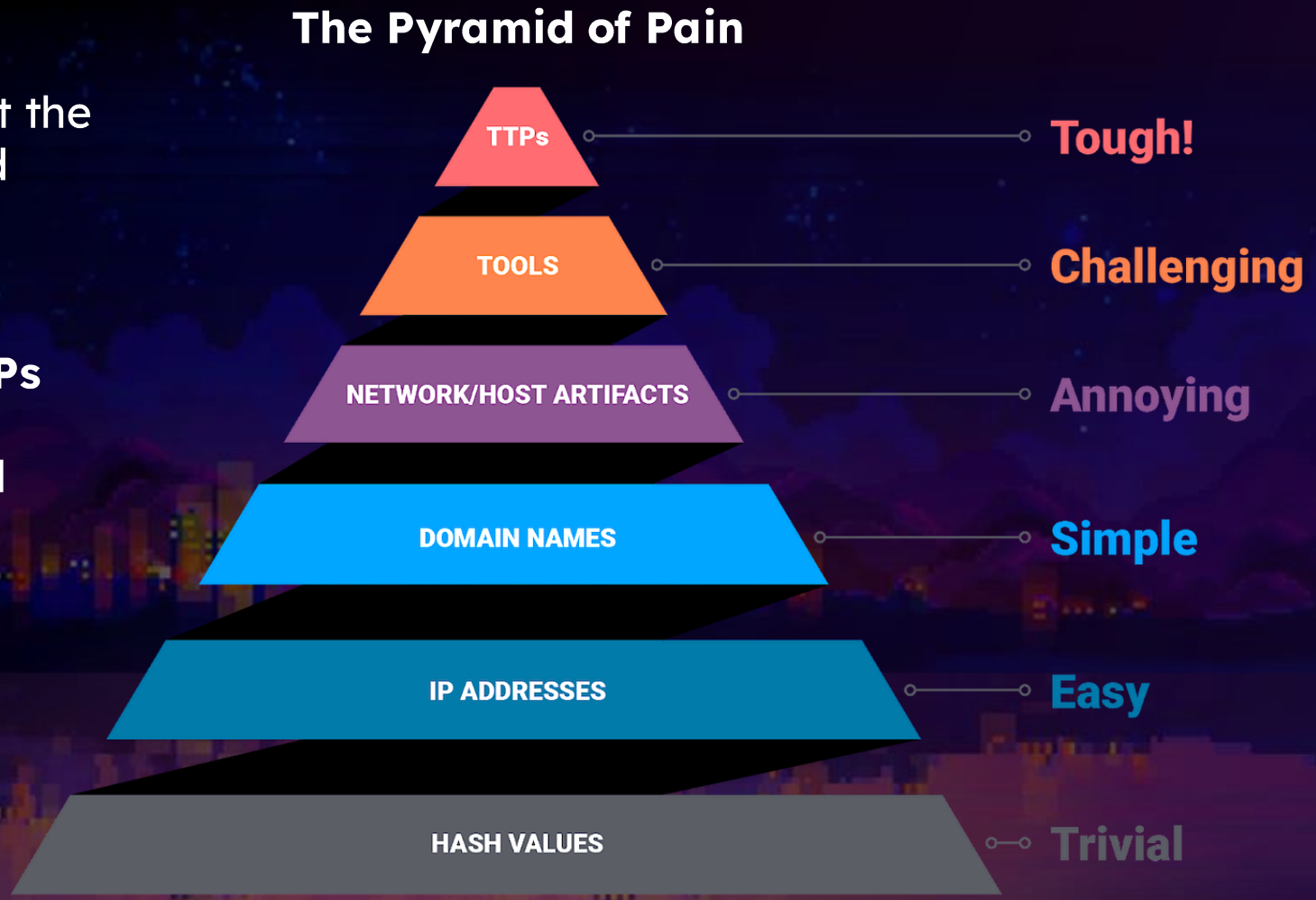
Tactics, Techniques and Procedures

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

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

Low levels = easy to swap, minimal impact

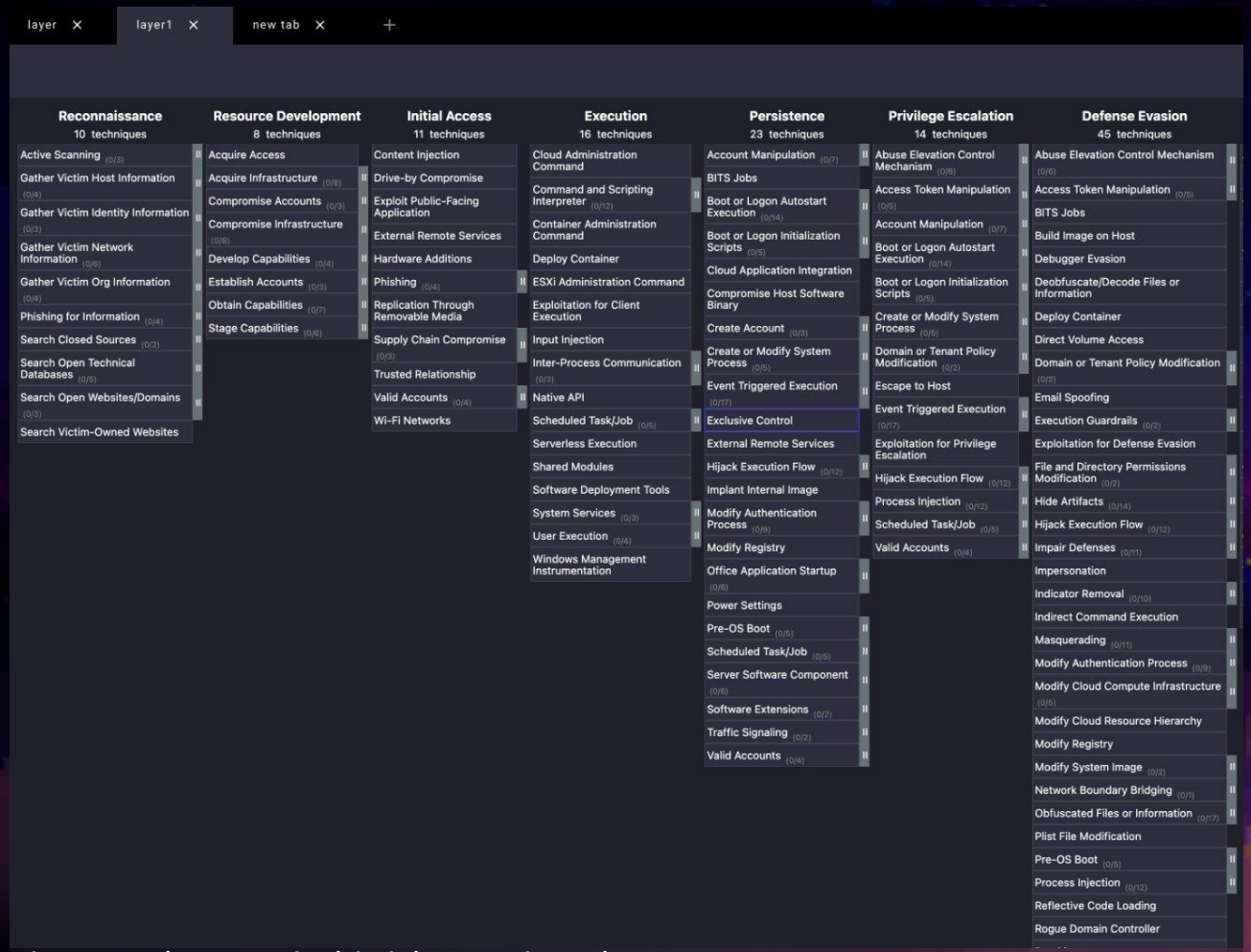
Focus on **behavior/TTP-based** detections and hunting



