

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Power the SOC of the Future with Splunk and Cisco

An Introduction to Splunk for Security

Simon O'Brien
Director, Global Security Strategists, Splunk
BRKSEC-1583

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1583>



So, what is a Splunk?

Build-anything platform



Splunk Enterprise
Splunk Enterprise Security
Splunk SOAR

Prescriptive offerings



Splunk Attack Analyzer
User Behavior Analytics
Splunk Security Essentials
Risk Based Analytics
SOAR Playbook Packs

Re-usable data



Enterprise Logging
IT Operations

Splunk Enterprise

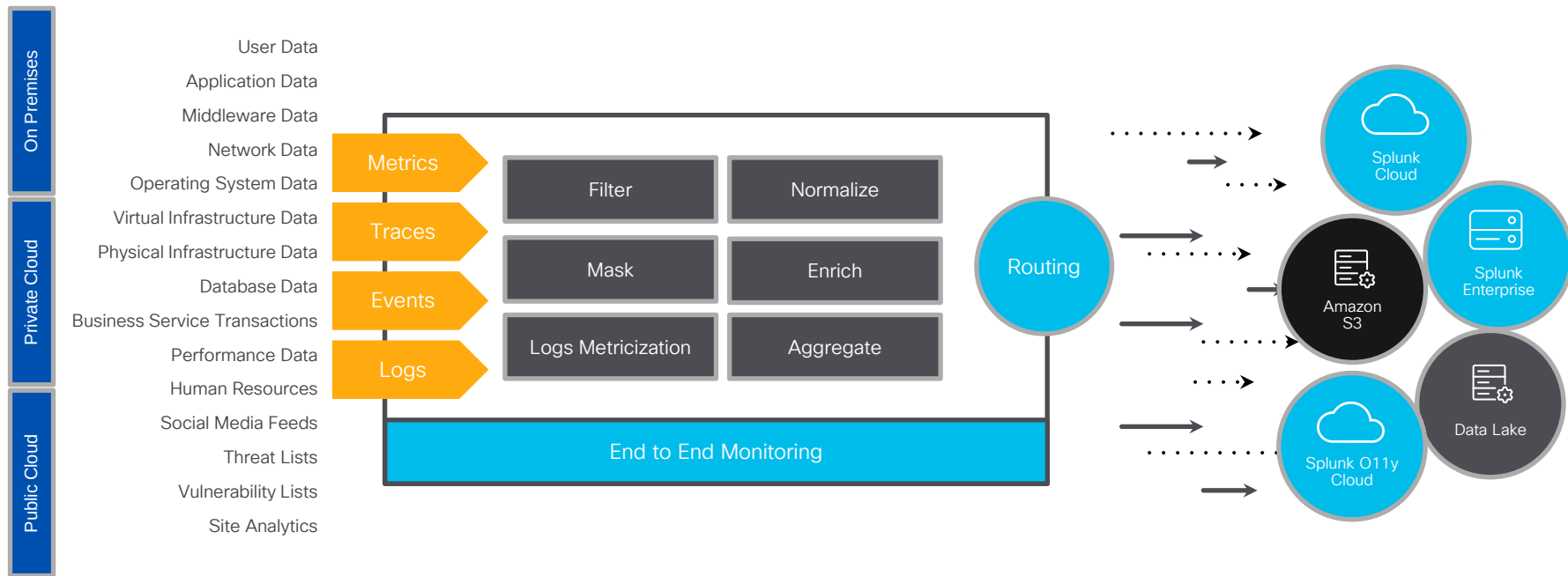
Powerful machine data aggregation, search, reporting and alerting

- Expansive data access
- Flexible data onboarding
- Full-fidelity investigation
- Real-time alerting
- Build custom apps
- SaaS or self-managed



Data configuration, processing and management

Common set of events, traces, metrics and logs for comprehensive visibility



Demo



Discover Apps

PLATFORM

☐ SPLUNK

> PRODUCT

> VERSION

☐ SPLUNK SOAR

> PRODUCT

> VERSION

CATEGORY

☐ Business Analytics

☐ DevOps

☐ Directory Service

☐ Email

☐ Endpoint

☐ Firewall

☐ Generic

☐ Identity Management

☐ Information

☐ Investigative

☐ IoT & Industrial Data

Showing 1-18 of 63 Results for **Cisco**

Sort by

Sort By Best Match



Cisco Networks Add-on for Splunk Enterprise
By Mikael Bjerkeland

The Cisco Networks Add-on for Splunk Enterprise (TA-cisco_ios) sets the correct sourcetype and fields used for...

PLATFORM Splunk Enterprise, Splunk Cloud

RATING ★★★★★ (21)

NOT SUPPORTED



Cisco Networks App for Splunk Enterprise
By Mikael Bjerkeland

The Cisco Networks App for Splunk Enterprise includes dashboards, data models and logic for analyzing data from...

PLATFORM Splunk Enterprise, Splunk Cloud

RATING ★★★★★ (41)

NOT SUPPORTED



Cisco Endpoint Security Analytics (CESA)
By Cisco Systems

Use and Cisco TAC support of this App and related Add-On require a purchase of Cisco Endpoint Security Analytics (CESA)...

PLATFORM Splunk Enterprise

RATING ★★★★★ (10)

DEVELOPER SUPPORTED APP



TA for Cisco CDR Reporting and Analytics
By Sideview LLC

This TA provides index-time settings to index and timestamp CDR and CMR data from Cisco CallManager and Cisco CUB...

PLATFORM Splunk Enterprise, Splunk Cloud

RATING ☆☆☆☆☆ (0)

DEVELOPER SUPPORTED ADDON



Cisco Bug Search and Analytics
By Pavel Prostin

Cisco Bug Search and Analytics offers unrestricted filtering, summarization, and correlation capabilities for vulnerability...

PLATFORM Splunk Enterprise, Splunk Cloud

RATING ★★★★★ (1)

DEVELOPER SUPPORTED APP



CCX Add-on for Cisco Secure Endpoint (AMP)
By Henrique Linsmeyer

About Us: CyberCX is Australia's greatest force of cyber security experts. Our highly skilled professional services tea...

PLATFORM Splunk Enterprise, Splunk Cloud

RATING ☆☆☆☆☆ (0)

DEVELOPER SUPPORTED ADDON



CCX Add-on for Cisco Secure Network Analytics...
By Matthew Orme

About Us: CyberCX is Australia's greatest force of cyber security experts. Our highly skilled professional services tea...



Splunk Add-on for Cisco Meraki
By Splunk Inc.

The Splunk Add-on for Cisco Meraki lets you monitor network and security events in your environment. The the Splunk Ad...



Cisco Web Security Appliance (WSA) Insight
By Pavel Prostin

Visualize hidden Cisco Web Security Appliance (WSA) statistics, simplify troubleshooting, find performance...

