Manuals+ — User Manuals Simplified.

SOC Modernization and the Role of XDR

CISCO User Group Soc Of The Future User Guide

Home » Cisco » CISCO User Group Soc Of The Future User Guide

Cisco User Group
Soc of the Future
Nathan Smith
Head of Security APAC

Contents

User Group Soc Of The Future

Nathan Smith Head of Security, APAC

Industry Trends

Major Breaches	Regulatory Compliance	Cyber Crime as a service grows
As data breaches scale up, organizations and governments will be forced to spend more money to recover from them	Critical infrastructure regulations , industry specific regulations demand detection & response capabilities.	Cyber Crime is big Business and the entry level is continually being lowered via as a service models.

Expanding Attack Surface
Persistent Security Operations Challenges
Siloed Tools, Teams, Data & Workflows
Growing Attack Volumes
Compliance Mandates and Requirements
Talent and Skills Shortage

Source: ESG SOC Trends Report 2023

Key technology shifts in the SOC

Past

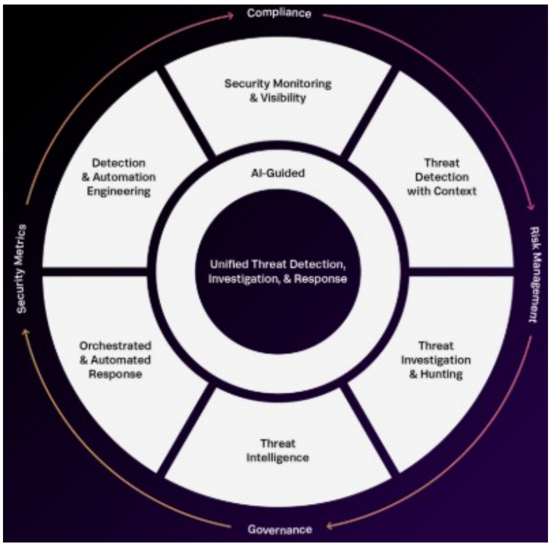
- Limited visibility across disconnected data sources and relying on ingest only approach hampers ability to identify high-risk threats amidst the digital noise.
- Reactive threat detection based on signatures or predefined rules with limited threat intelligence enrichment leading longer attacker dwell times.
- Reliance on manual efforts with limited automation for select routine tasks keeping your security team stuck in a reactive mode moving from tool to too.
- Lack of AI to help guide SOC workflows providing no relief for an already overworked and overwhelmed security team.
- Disjointed threat detection, investigation, and response limiting MTTD and MTTR.

Future

- Comprehensive visibility across all data, no matter where located with context for full attack-surface coverage with no “weak” signals missed.
- Proactive threat detection using AI/ML, risk based approach, and comprehensive threat intelligence stopping advanced attacks and slashing dwell times.
- Pervasive automation across threat analysis, containment, response and recovery actions increasing security team’s productivity and efficiency.
- AI guided SOC workflows to help increase efficiency and effectiveness of the security team
- Unified threat detection, investigation, and response dramatically improving MTTD and MTTR.

The SOC of the Future

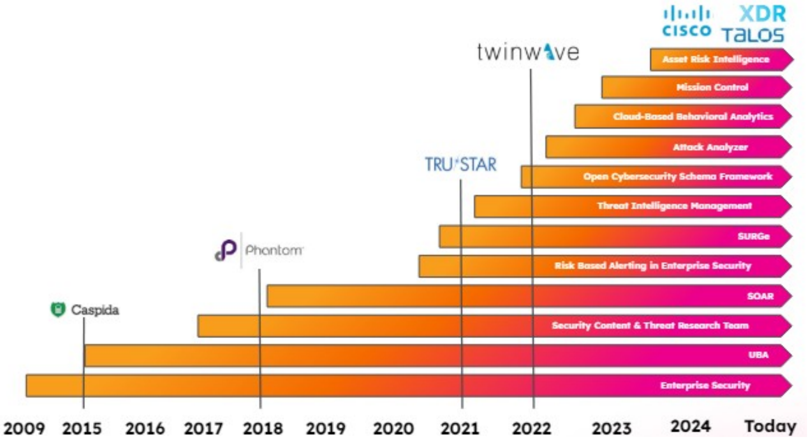
Unified Threat Detection, Investigation and Response at the Core.