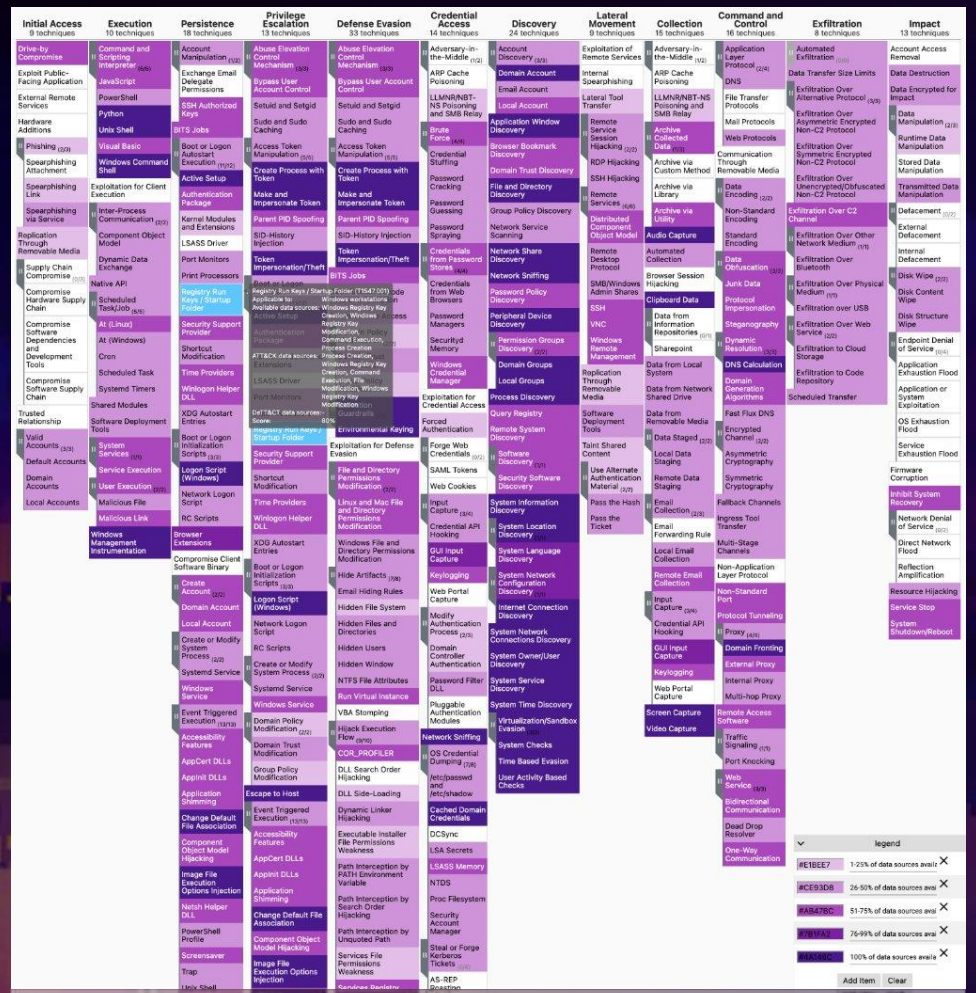
How to find the right Content

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**

Leverage MITRE ATT&CK

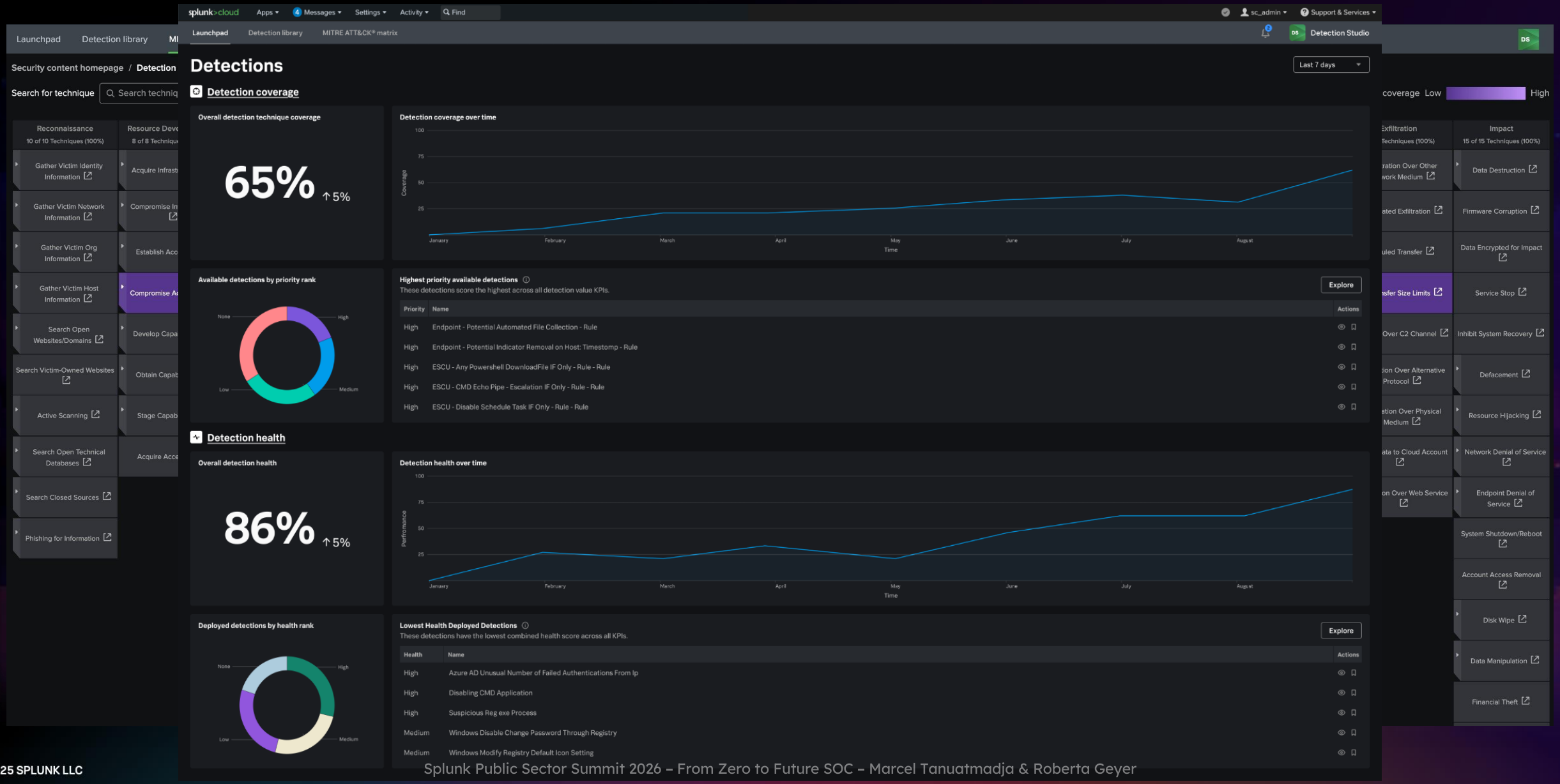


https://mitre-attack.github.io/attack-navigator/



https://github.com/rabobank-cdc/DeTTECT

Leverage MITRE ATT&CK with Splunk Detection Studio