Some notable apps & add-ons

Built for Splunk platform users

- [Splunk Security Essentials \(SSE\)](#) allows you to browse, bookmark and deploy ESCU analytic stories from the [Security Content Library](#) with just a few clicks to enhance searches in your Splunk environment. Also provides automatic mapping of data and security detections to the MITRE ATT&CK® and Cyber Kill Chain® frameworks.
- [Compliance Essentials for Splunk](#) streamlines continuous monitoring efforts, improves cybersecurity posture, and addresses the requirements of different National Institute of Standards and Technology (NIST)-based control frameworks, including the following: Risk Management Framework (RMF), Cybersecurity Maturity Model Certification (CMMC), Defense Federal Acquisition Regulation Supplement (DFARS) and the Office of Management (OMB) M-21-31 MEMORANDUM.
- [InfoSec App for Splunk](#) relies on accelerated data models and the Common Information Model (CIM) to provide a consistent and normalized view into the event data that you'll bring into Splunk. This app can help you address basic security use cases, including monitoring and security investigations.
- [The Splunk AI Assistant](#)* makes SPL more accessible, enabling users to create SPL queries from plain English, and view plain English explanations of any well-formed SPL searches. **The Splunk AI Assistant is available as a preview and is not officially supported.*
- [Splunk Mobile App](#) allows users to access your Splunk data anywhere at any time. Get notified with actionable alerts and make decisions faster with dashboards and reports at your fingertips.
- [Splunk Machine Learning Toolkit](#) helps you apply a variety of machine-learning techniques and methods, such as classification (predicting a yay or nay), regression, anomaly detection, and outlier detection against your data. In v5.4 or higher you can upload pre-trained [ONNX](#) models for inferencing in MLTK.

Our product vision

To provide visibility and insights across an enterprise's **entire digital footprint**, powering actions that improve security, reliability, and innovation velocity



Access the
right data



Apply the
right analytics



Accelerate the
right actions

Cisco technology add-ons / apps / SOAR connectors

Built by Splunk and Cisco

Technology Add-ons

- Cisco ACI Add-on for Splunk Enterprise
- Cisco Catalyst SD-WAN Add-on for Splunk
- Cisco Secure eStreamer Client Add-On for Splunk
- Cisco SecureX threat response - Custom Search Command
- Splunk Add-on for AppDynamics
- Splunk Add-on for Cisco ASA
- Splunk Add-on for Cisco ESA
- Splunk Add-on for Cisco Identity Services
- Splunk Add-on for Cisco Meraki
- Splunk Add-on for Cisco UCS
- Splunk Add-on for Cisco WSA

SOAR Connectors

- Cisco ESA
- Cisco Firepower
- Cisco ISE
- Cisco Secure Malware Analytics (ThreatGrid)
- Cisco Umbrella
- Cisco Umbrella Investigate
- Cisco Webex
- FireAMP

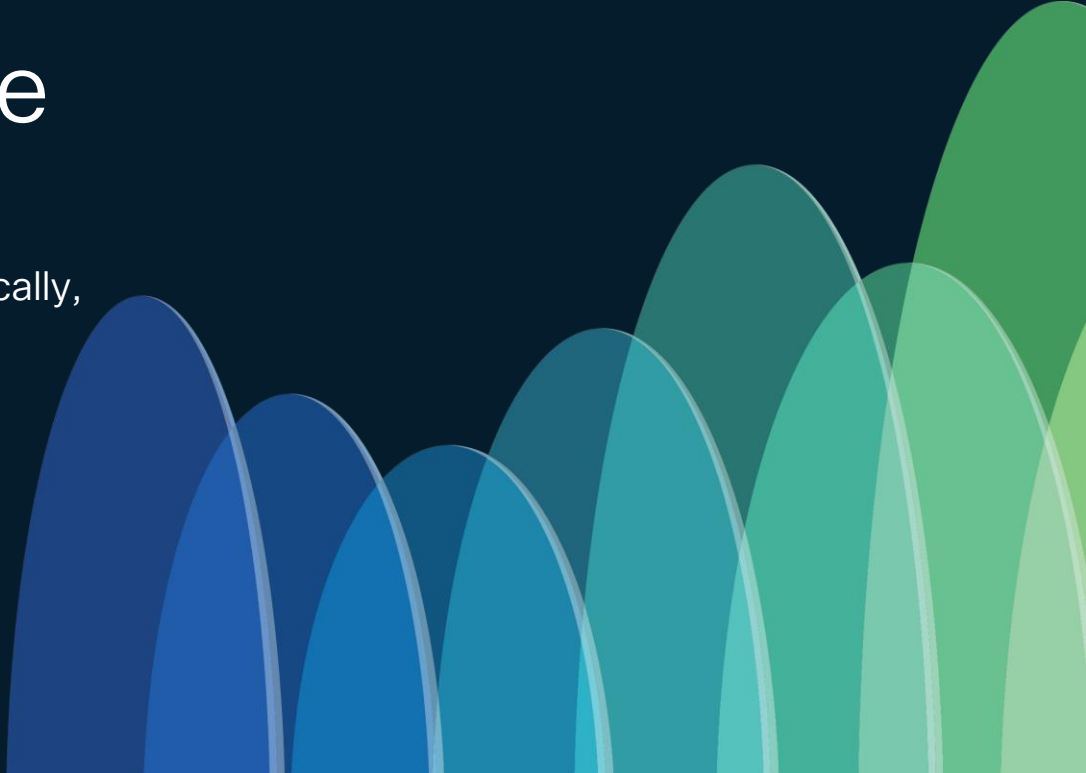
Apps

- Cisco ACI App for Splunk Enterprise
- Cisco Catalyst SD-WAN App for Splunk
- Cisco Secure Endpoint (formerly AMP for endpoints)
- Cisco Secure Firewall App for Splunk
- Cisco Secure Malware Analytics
- Cisco Secure Network Analytics (Stealthwatch) App for Splunk Enterprise)
- Cisco Security Cloud
- Duo Splunk Connector