Compliance
Risk Management
Governance
Security Metrics
Security Monitoring & Visibility
Threat Detection with Context
Threat Investigation & Hunting
Threat Intelligence
Orchestrated & Automated Response
Detection & Automation Engineering
AI-Guided
Unified Threat Detection, Investigation, & Response

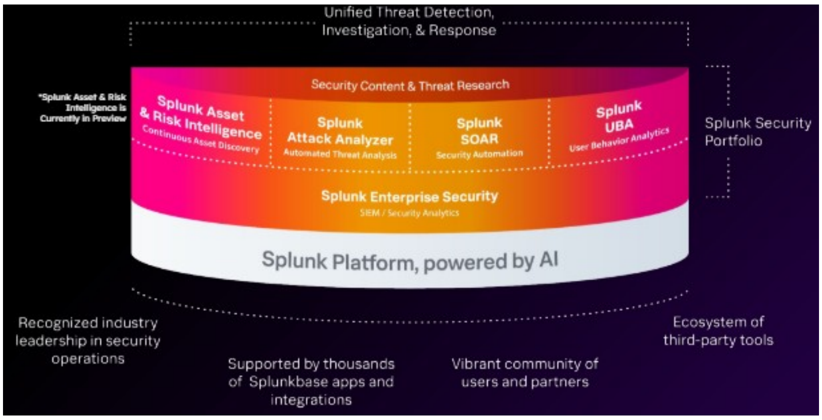
Delivering the essential capabilities

SOC of the Future	Splunk Security Delivers
Comprehensive Visibility	● Ingest and normalize any data at scale ● Federated search and analytics to access data from anywhere ● Open Cybersecurity Schema Framework open standard
Proactive Threat Detection	● 1,500+ curated detections crafted by Splunk Threat Research ● Behavioral Analytics to detect unknown threats and anomalies ● MLTK to build custom ML solutions for any use case ● Risk based alerting to tackle alert fatigue ● Integrated Threat Intelligence Enrichment
Pervasive Automation	● Automated Threat Analysis for decisive action and rapid response ● Powerful SOAR to increase speed of investigation and response ● Automate efficiently using pre-built playbooks and integrations
AI guided SOC workflows	● Splunk AI Assistant to search for data using natural language ● Embed Splunk AI Assistant for security into workflows
Unified TDIR	● Single, modern worksurface to unify TDIR ● Codify processes into response templates to simplify workflows ● Easy case management within your response templates

Building on SIEM to drive continued innovation to evolve the SOC



Powering the SOC of the future with the feading TDIR solution


Unified Threat Detection, Investigation, & Response
Security Content & Threat Research
*Splunk Asset & Risk Intelligence is Currently in Preview
Splunk Asset & Risk Intelligence
Continuous Asset Discovery
Splunk Attack Analyzer
Automated Threat Analysis
Splunk SOAR
Security Automation
Splunk UBA
User Behavior Analytics
Splunk Security Portfolio
Splunk Enterprise Security
SIEM / Security Analytics
Splunk Platform, powered by AI
Recognized industry leadership in security operations
Supported by thousands of Splunkbase apps and integrations
Vibrant community of users and partners
Ecosystem of third-party tools

Foundational use cases

Providing the critical capabilities on your resilience journey

Foundational Visibility See across environments Data Optimization Security Monitoring Incident Management Asset Discovery & Management Compliance Visualization & Reporting	Guided Insights Detect threats and issues with context Threat Intelligence Enrichment Leverage Cybersecurity Frameworks Risk Based Alerting AI Assisted Guidance Anomaly Detection Threat Hunting	Proactive Response Get ahead of issues Automate Threat Analysis Automate Containment & Response Actions Orchestrate Response Workflows	U C A e S R A F

Accelerated by Splunk AI

What about AI?

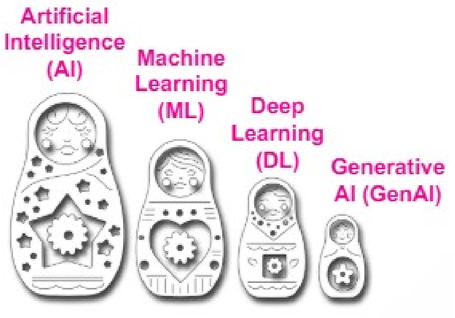
What is AI and Machine Learning?

Artificial Intelligence (AI) – capability of a computer system to mimic human cognitive functions such as learning and problem-solving

Machine Learning (ML) – subset of AI that uses mathematical models of data to help a computer learn without direct instruction

Deep Learning – subset of AI that uses computationally intense ML models inspired by the “deep” layers of the biological neural network of the human brain to accomplish complex goals like image recognition Example: Self driving car recognizes stop sign Generative AI – subset of AI that involves the use of algorithms and techniques to generate new data, things that have not existed in the world before being created by the models

Example: OpenAI Chat GPT



Recent AI Breakthroughs and Trends

1. Traditional Cognitive Tasks

   Human parity in

   - image classification (2015, Microsoft)
   - speech recognition (2017, Microsoft)
   - text summarization (2019, Google)
   - translation (2022, OpenAI)
   - reading comprehension (2023, OpenAI)
2. New and Emerging Capabilities

   Generative AI Capabilities

   - Chat
   - Q&A
   - Summarization
   - Suggestion
   - Code generation
   - Image generation
   - ……
3. Domain Specific Innovations

   New product categories

   - ChatBot
   - Security Copilot’s
   - Google Duet AI
   - AI Assistant
   - ……

What’s the benefit to the SOC?