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**

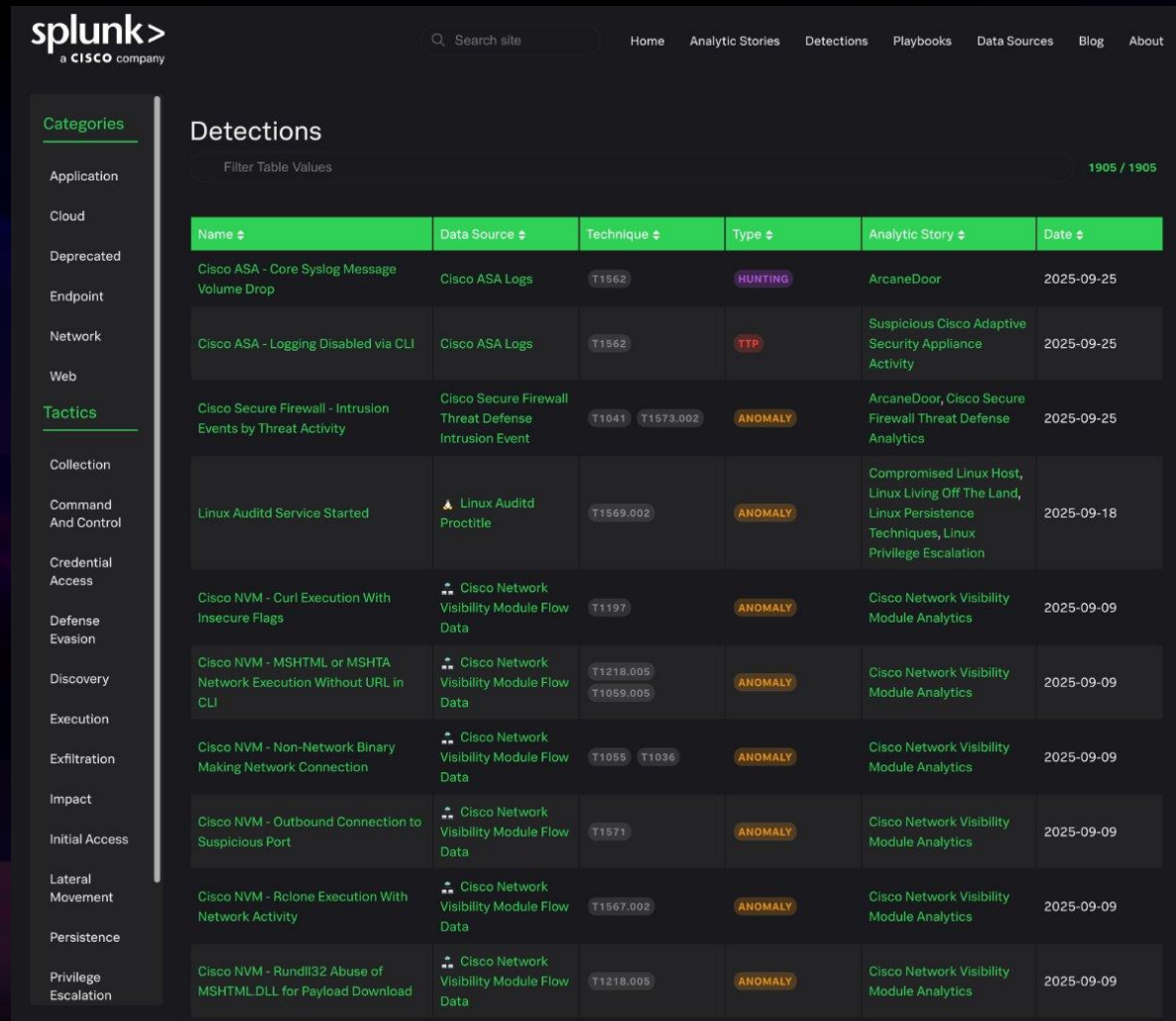
Time	Title	Type	Entity	Entity priority	Risk score	Urgency	Status	Actions
Yesterday, 7:03 AM	User pcerf@splunktshirtcompany.com has started traffic to a monitored site	FINDING	pcerf@splunktshirtcompany.com	high	20	Medium	In Progress	