... And more built by 3rd party communities & individuals

Splunk Enterprise Security

Detect what matters, investigate holistically,
and respond rapidly

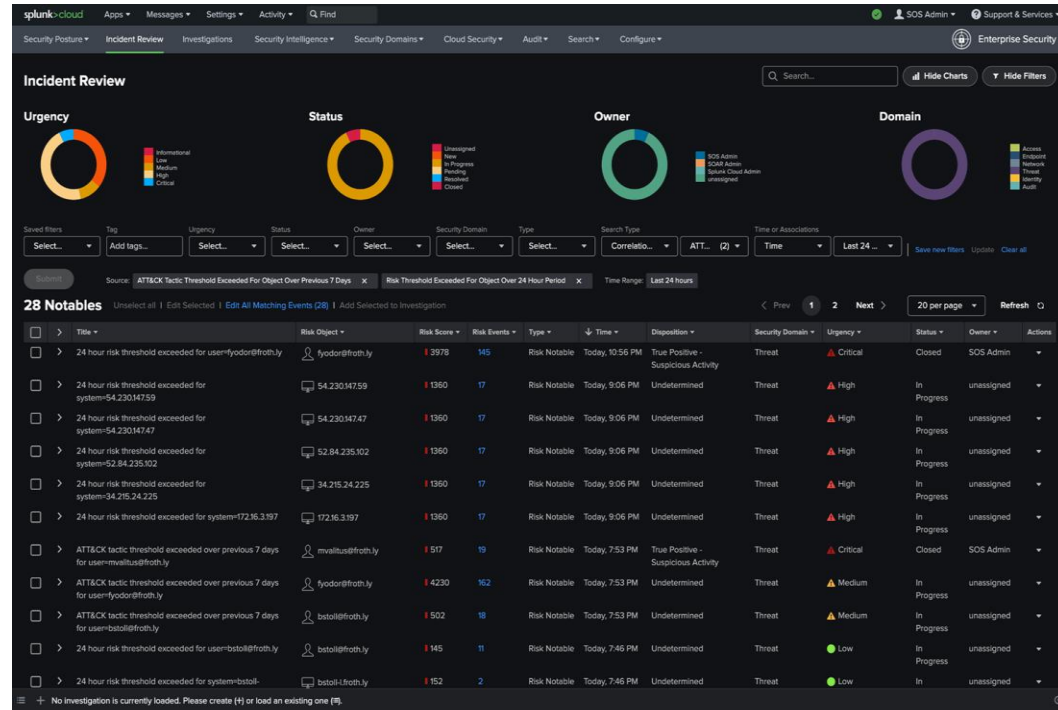


Splunk Enterprise Security is an industry-defining SIEM and security analytics solution **trusted by SOCs around the globe**. Its powerful capabilities enable you to **realise comprehensive visibility, empower accurate detection with context, and fuel operational efficiency**.

A full featured SIEM

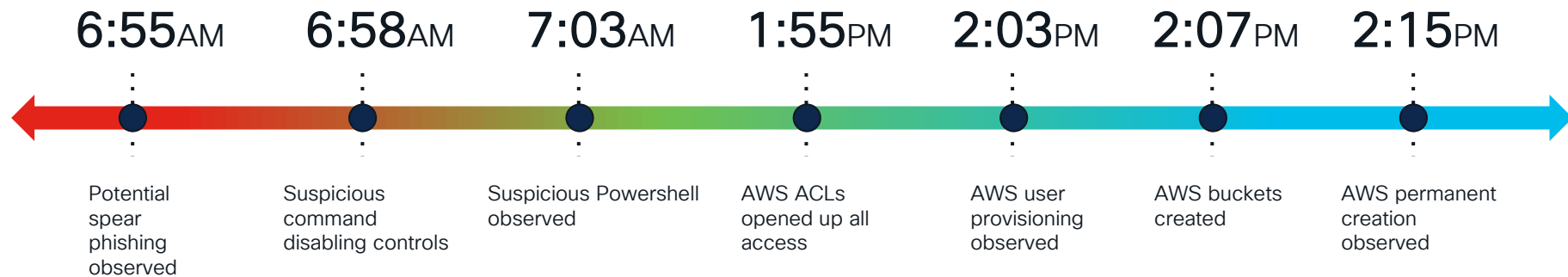
Purpose-built security capabilities built on top of Splunk

- Operational Workbench
- Robust Content Library
- Detections built on SPL
- Massive scale and enterprise capability