Guidance

Provide guidance to analyst on next steps, lowing the entry level of knowledge needed to investigate and respond.

Faster Response

Reducing the time need to investigate and increasing the response time in taking actions.

Proactive

AI will help SOC teams prioritise activities and to move from reactive to proactive activities.

New

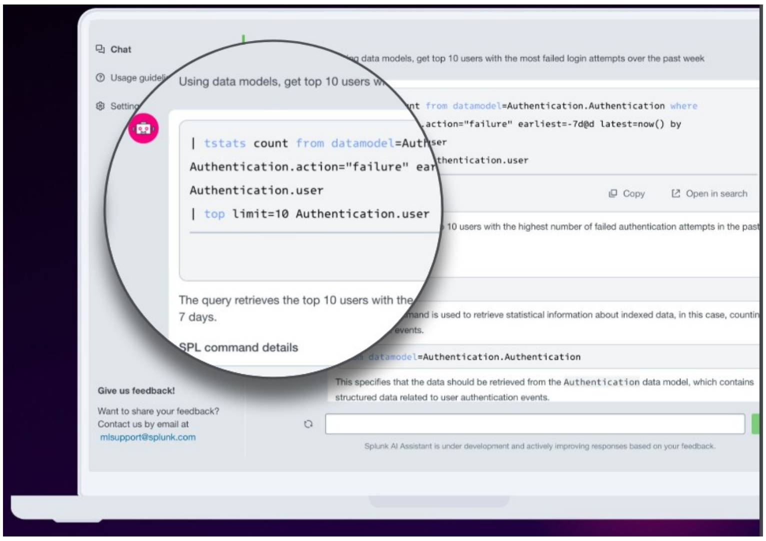
AI Assistant for SPL

Preview in Q1 & GA at .conf

▶ Upskill new and advanced Splunk users quickly.

▶ Translate bi-directionally between NL and SPL.

▶ Receive personalized recommendations.



Chat

Usage guideli

Setting

Using data models, get top 10 users with the most failed login attempts over the past week

```
| tstats count from datamodel=Authentication.Authentication where
Authentication.action="failure" earliest=-7d@d latest=now() by
Authentication.user
| top limit=10 Authentication.user
```

Copy Open in search

The query retrieves the top 10 users with the highest number of failed authentication attempts in the past 7 days.

SPL command details

…mand is used to retrieve statistical information about indexed data, in this case, countin… events.

```
datamodel=Authentication.Authentication
```

This specifies that the data should be retrieved from the `Authentication` data model, which contains structured data related to user authentication events.

Give us feedback!

Want to share your feedback? Contact us by email at mlsupport@splunk.com

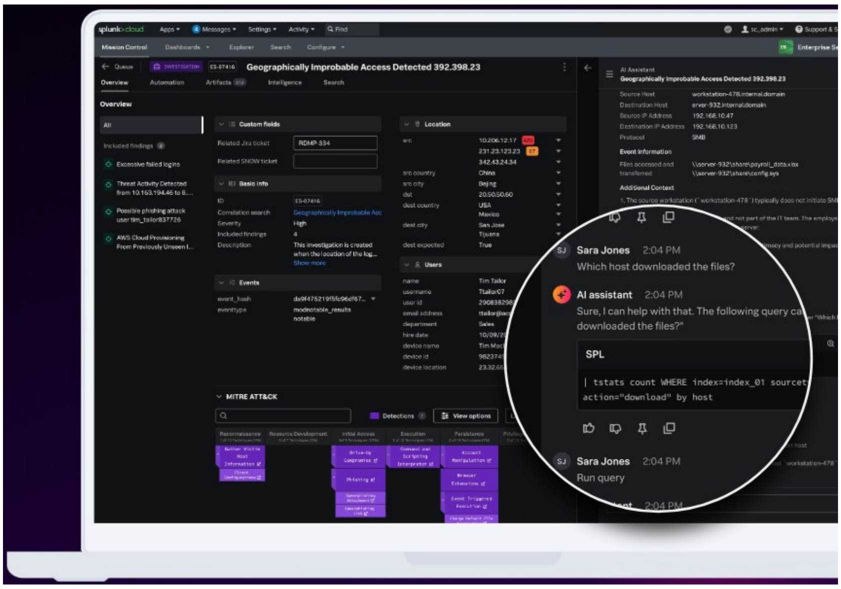
Splunk AI Assistant is under development and actively improving responses based on your feedback.

New

AI Assistant for Security

Investigate faster.

- ▶ Answer analyst questions to speed up daily workflows.
- ▶ Save time while addressing threats more rapidly.
- ▶ Access natively within Splunk ES.