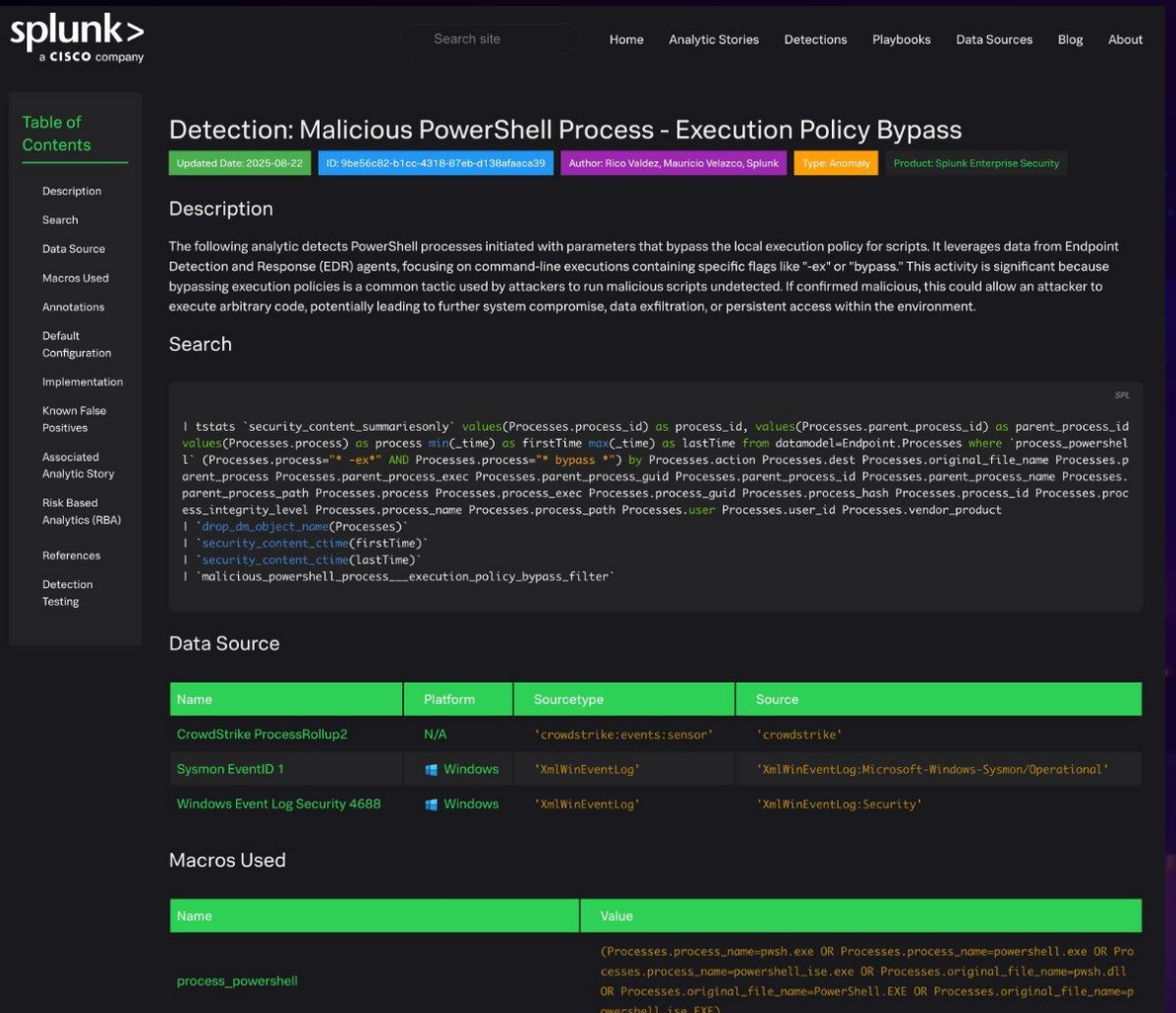
Assigned Severity

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





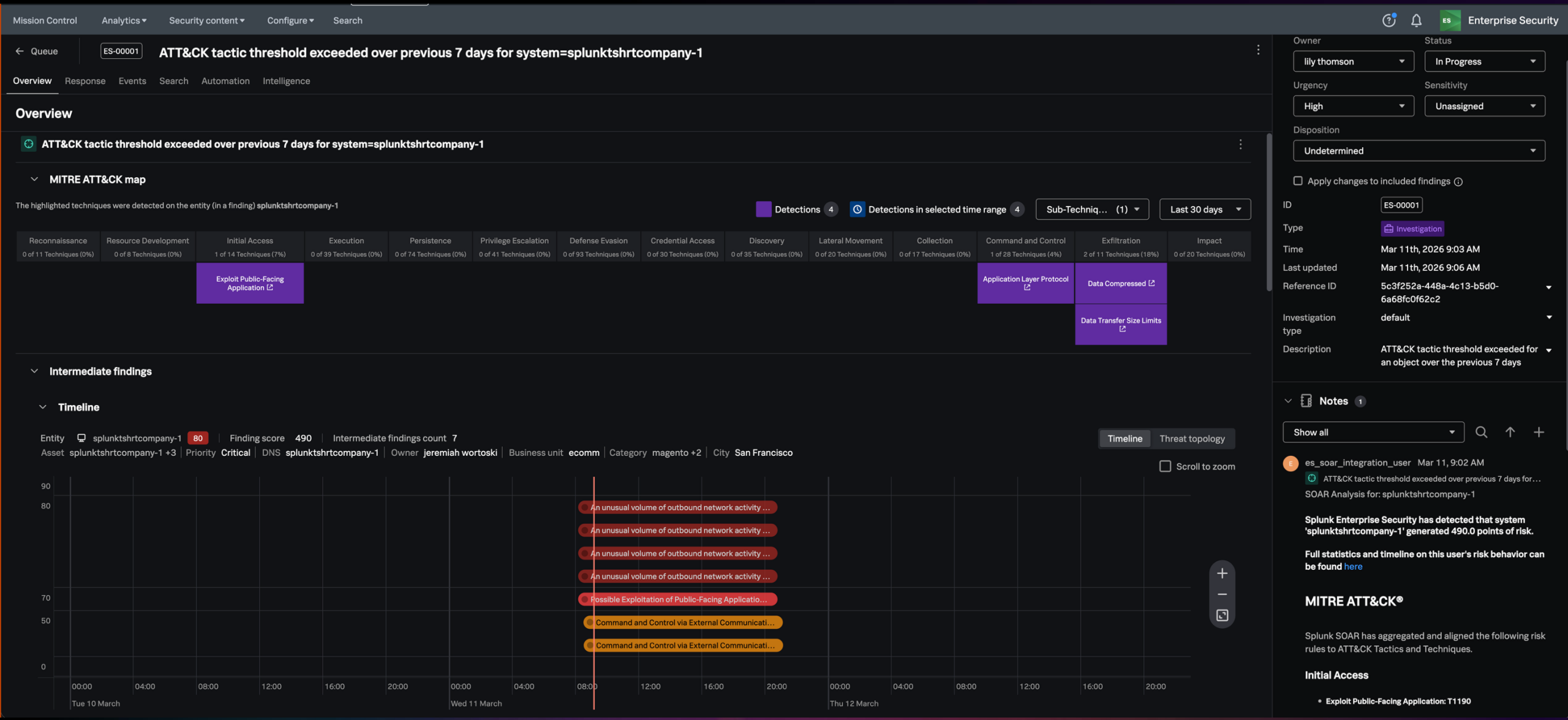