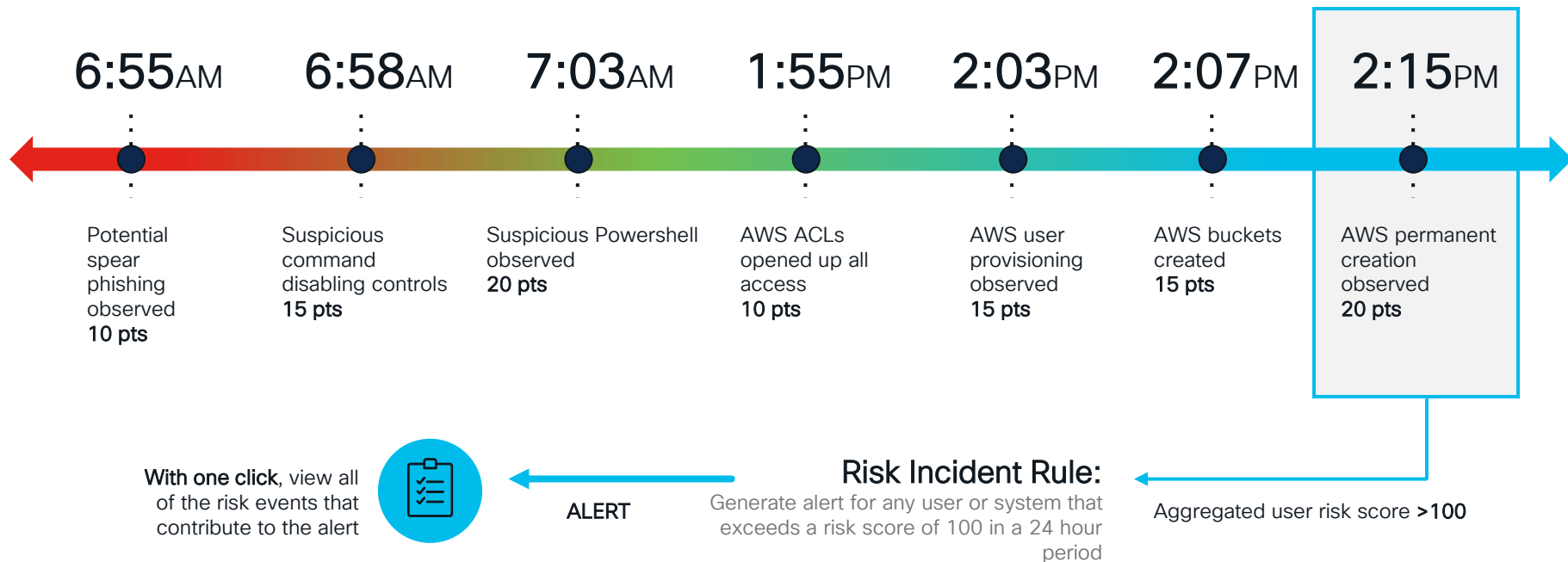
Traditional SIEM alerting

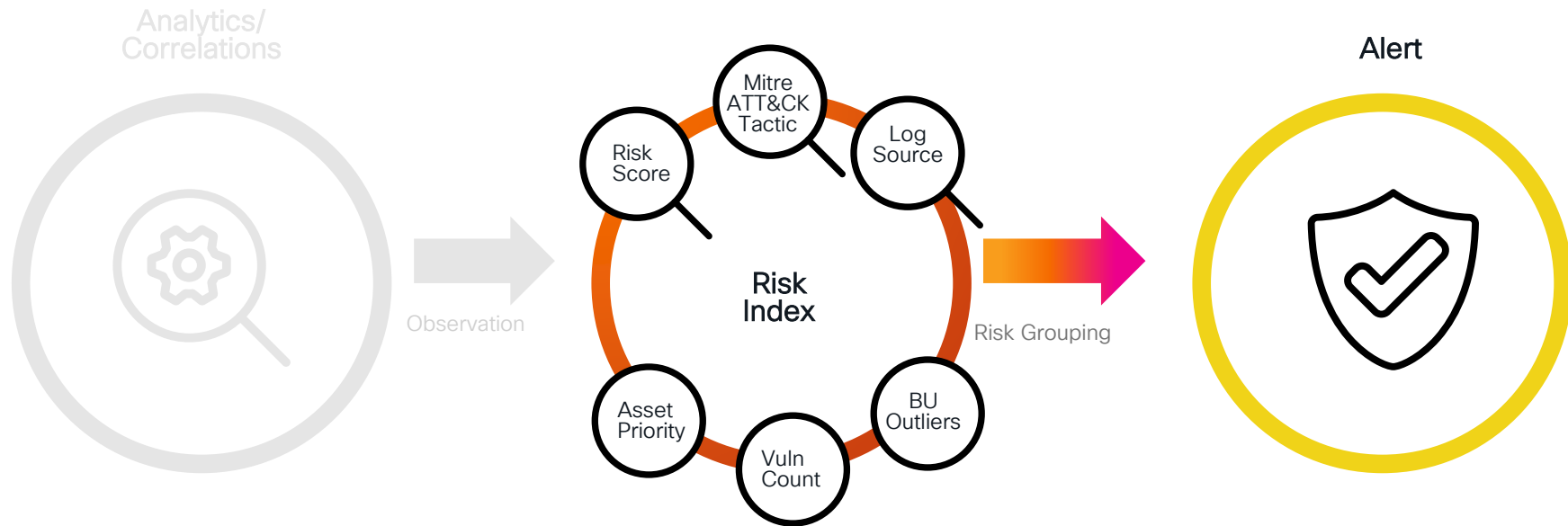
Traditionally, the events below might be considered too noisy and would be abandoned



Risk-based alerting

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





Analytics/
Correlations



Investigation



Alerting



Adv Sim



Threat Hunting



Case management made to support your team

Where automation and analysts meet

- Automation when and where you want it
- A collaborative case management system that works *with your team* rather than as a chore
- Let your junior analysts work like your experienced ones

The screenshot displays the Splunk Case Management interface. The main header shows navigation tabs: Mission Control, Analytics, Security content, Configure, and Search. Below this, a breadcrumb trail indicates the current case: Queue > ES-00001 > ATT&CK tactic threshold exceeded over previous 7 days for system=splunktshtcompany-1. The 'Response' tab is selected, showing a 'Findings Response' section with a progress bar at 33% completed. The 'Review IOCs' section is also visible, showing a description and a list of actions. The right sidebar provides detailed information about the case, including the owner (simon.geatarfunk), status (In Progress), urgency (Informational), sensitivity (Unassigned), disposition (Undetermined), ID (ES-00001), type (INVESTIGATION), time (Nov 6th, 2024 6:25 AM), last updated (Nov 6th, 2024 6:32 AM), reference ID (bde82e39-67bd-4972-aff6-716c0684f87), investigation type (default), and description (ATT&CK tactic threshold exceeded for an object over the previous 7 days). The bottom right shows a list of notes with timestamps and content.