Geographically Improbable Access Detected 392.398.23

AI Assistant

Geographically Improbable Access Detected 392.398.23

Source Host	workstation-478.internal.domain
Destination Host	erver-932.internal.domain
Source IP Address	192.168.10.47
Destination IP Address	192.168.10.123
Protocol	SMB

Event Information

Files accessed and transferred	\\server-932\share\payroll_data.xlsx \\server-932\share\config.sys

Additional Context

Sara Jones 2:04 PM
Which host downloaded the files?

AI assistant 2:04 PM
Sure, I can help with that. The following query ca… downloaded the files?"

SPL

```
| tstats count WHERE index=index_01 sourcet…
action="download" by host
```

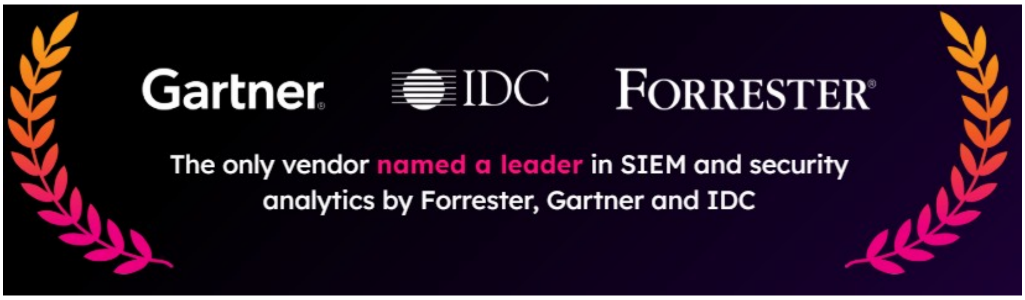
Sara Jones 2:04 PM
Run query

Splunk AI Assistant for Security

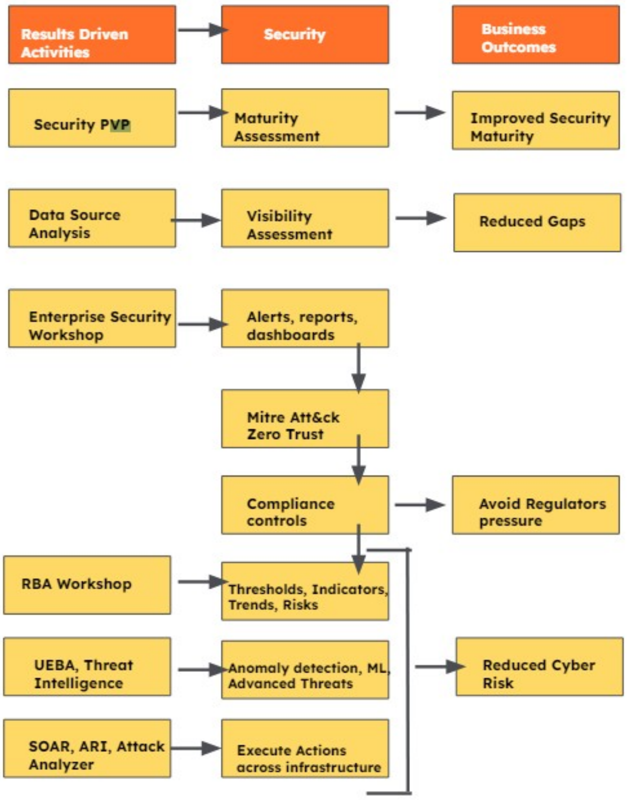
Accelerate the SOC with GenAI

Incident Summarization	Assisted Troubleshooting	Recommended Response	Detection Er

A recognizes leader in cybersecurity


Gartner
IDC
FORRESTER
The only vendor named a leader in SIEM and security analytics by Forrester, Gartner and IDC

TrustRadius	PeerSpot	kuppin
5 awards for SIEM and SOAR	Leader Award SIEM and SOAR	A leader in SOA


Results Driven Activities
Security
Business Outcomes
Security PVP
Maturity Assessment
Improved Security Maturity
Data Source Analysis
Visibility Assessment
Reduced Gaps
Enterprise Security Workshop
Alerts, reports, dashboards
Mitre Att&ck Zero Trust
Compliance controls
Avoid Regulators pressure
RBA Workshop
Thresholds, Indicators, Trends, Risks
UEBA, Threat Intelligence
Anomaly detection, ML, Advanced Threats
Reduced Cyber Risk
SOAR, ARI, Attack Analyzer
Execute Actions across infrastructure

How to get started

Thank you

Documents / Resources

 Cisco User Group Soc of the Future Nathan Smith Head of Security APAC splunk>	CISCO User Group Soc Of The Future [pdf] User Guide User Group Soc Of The Future, User Group Soc Of The Future, Soc Of The Future, The Future, Future

References

- User Manual