https://research.splunk.com/

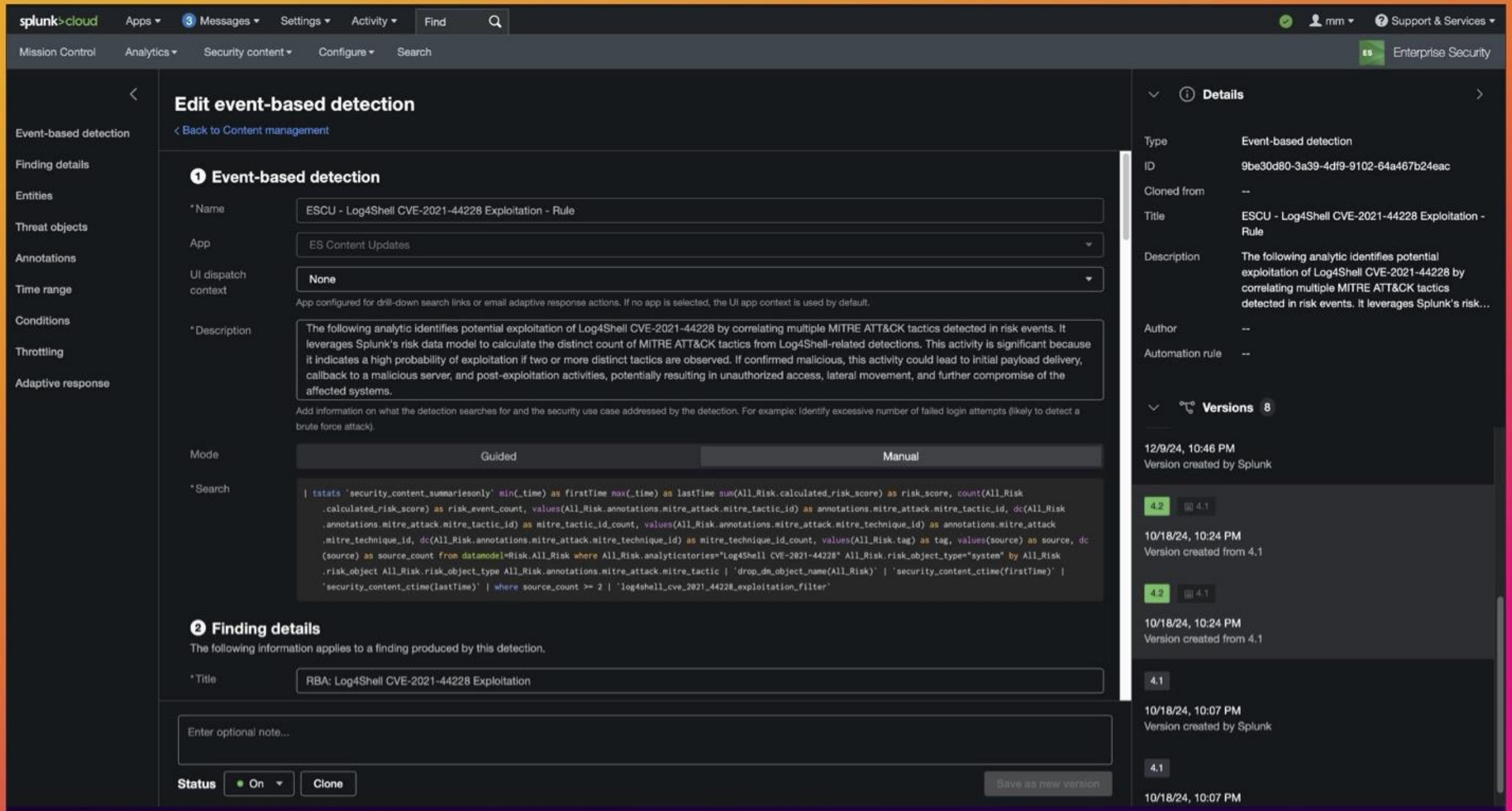
Event-Based Detections

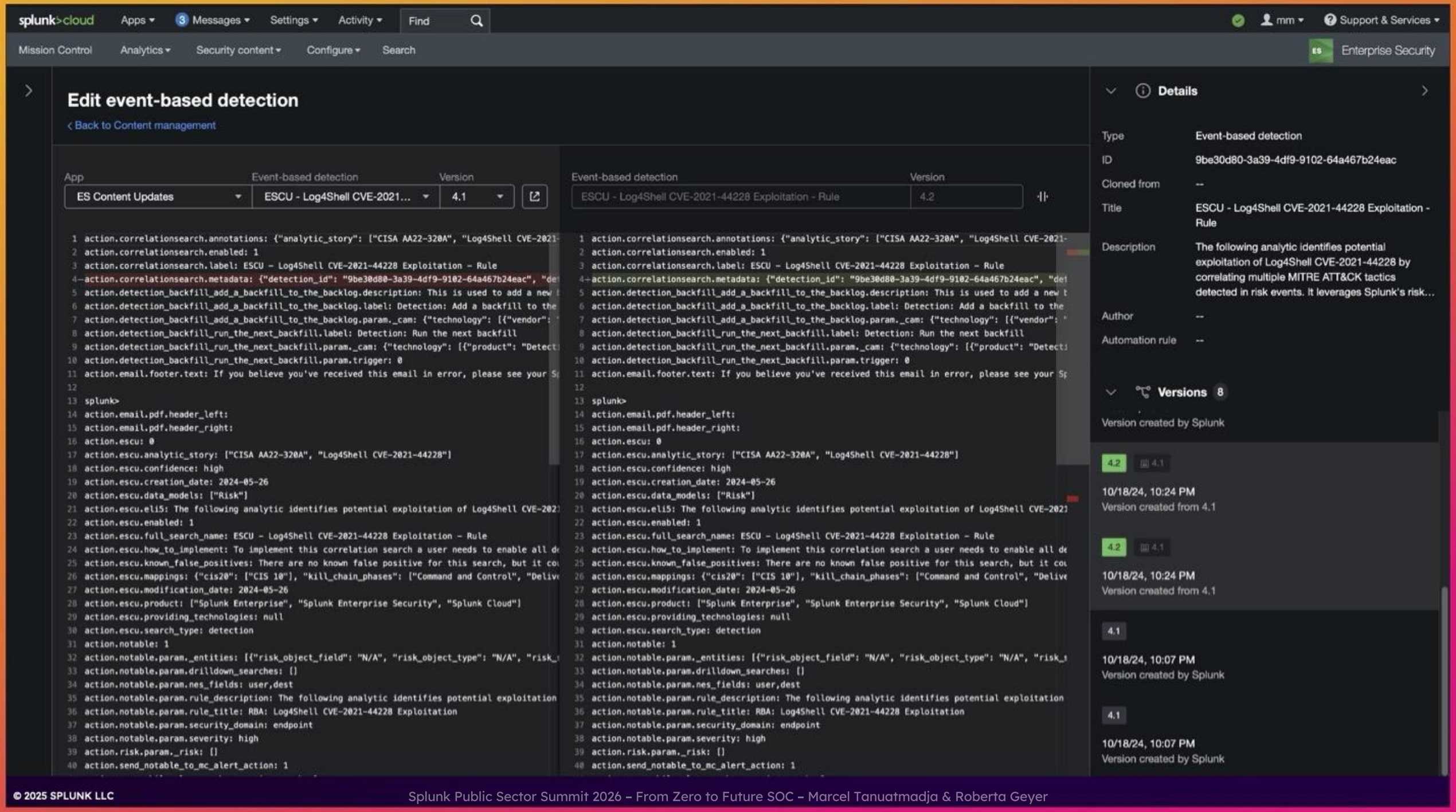
Finding-Based Detections

index=risk

Finding-Based Detections







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.