Use case keywords



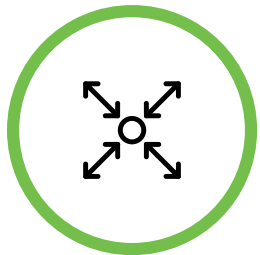
Security
Monitoring &
Analysis



Advanced &
Insider Threat
Detection



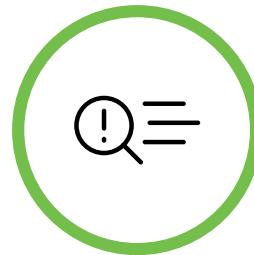
Incident
Investigation &
Forensics



Incident
Response



Compliance



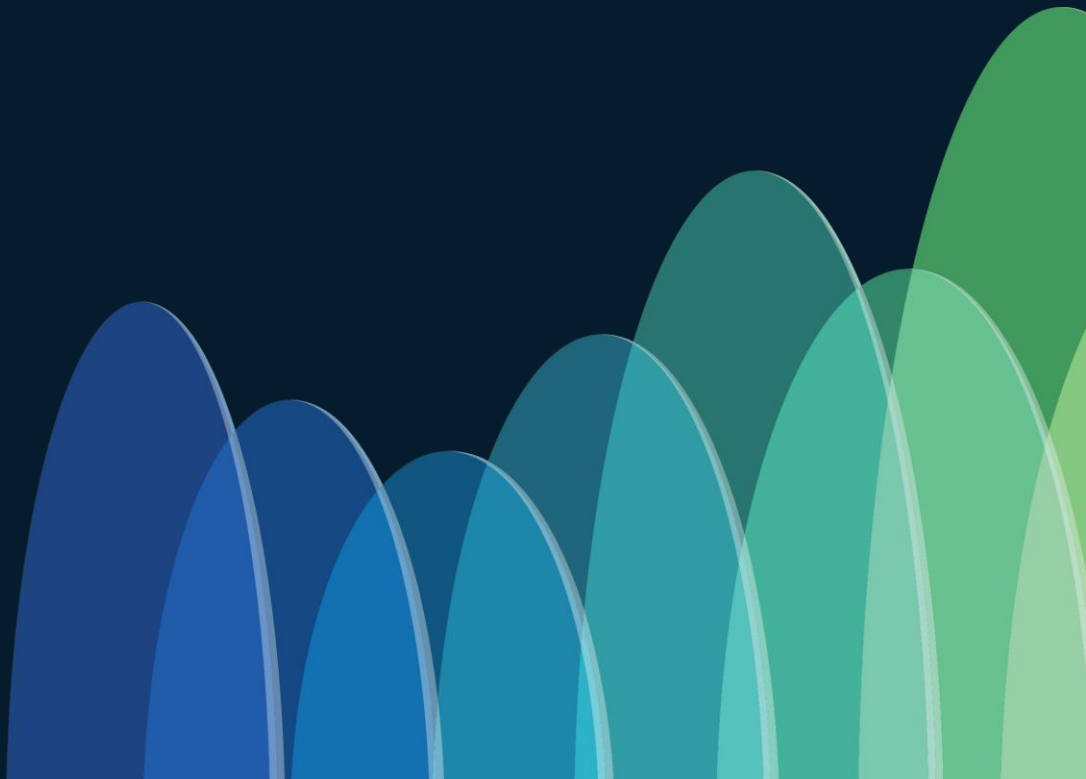
Threat
Hunting

Splunk SOAR

Work smarter

Respond faster

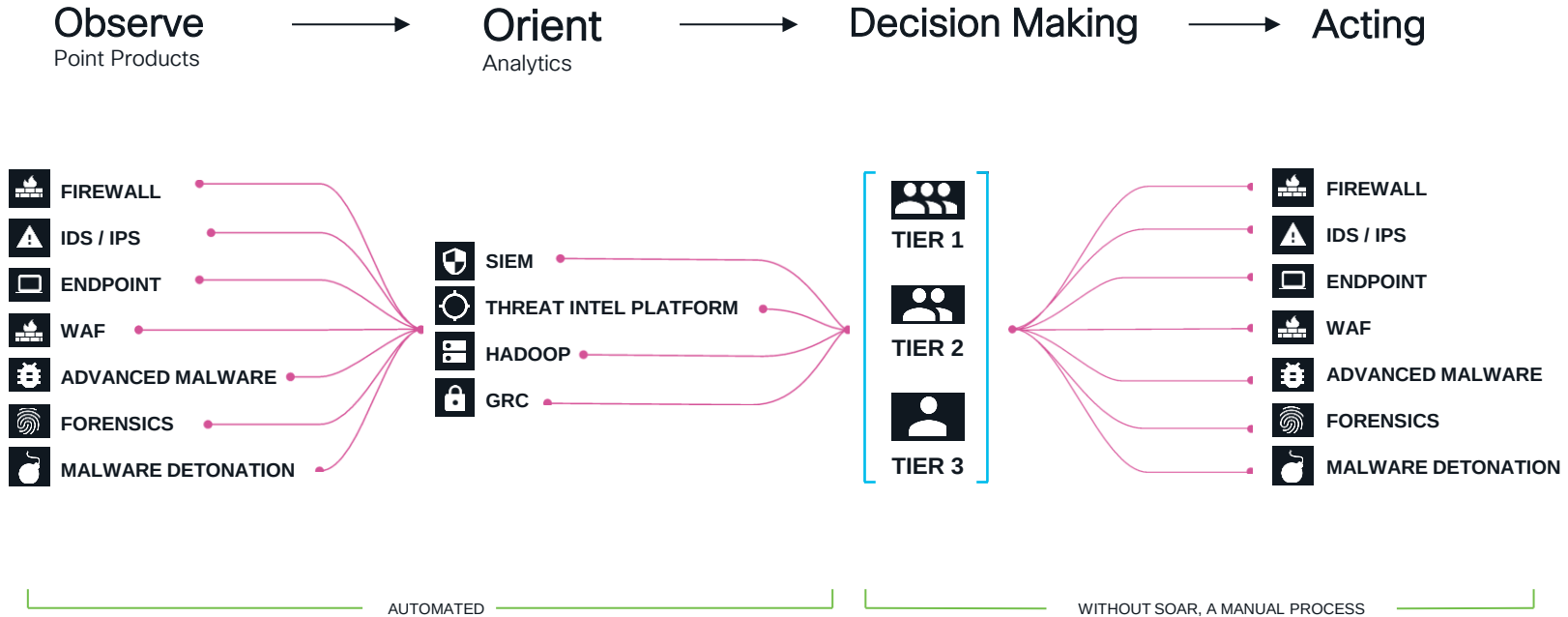
Empower your SecOps



Splunk SOAR provides security orchestration, automation and response capabilities that allow security analysts to **work smarter by automating repetitive tasks**; respond to security incidents faster with automated alert triage, investigation, and response; and **strengthen defenses by connecting and coordinating complex workflows** across their team and tools.

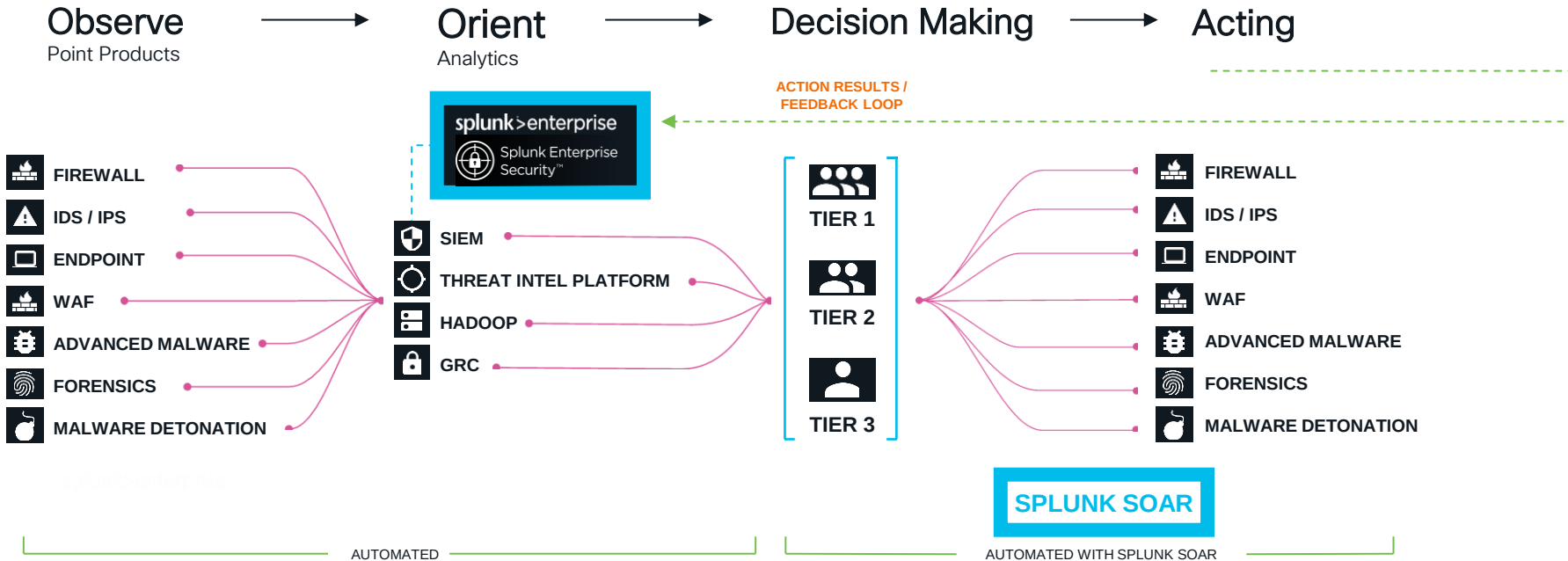
SOAR for security operations

Faster execution through the OODA loop yields better security



SOAR for security operations

Faster execution through the OODA loop yields better security



Discover Apps

PLATFORM

Clear

☐ SPLUNK

> PRODUCT

> VERSION

☒ SPLUNK SOAR

> PRODUCT

> VERSION

CATEGORY

☐ Business Analytics☐ DevOps☐ Directory Service☐ Email☐ Endpoint☐ Firewall☐ Generic☐ Identity Management☐ Information☐ Investigative☐ IoT & Industrial Data

Showing 1-7 of 7 Results for

Cisco X

Filtered by:

Splunk SOAR X

Sort by

Sort By Best Match

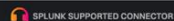
**Cisco ISE**

By Splunk Inc.

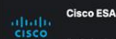
This app implements investigative and containment actions on a Cisco ISE device

PLATFORM SOAR On-Prem, SOAR Cloud

RATING ★★★★★ (2)



SPLUNK SUPPORTED CONNECTOR

**Cisco ESA**

By Splunk Inc.

This app supports investigation on the Cisco Email Security Appliance (ESA) device

PLATFORM SOAR On-Prem, SOAR Cloud

RATING ☆☆☆☆☆ (0)



SPLUNK SUPPORTED CONNECTOR

**Cisco Umbrella Investigate**

By Splunk Inc.

This app implements investigative actions by querying the Cisco Umbrella Investigate cloud service

PLATFORM SOAR On-Prem, SOAR Cloud

RATING ☆☆☆☆☆ (0)



SPLUNK SUPPORTED CONNECTOR

**Cisco Webex**

By Splunk Inc.

This app integrates with Cisco Webex to implement investigative and generic actions

PLATFORM SOAR On-Prem, SOAR Cloud

RATING ☆☆☆☆☆ (0)



SPLUNK SUPPORTED CONNECTOR

**Cisco Umbrella**

By Splunk Inc.

This app allows management of a domain list on the Cisco Umbrella Security platform

PLATFORM SOAR On-Prem, SOAR Cloud

RATING ☆☆☆☆☆ (0)



SPLUNK SUPPORTED CONNECTOR

**Cisco Firepower**

By Splunk Inc.

This app interfaces with Cisco Firepower devices to add or remove IPs or networks to a Firepower Network Group Object,...

PLATFORM SOAR On-Prem

RATING ☆☆☆☆☆ (0)



SPLUNK SUPPORTED CONNECTOR

**FireAMP**

By Splunk Inc.

[Collections](#)
[Apps](#)

[Submit an App](#)
[Log In](#)

Cisco ISE

This app implements investigative and containment actions on a Cisco ISE device

Built by [Splunk Inc.](#)

SOAR

Login to Download

Latest Version 3.0.2

December 22, 2023

[Release notes](#)

Compatibility

SOAR On-Prem, SOAR Cloud

Platform Version: 6.2, 6.1, 6.0, 5.5, 5.4, 5.3, 5.2, 5.1

Rating

5 ★★★★★ (2)

Log in to rate this app

Support

Splunk Supported Connector

[Learn more](#)

Ranking

#1 In Network Access Control

#4 In Network Security

[Summary](#)
[Details](#)
[Installation](#)
[Troubleshooting](#)
[Contact](#)
[Version History](#)

This app implements investigative and containment actions on a Cisco ISE device

Supported Actions

- test connectivity: Validate the asset configuration for connectivity. This action logs into the device using a REST API call to check the connection and credentials
- list endpoints: List the endpoints configured on the system
- get device info: Get information about a specific endpoint
- update device info: Update information or attributes for a specific endpoint
- list sessions: List the sessions currently available on the Monitoring node
- terminate session: Terminate sessions
- list resources: Lists all the resources configured on the system of a particular resource
- get resources: Get the information about resource if resource_id is provided. Fetch the list of resources match with the key-value filter
- delete resource: Delete a resource
- create resource: Create a resource
- update resource: Update a resource
- apply policy: Apply policy on selected Ip address or MAC address

Categories

Network Access Control, Network Security

Created By

Splunk Inc.

Source Code

[GitHub](#)

Type

connector

Downloads

22,239

Licensing

CISCO *Live!*

#CiscoLiveAPJC

BRKSEC-1583

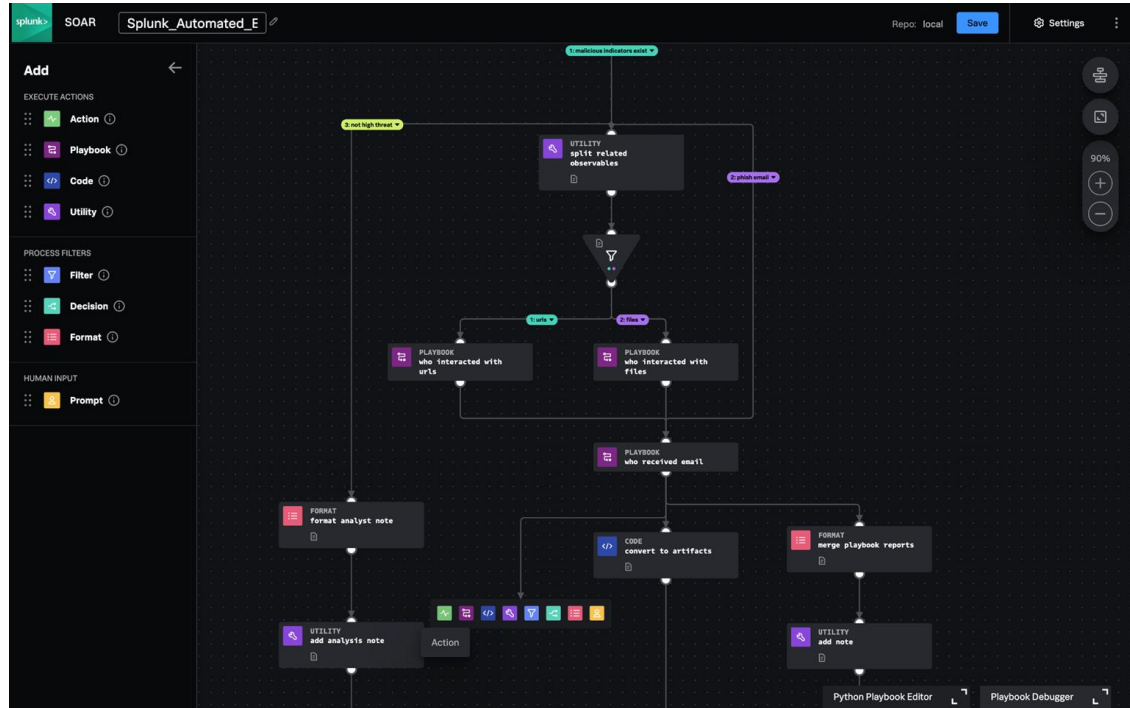
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