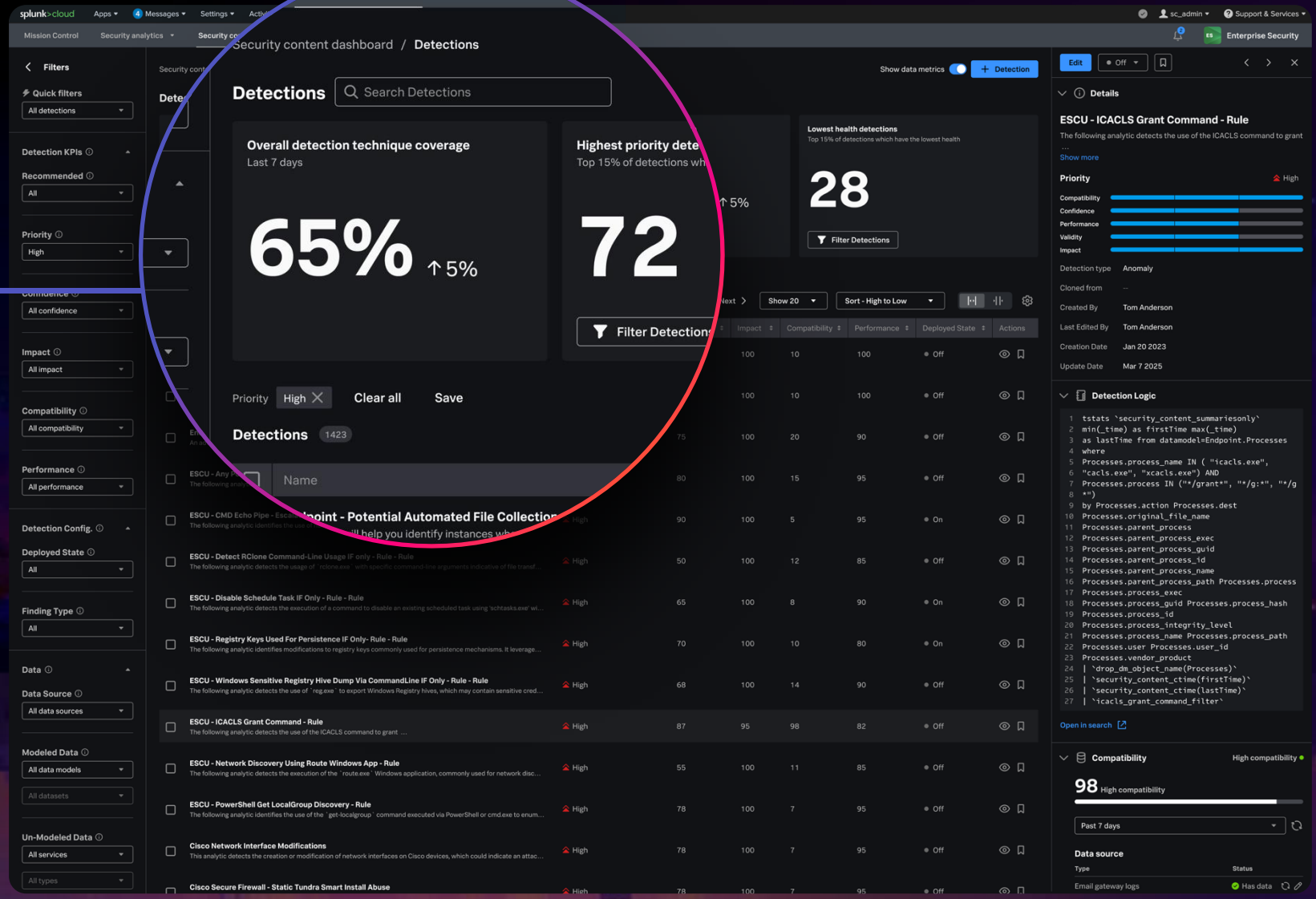
https://github.com/splunk/attack_range

Alpha Now

Detection Studio

Powered by SnapAttack

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



05 Powering the Future SOC

What defines a Future-Ready SOC?

Agentic and automated

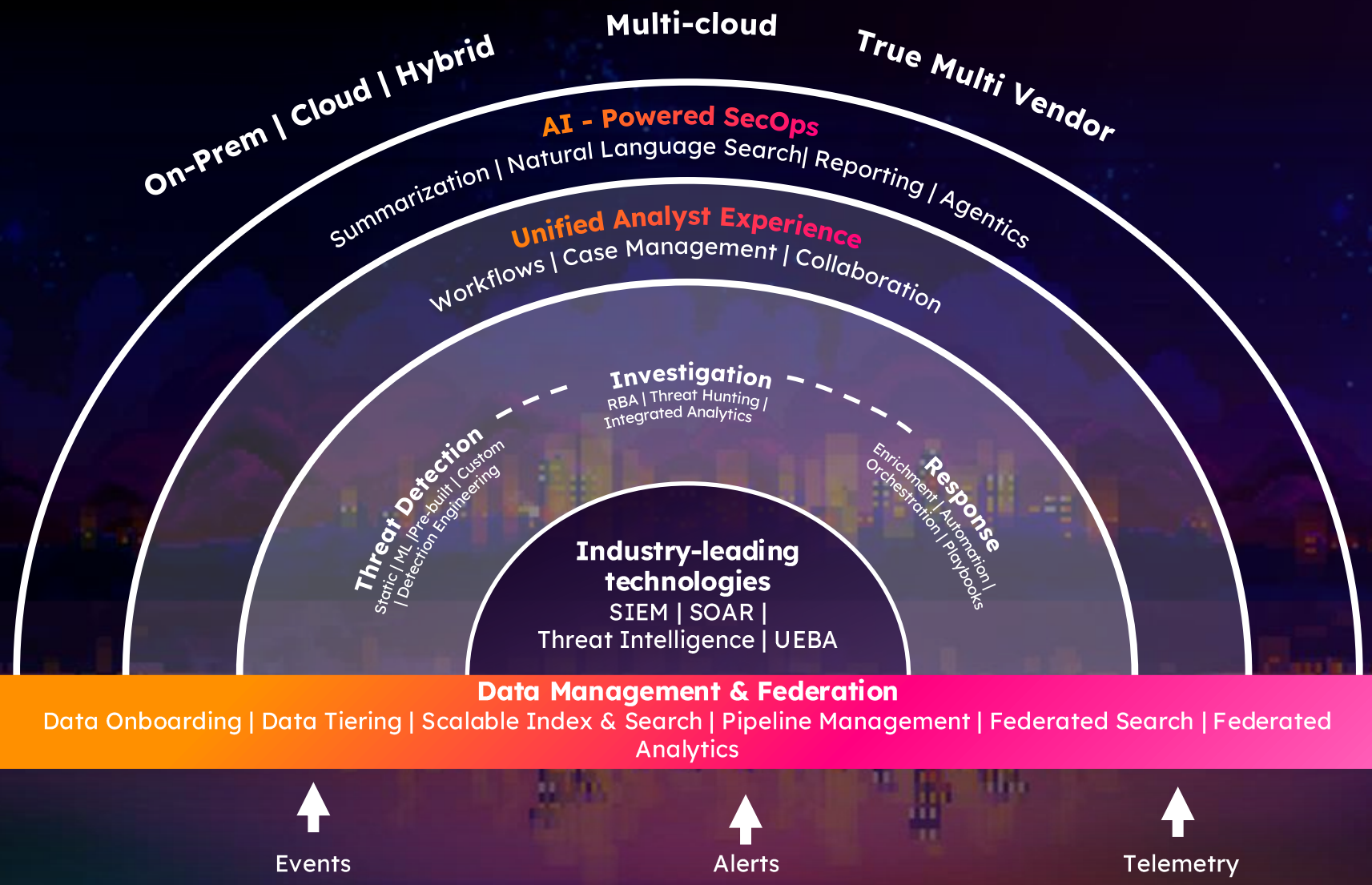
Unified and integrated

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

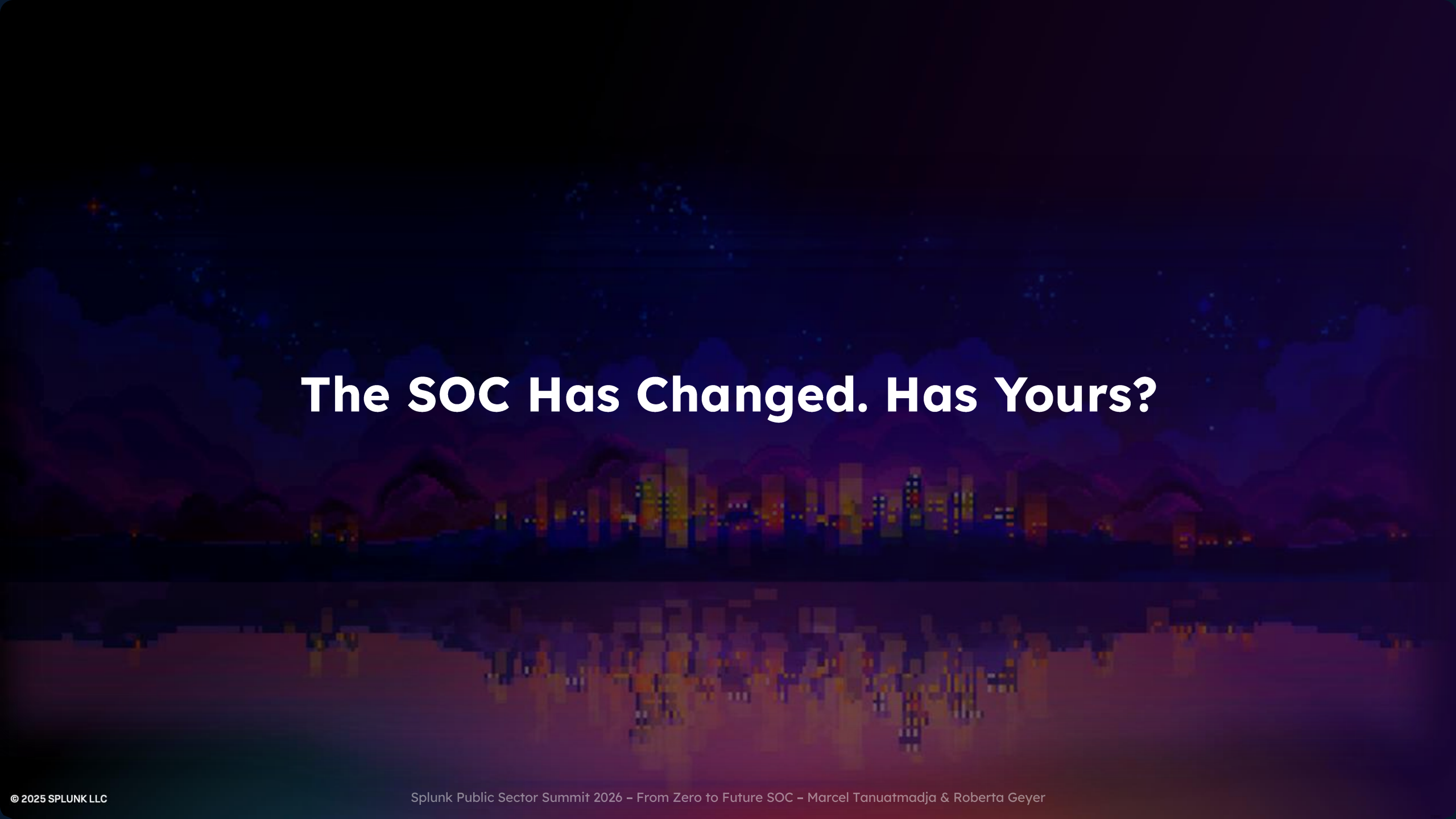
- Cut through alert fatigue with Risk-based alerting
- MITRE-mapped detections from Splunk Threat Research Team
- Native Findings grouping

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



Thank You!

Contact Us

Marcel Tanuatmadja mtanuatm@cisco.com
Roberta Geyer robertag@cisco.com