34

Build out automation playbooks

Leverage automation so your team can do more with less

- Build playbooks using our low code / no code **Visual Playbook Editor**
- Combines the **business logic** of your processes with the **automated use of the tools and services** your team relies on
- Run process **immediately, 24/7**, consistently, just like your most experience team members... all without spending your team's time



Use case keywords



Orchestration
and
automation



Case /
workflow
management



Enrichment



Alert volume,
capacity



Rapid
response

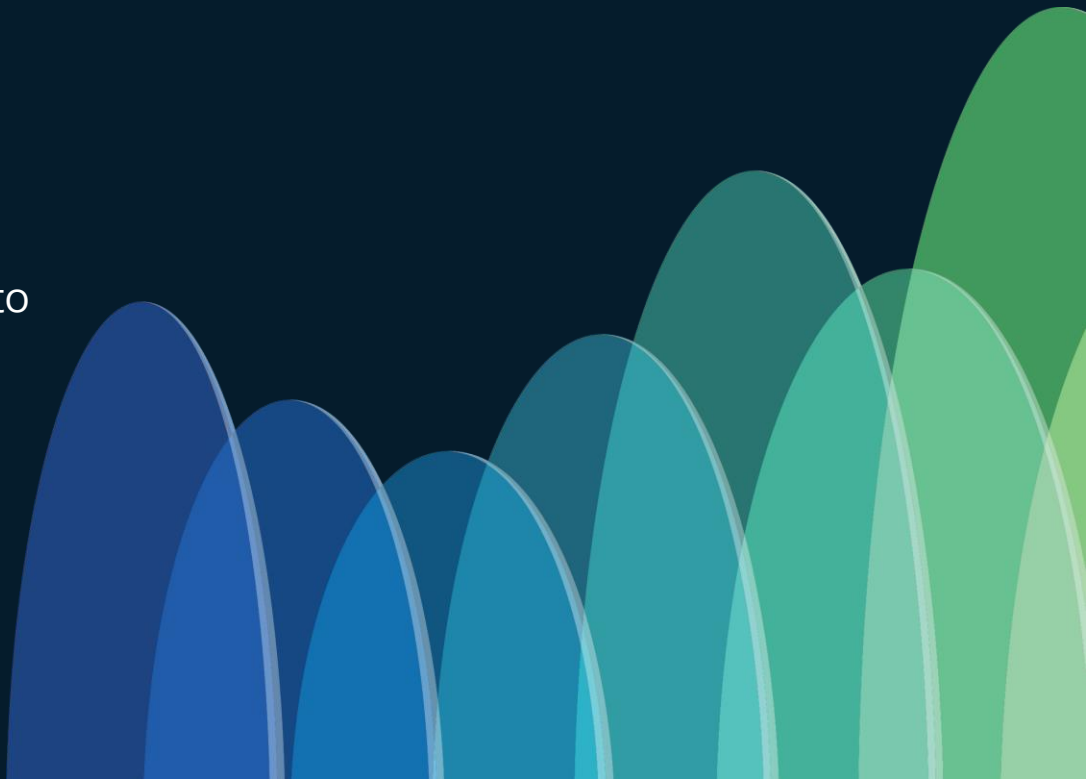


Skill gap /
hiring issues

Splunk Attack Analyzer

Automated Threat Analysis of Malware and
Credential Phishing Threats

Splunk Attack Analyzer **automates analysis of suspected malware and credential phishing threats.** Unlike other analysis tools that require manual workflows, the solution **automatically follows and analyses each step in complex attack chains** to identify and extract forensics and render a verdict to help analysts understand active threats and **accelerate investigations.**



Take the manual work out of threat analysis

Not just a sandbox

- Attack Chain Following means that Splunk Attack Analyzer is going to jump through the hoops for you, think **anti-anti-analysis**.
- Attacks are **not just binaries and exploits** so your analysis platform shouldn't be, either.

The screenshot displays the Splunk Attack Analyzer interface for a file named **MobileActivation.eml**. The interface is dark-themed and includes a top navigation bar with 'SAA', 'Attack Analyzer', 'Recent', and 'Search' options. The main content area is divided into several sections:

- Metadata:** Shows a Score of 100, Verdict of Phish, Malware Family of AgentTesla, and Phished Brands of Microsoft and Microsoft 0365. It also lists submission details like 'Submitted: 10/18/2023, 12:24:49 PM by API - soar' and file information like 'File Type: SMTP mail, ASCII text, with CRLF, LF line terminators' and 'File Size: 187 KB'.
- Resources Analyzed:** A tree view showing the file's internal structure, including attachments like **MobileLoginActivation.pdf** and various links and downloads.
- Summary:** A list of analysis tasks with their status. Tasks like 'Consolidated', 'Email Analyzer', 'Static File Analysis', 'ClamAV', 'YARA', and 'Windows 7 Sandbox' are all marked as 'OK'.
- Task Results:** A table showing details for the initial submission, including job duration (7 minutes), resources analyzed (3 URLs, 5 files), and verdict (Phish).
- Detections (47):** A list of specific findings, such as 'Detected Microsoft Phishing Attempt' and 'Uriscan.io: detected the following categories: phishing', each with a score of 100.

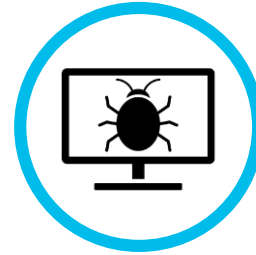
Use case keywords



Phishing



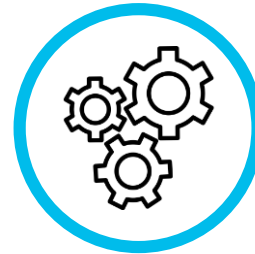
Enrichment



Sandboxing,
Malware



Brand
Reputation



Automation

Demo

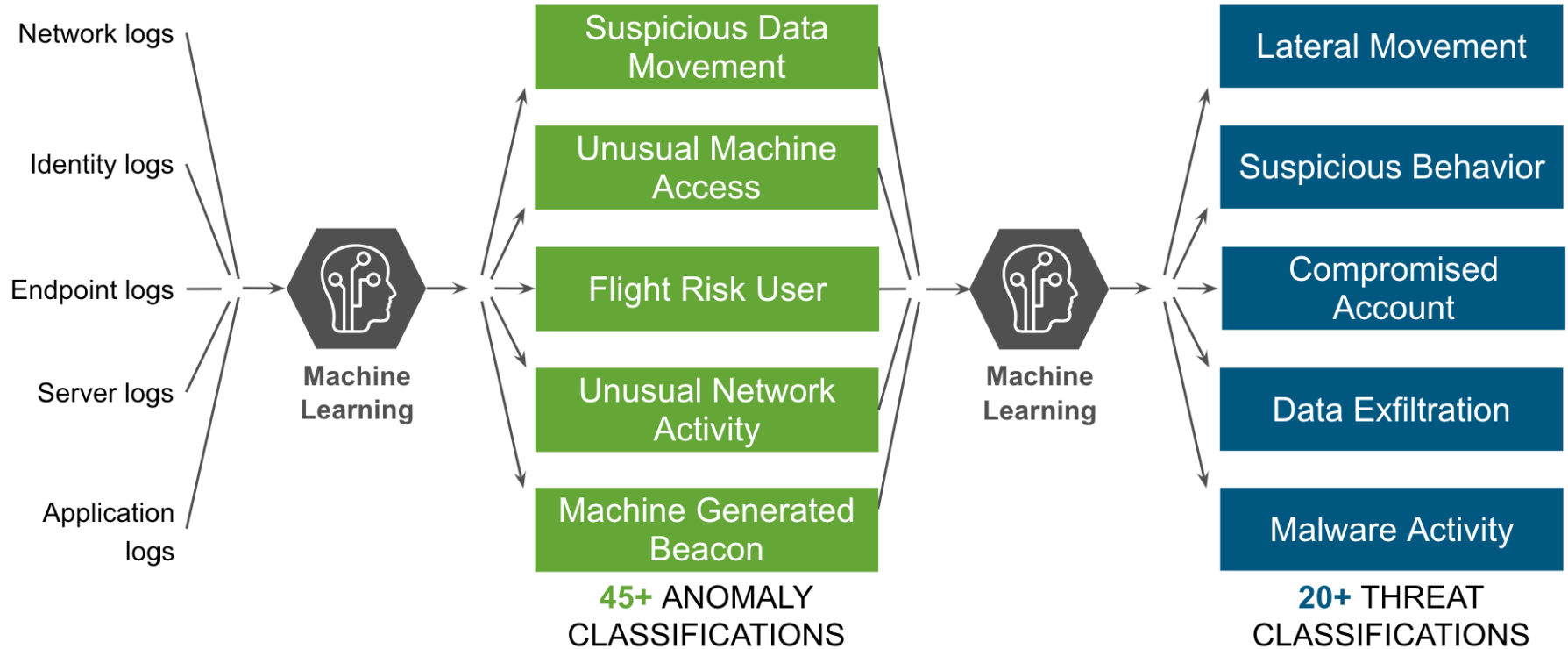


Splunk User Behavior Analytics (UBA)

Detect unknown threats and anomalous behaviour using machine learning

Splunk User Behavior Analytics (UBA) **detects advanced threats using machine learning, enhances security visibility and generates rich contextual insights** to help security teams assess risk and take rapid action, streamlines incident investigations, and increases SOC efficiency.

How Does Splunk UBA Work?



CISCO *Live!*



Use case keywords



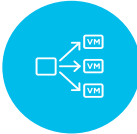
Account misuse



Compromised user account



Compromised and infected machine (malware)



Lateral movement



Data exfiltration



Suspicious behaviour and unknown threat

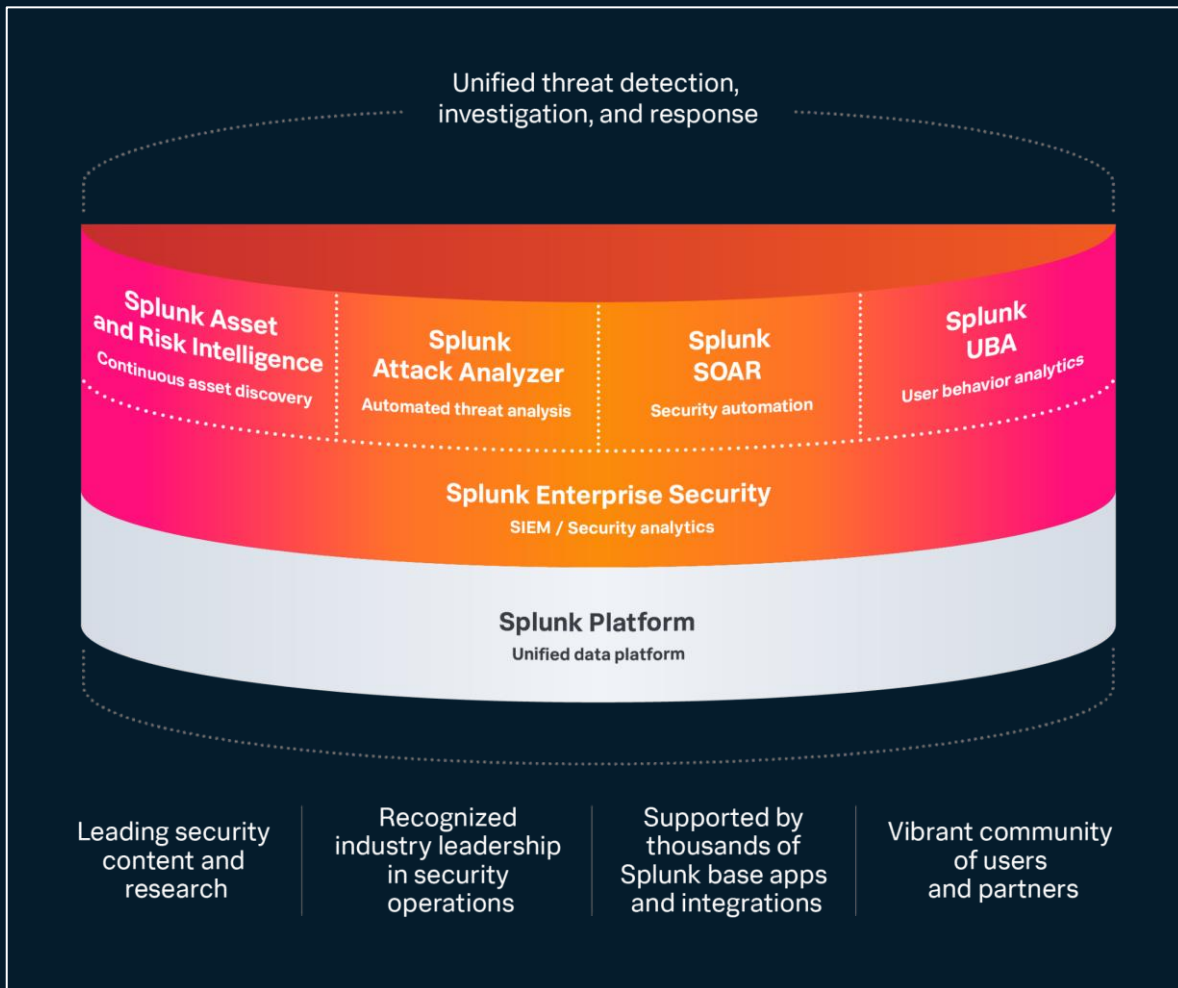


Contextual intelligence



External attack

In Summary



QUESTIONS?

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: sobrien@splunk.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC