Turning Data into Defense

How Splunk can be leveraged to correlate events, visualize risks, and create a proactive security posture.

Cisco Connect | Dallas, TX
December 2024

Chris Perkins, Staff Solutions Architect
Splunk, a Cisco Company

© 2024 SPLUNK INC.

Chris Perkins

- ➔ Staff Solutions Architect
- ➔ 18/4.5
- ➔ Based in New Mexico (ABQ -> LC)

© 2024 SPLUNK INC.

Chris Perkins

- Staff Solutions Architect
- 18/4.5
- Based in New Mexico (ABQ -> LC)

I’m an SME (subject matter expert) in security, anti-fraud and data analytics.

© 2024 SPLUNK INC.

Chris Perkins

- Staff Solutions Architect
- 18/4.5
- Based in New Mexico (ABQ -> LC)

I’m an SME (subject matter expert) in security, anti-fraud and data analytics.

I work at Splunk as a technical seller.

© 2024 SPLUNK INC.

Chris Perkins

- → Staff Solutions Architect
- → 18/4.5
- → Based in New Mexico (ABQ -> LC)

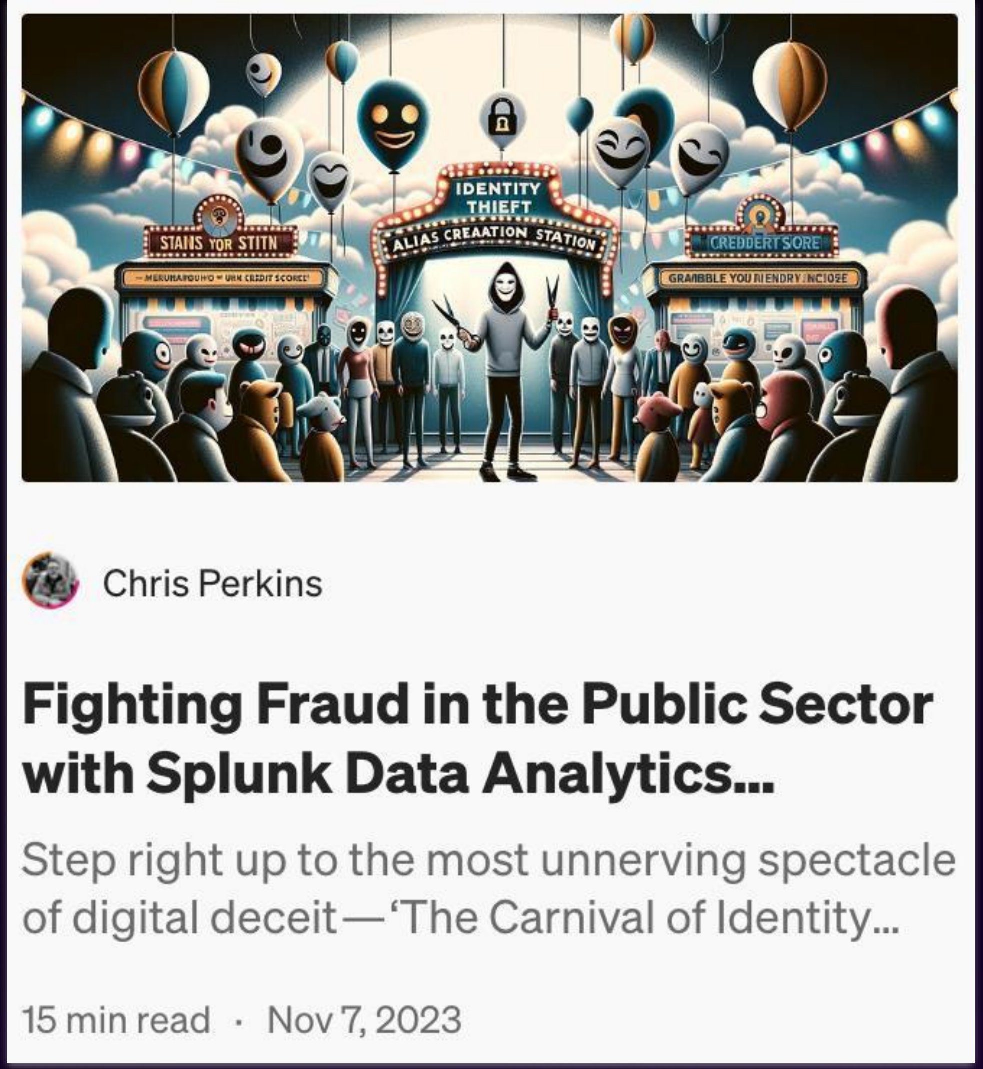
I'm an SME (subject matter expert) in security, anti-fraud and data analytics.

I work at Splunk as a technical seller.

My role includes consulting every state, local and tribal government - as well as all k-20 schools - in the U.S.

© 2024 SPLUNK INC.

Medium 2023-2024

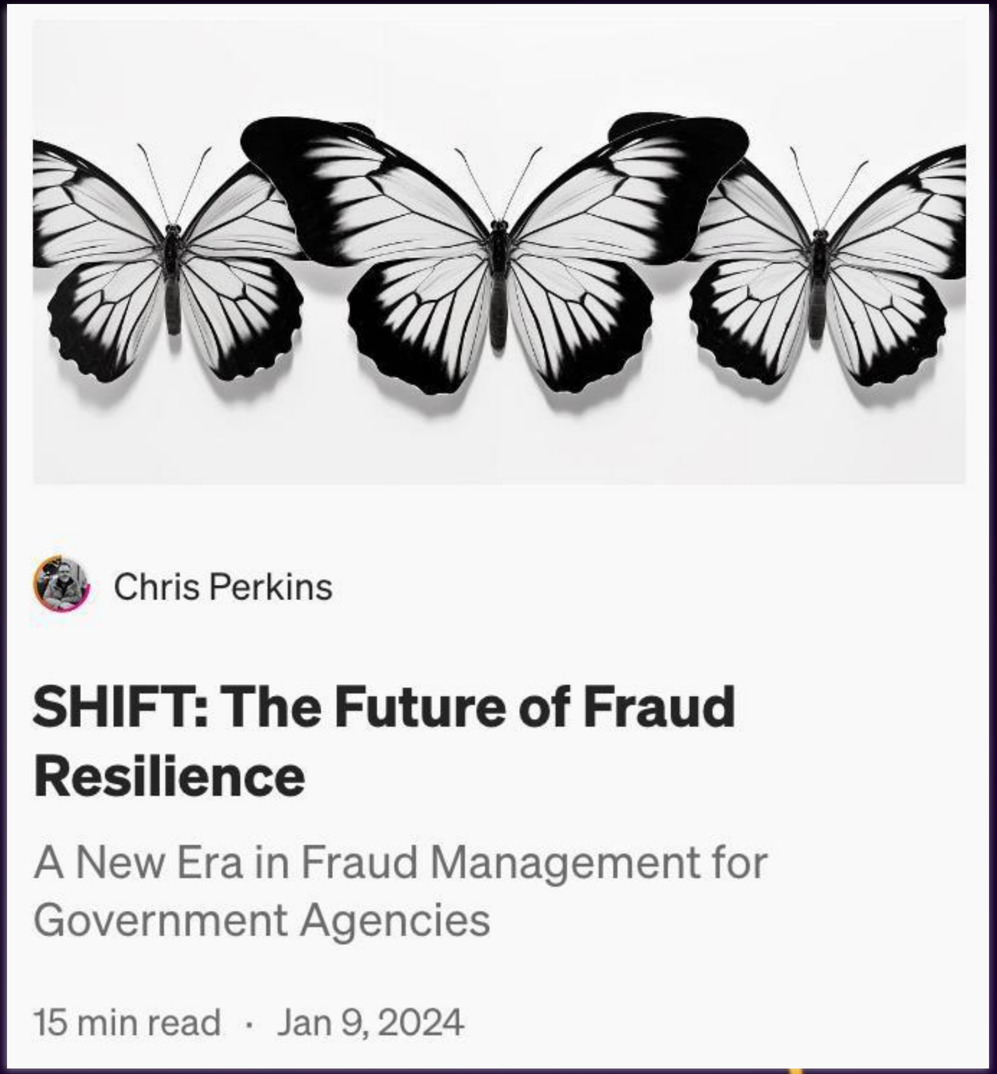


Chris Perkins

Fighting Fraud in the Public Sector with Splunk Data Analytics...

Step right up to the most unnerving spectacle of digital deceit—'The Carnival of Identity...

15 min read · Nov 7, 2023

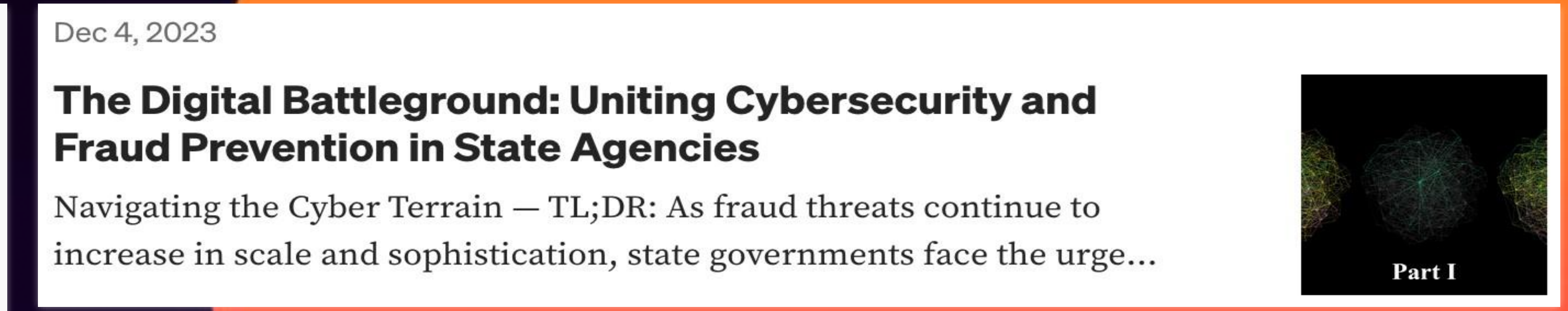


Chris Perkins

SHIFT: The Future of Fraud Resilience

A New Era in Fraud Management for Government Agencies

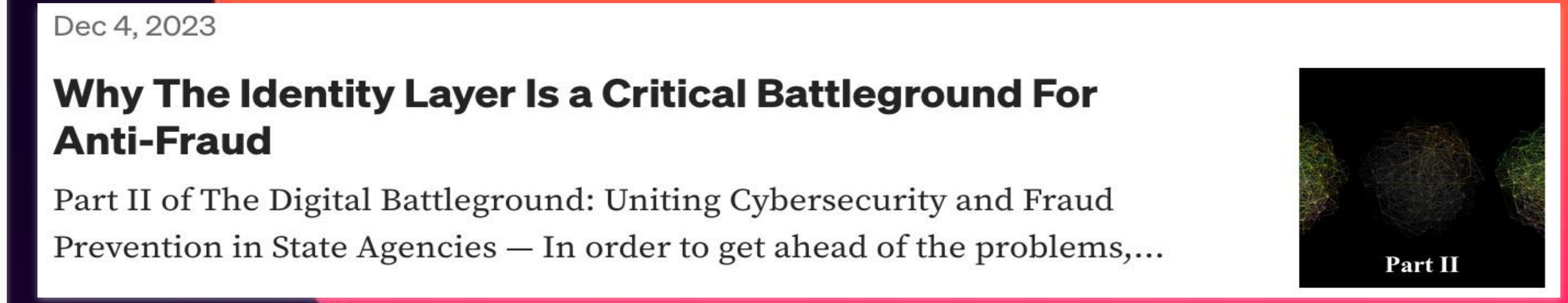
15 min read · Jan 9, 2024



Dec 4, 2023

The Digital Battleground: Uniting Cybersecurity and Fraud Prevention in State Agencies

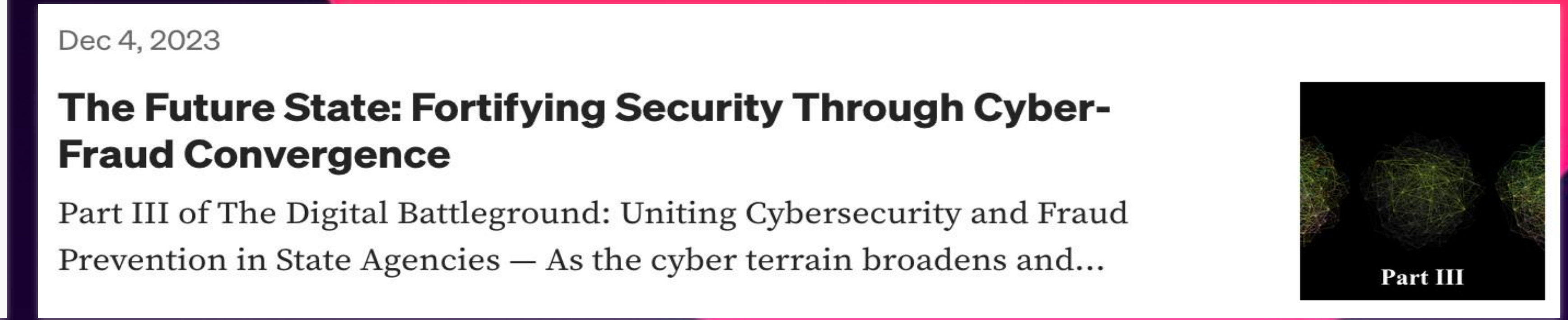
Navigating the Cyber Terrain — TL;DR: As fraud threats continue to increase in scale and sophistication, state governments face the urge...



Dec 4, 2023

Why The Identity Layer Is a Critical Battleground For Anti-Fraud

Part II of The Digital Battleground: Uniting Cybersecurity and Fraud Prevention in State Agencies — In order to get ahead of the problems,...



Dec 4, 2023

The Future State: Fortifying Security Through Cyber-Fraud Convergence

Part III of The Digital Battleground: Uniting Cybersecurity and Fraud Prevention in State Agencies — As the cyber terrain broadens and...

https://medium.com/@chrisperkins505

© 2024 SPLUNK INC.

Chris Perkins

ODAM, a Revolution! Reinventing the Cybersecurity Workforce in...

In this article, we're going to take a deep dive into two intertwined challenges that public...

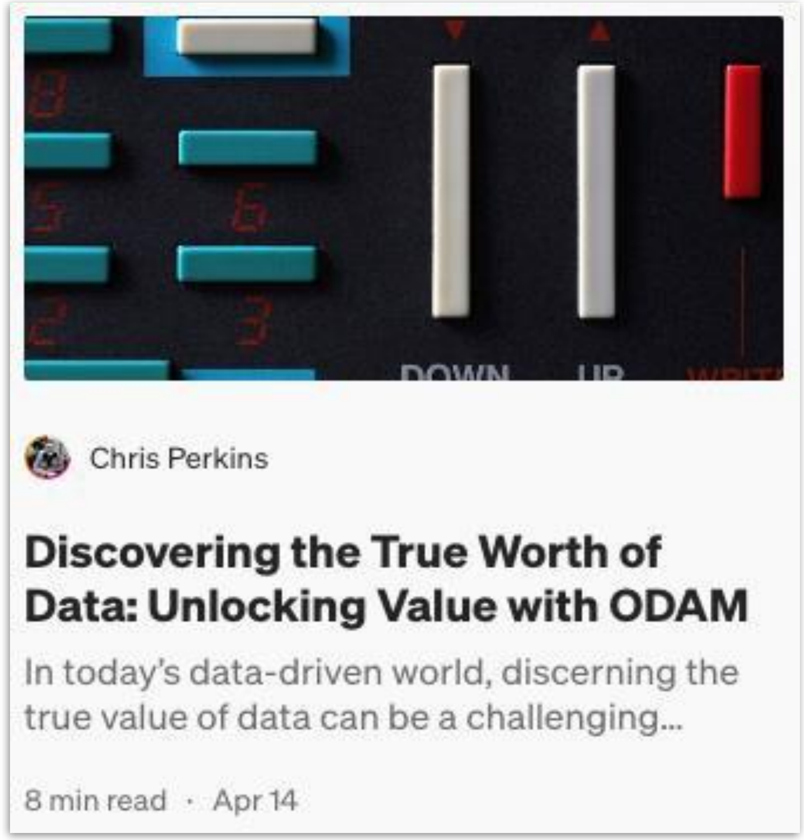
12 min read · 1 day ago

Chris Perkins

Unraveling Zero Trust: An Airport Security Analogy + ODAM

This blog post aims to present a comprehensive examination of the intricate...

6 min read · Jun 30

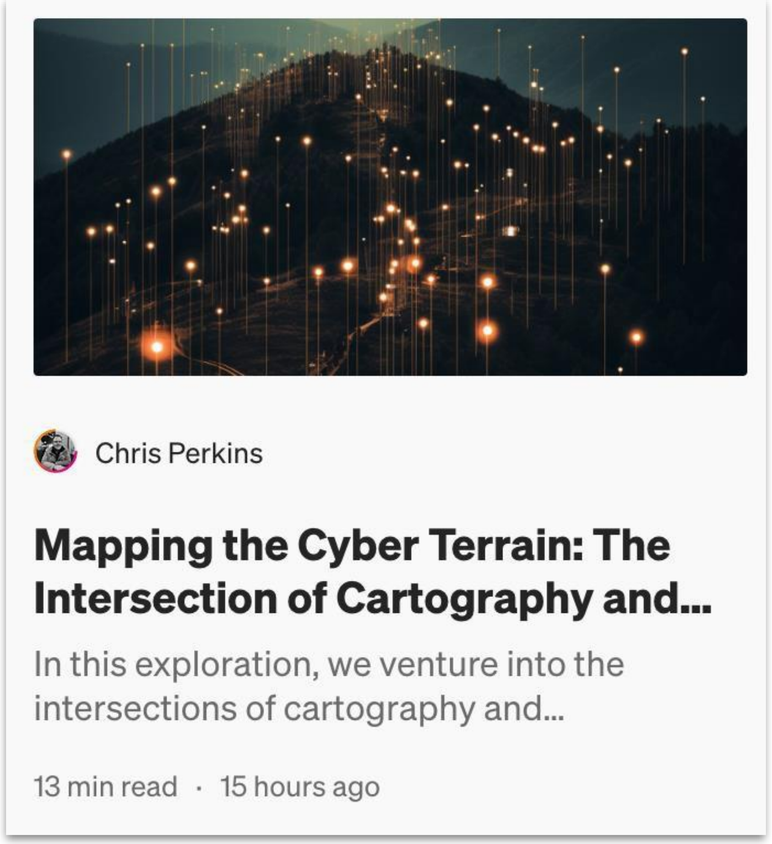


Chris Perkins

Discovering the True Worth of Data: Unlocking Value with ODAM

In today's data-driven world, discerning the true value of data can be a challenging...

8 min read · Apr 14



Chris Perkins

Mapping the Cyber Terrain: The Intersection of Cartography and...

In this exploration, we venture into the intersections of cartography and...

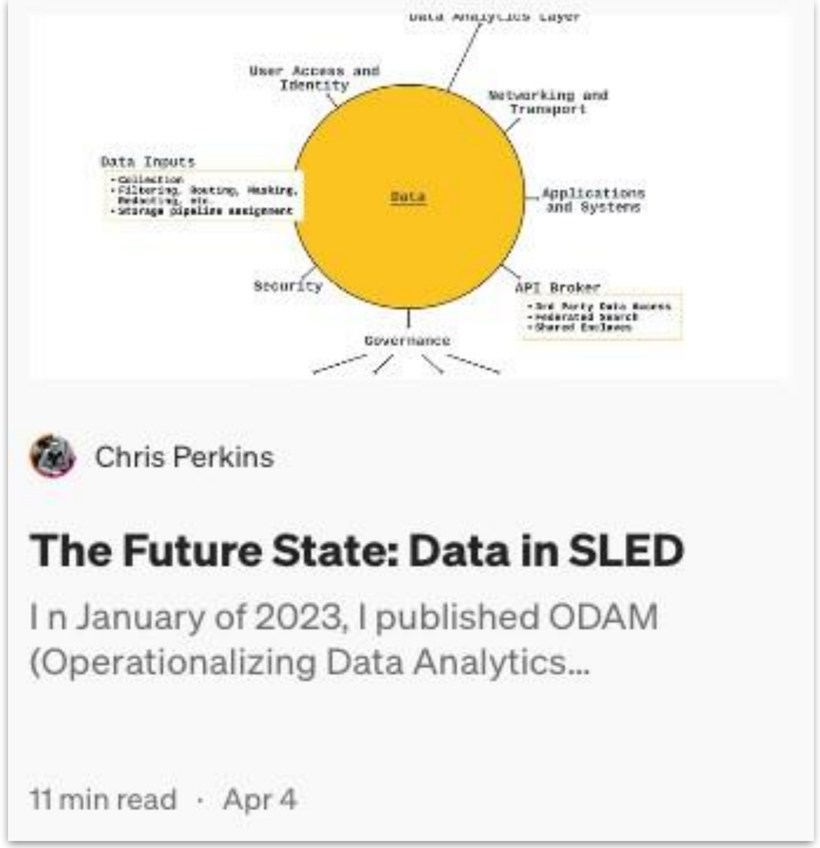
13 min read · 15 hours ago

Chris Perkins

ODAM: a Digital Resilience Strategy

Operationalizing Data Analytics Methodology (ODAM) is a game-changer for organization...

3 min read · Apr 5



Chris Perkins

The Future State: Data in SLED

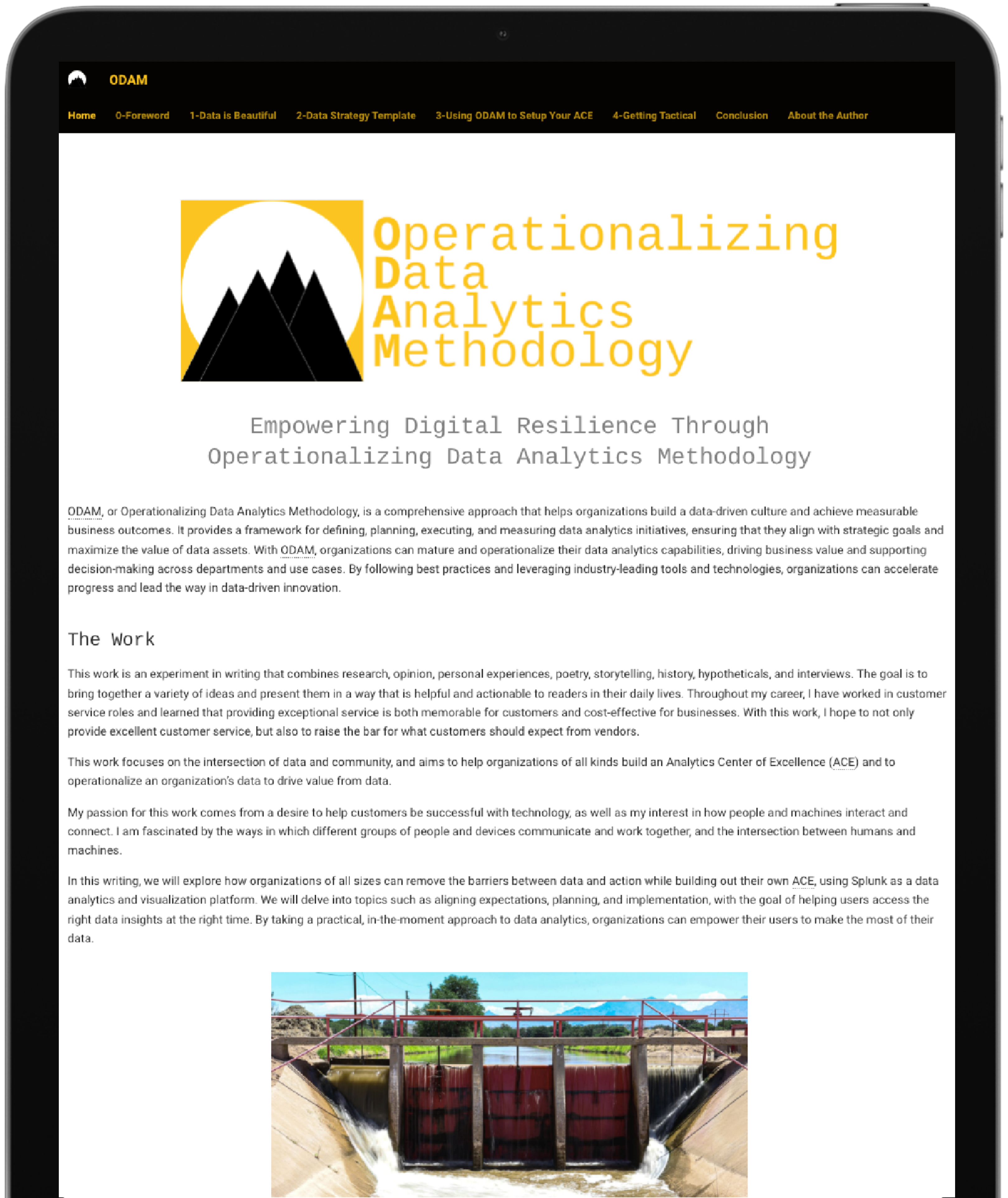
I n January of 2023, I published ODAM (Operationalizing Data Analytics...

11 min read · Apr 4

Medium

2023

© 2021 SPLUNK INC.



Operationalizing Data Analytics Methodology

Empowering Digital Resilience Through
Operationalizing Data Analytics Methodology

ODAM, or Operationalizing Data Analytics Methodology, is a comprehensive approach that helps organizations build a data-driven culture and achieve measurable business outcomes. It provides a framework for defining, planning, executing, and measuring data analytics initiatives, ensuring that they align with strategic goals and maximize the value of data assets. With ODAM, organizations can mature and operationalize their data analytics capabilities, driving business value and supporting decision-making across departments and use cases. By following best practices and leveraging industry-leading tools and technologies, organizations can accelerate progress and lead the way in data-driven innovation.

The Work

This work is an experiment in writing that combines research, opinion, personal experiences, poetry, storytelling, history, hypotheticals, and interviews. The goal is to bring together a variety of ideas and present them in a way that is helpful and actionable to readers in their daily lives. Throughout my career, I have worked in customer service roles and learned that providing exceptional service is both memorable for customers and cost-effective for businesses. With this work, I hope to not only provide excellent customer service, but also to raise the bar for what customers should expect from vendors.

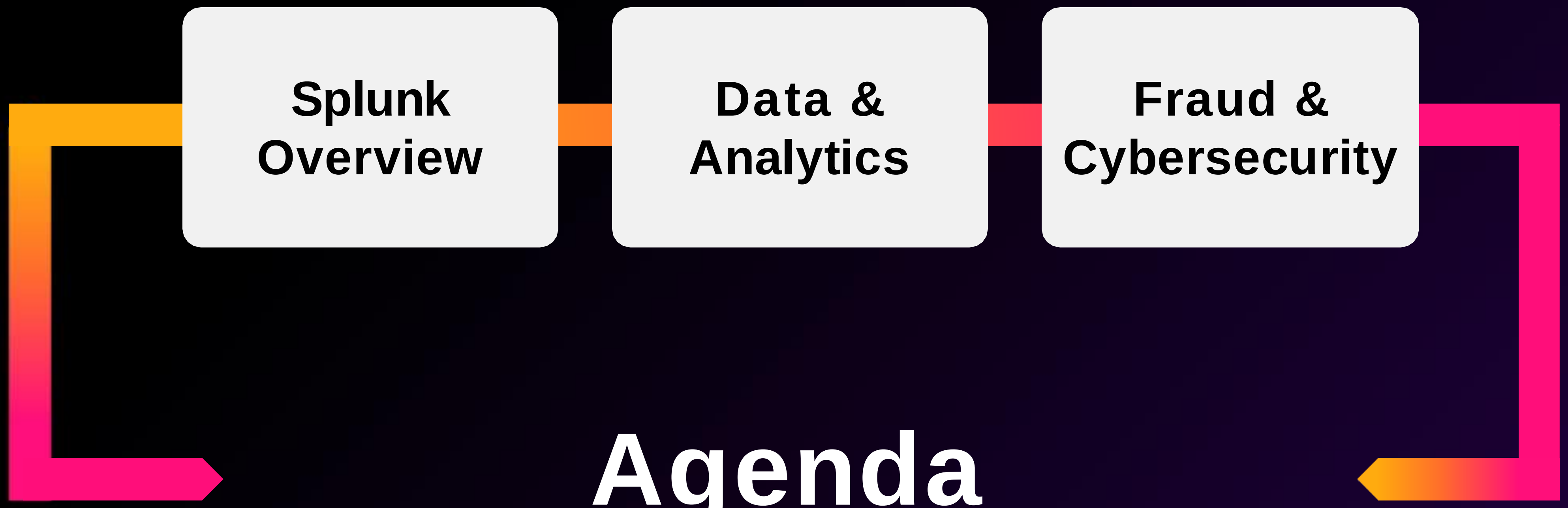
This work focuses on the intersection of data and community, and aims to help organizations of all kinds build an Analytics Center of Excellence (ACE) and to operationalize an organization's data to drive value from data.

My passion for this work comes from a desire to help customers be successful with technology, as well as my interest in how people and machines interact and connect. I am fascinated by the ways in which different groups of people and devices communicate and work together, and the intersection between humans and machines.

In this writing, we will explore how organizations of all sizes can remove the barriers between data and action while building out their own ACE, using Splunk as a data analytics and visualization platform. We will delve into topics such as aligning expectations, planning, and implementation, with the goal of helping users access the right data insights at the right time. By taking a practical, in-the-moment approach to data analytics, organizations can empower their users to make the most of their data.

odam.community

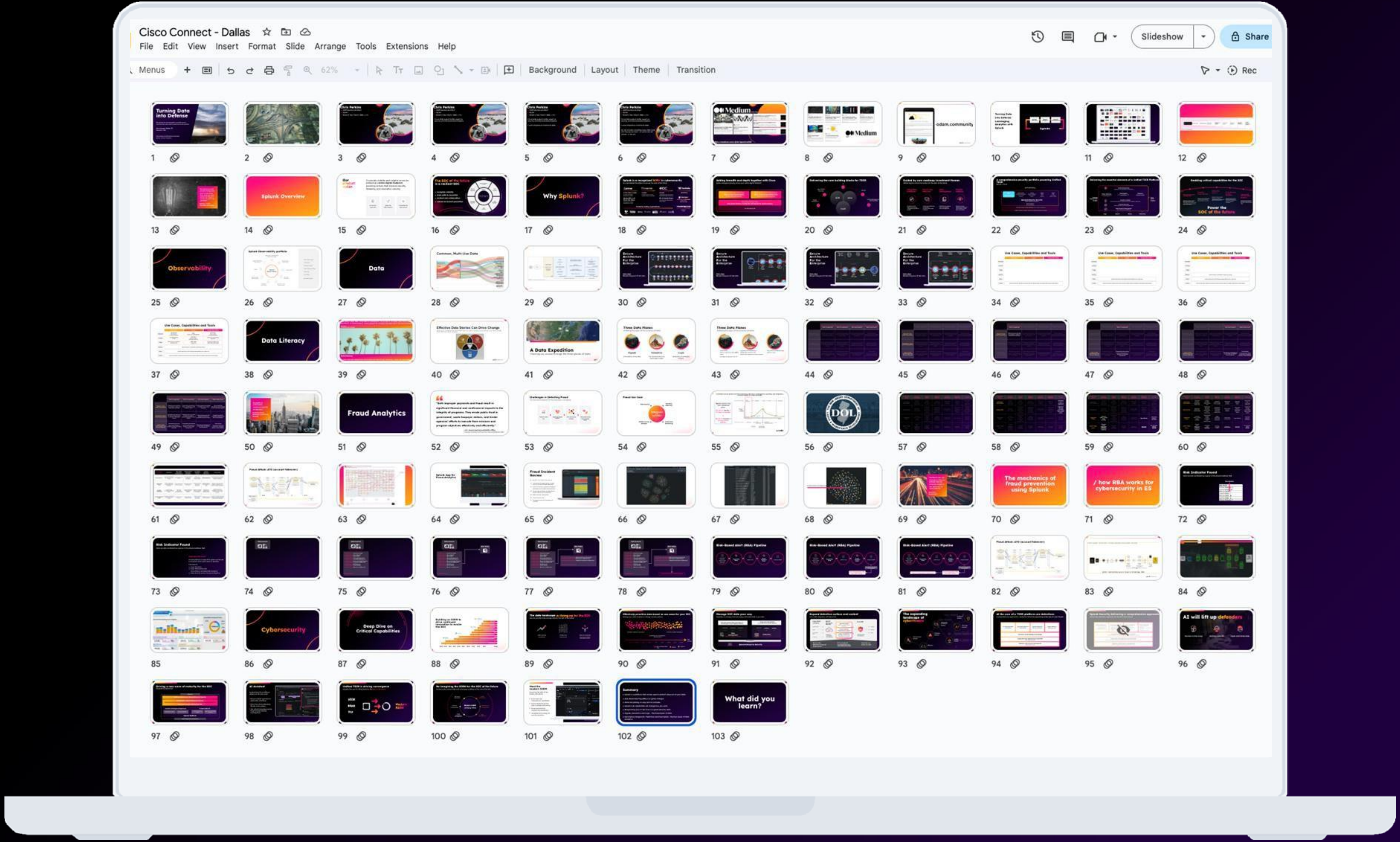
Turning Data into Defense: Leveraging Analytics with Splunk



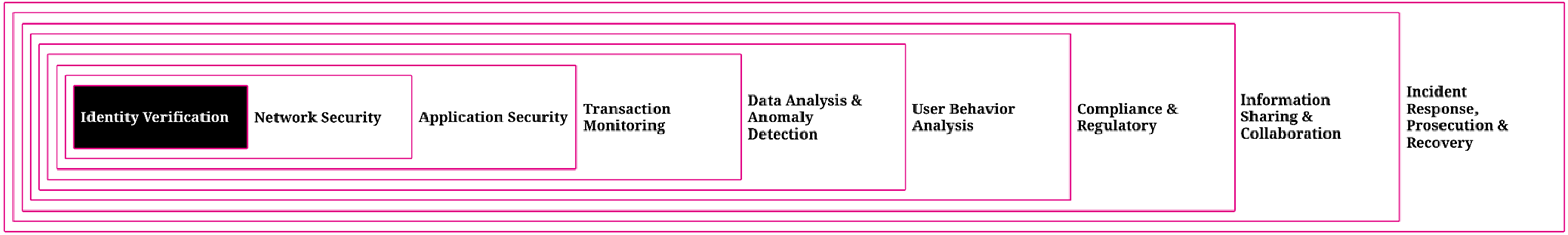
Agenda

- Splunk Overview
- Data & Analytics
- Fraud & Cybersecurity

© 2024 SPLUNK INC.



© 2024 SPLUNK INC.



Identity Verification

Network Security

Application Security

Transaction Monitoring

Data Analysis & Anomaly Detection

User Behavior Analysis

Compliance & Regulatory

Information Sharing & Collaboration

Incident Response, Prosecution & Recovery

The Layers of Complexity

© 2024 SPLUNK INC.

“ Our dilemma is that we hate change and love it at the same time; what we really want is for things to remain the same but get better.”

Sydney J. Harris
Journalist and Author

Splunk Overview

© 2024 SPLUNK INC.

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

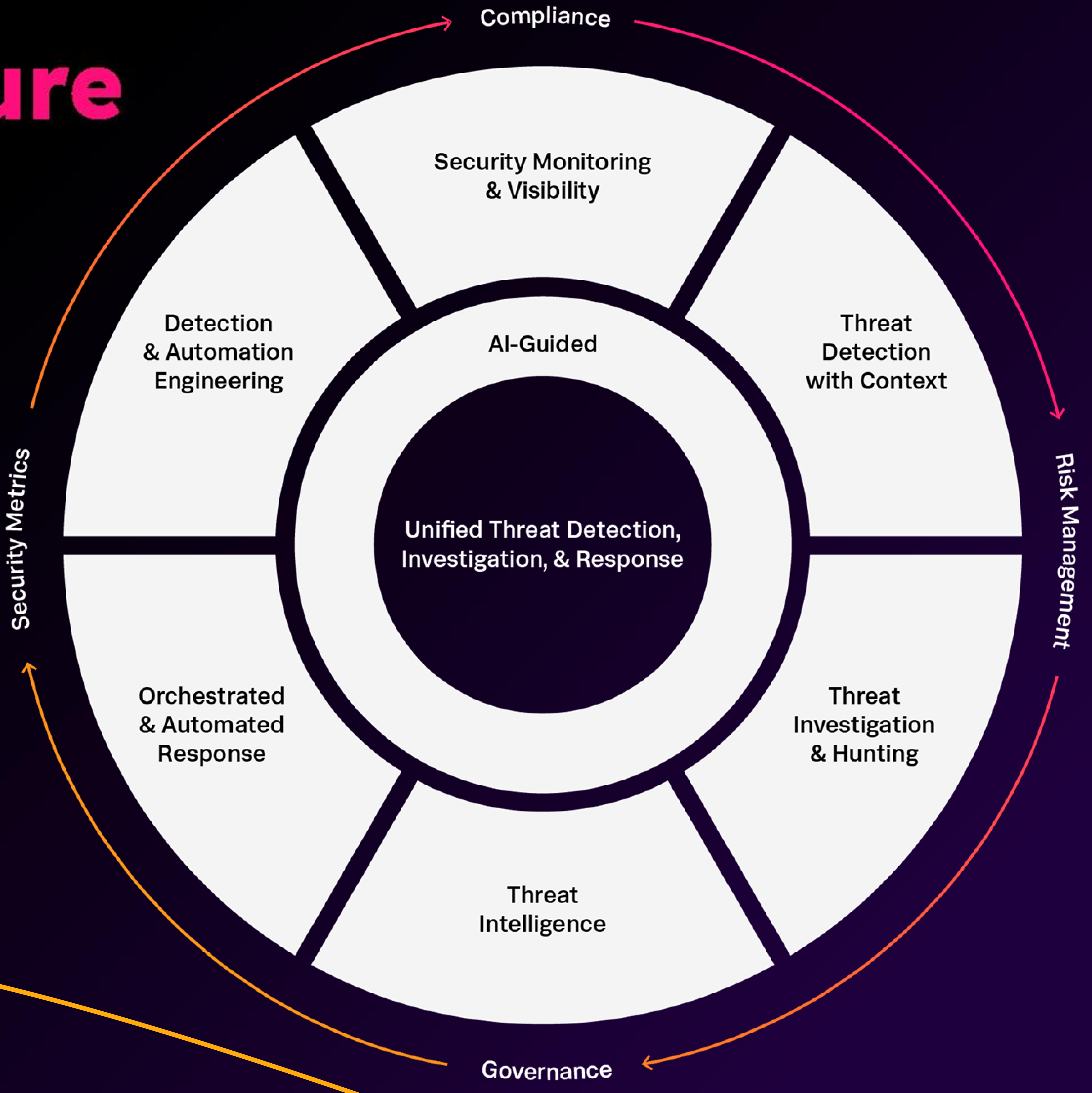
Apply the right analytics

Accelerate the right actions

© 2024 SPLUNK INC.

The SOC of the future is a resilient SOC

- Complete visibility
- Clear path to resolution
- xt and collaboration
- ovement prevention


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

Why Splunk?

© 2024 SPLUNK LLC

Splunk is a recognized leader in cybersecurity

An unparalleled foundation to power the SOC of the future

Gartner®

A Ten-Time Leader

2024 Gartner® Magic Quadrant™ for SIEM

Ranked #1 in all three Use Cases

2024 Gartner® Critical Capabilities for SIEM

FORRESTER®

Leader

Forrester Wave™: Security Analytics Platforms, Q4 2022

IDC

Leader

IDC MarketScape: Worldwide SIEM 2023 Vendor Assessment

#1 in Market Share

IDC Worldwide SIEM Market Share Report

TrustRadius

5 awards for
SIEM and SOAR

PeerSpot

Leader Award
SIEM and SOAR

kuppingercole ANALYSTS

A leader in
SOAR

Trusted by leading organizations

Soriana · tide · TESCO · CAL POLY · REI co-op · Carnival® · SINGAPORE AIRLINES

© 2024 SPLUNK LLC

Adding breadth and depth together with Cisco

Game-changing security across your entire digital footprint

Secure Data Center Networking
Enhance multi-cloud protection
for AI-ready data centers.

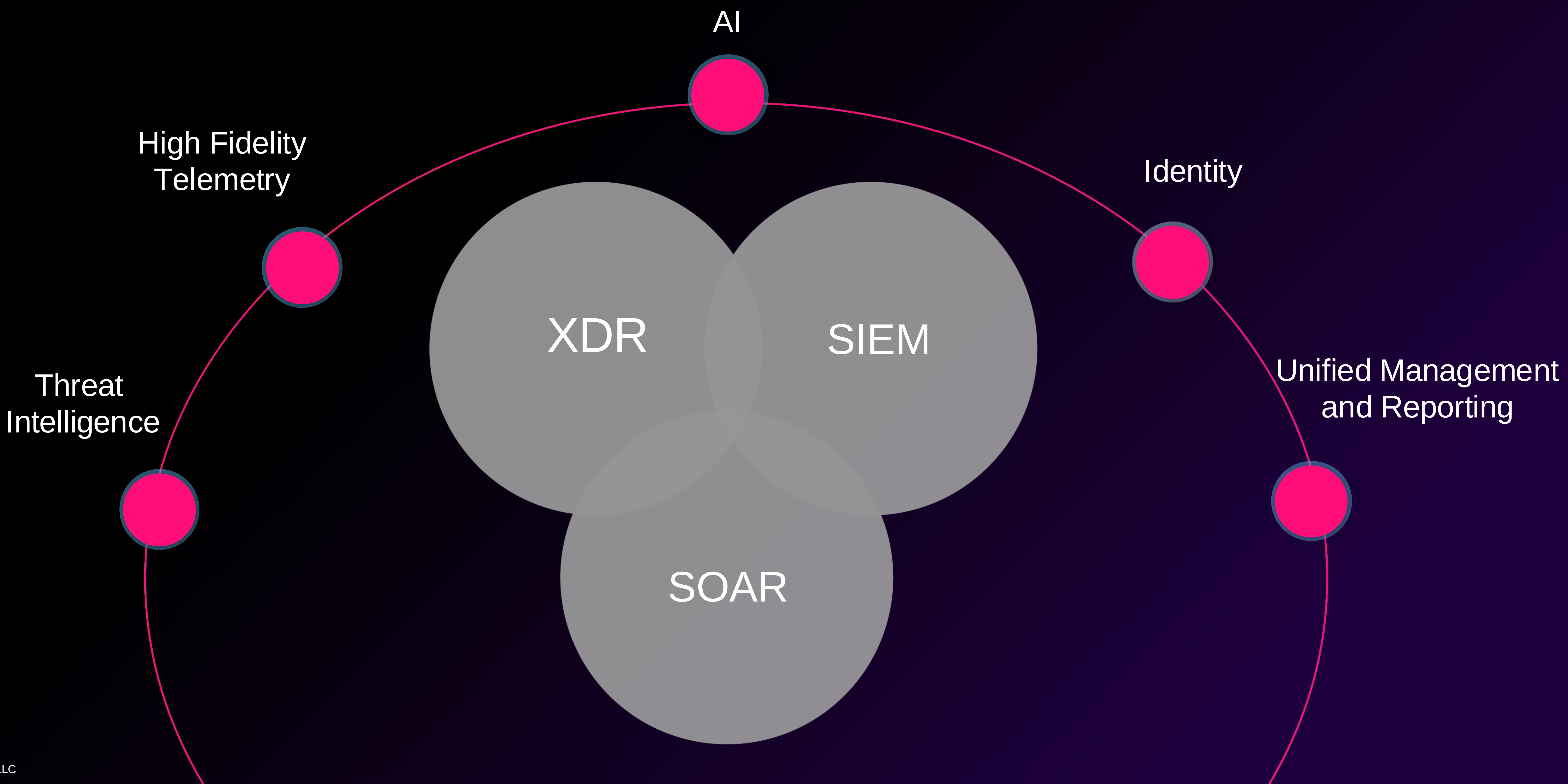
Accelerate Zero Trust Network Access
Enable Secure Access and Zero Trust
for a future-proof workplace.

Power Security Operations
Unify threat detection, investigation and response for digital resilience.

Accelerated by AI

© 2024 SPLUNK LLC

Delivering the core building blocks for TDIR



© 2024 SPLUNK LLC

Guided by core roadmap investment themes

Delivering the critical innovation for the SOC of the future

Integrated workflows

Simplify the SOC experience through integrated automation and AI.

World class detection

World class detections powered by purpose-built threat analytics.

Data management

Flexibility to optimize costs and simplify data management.

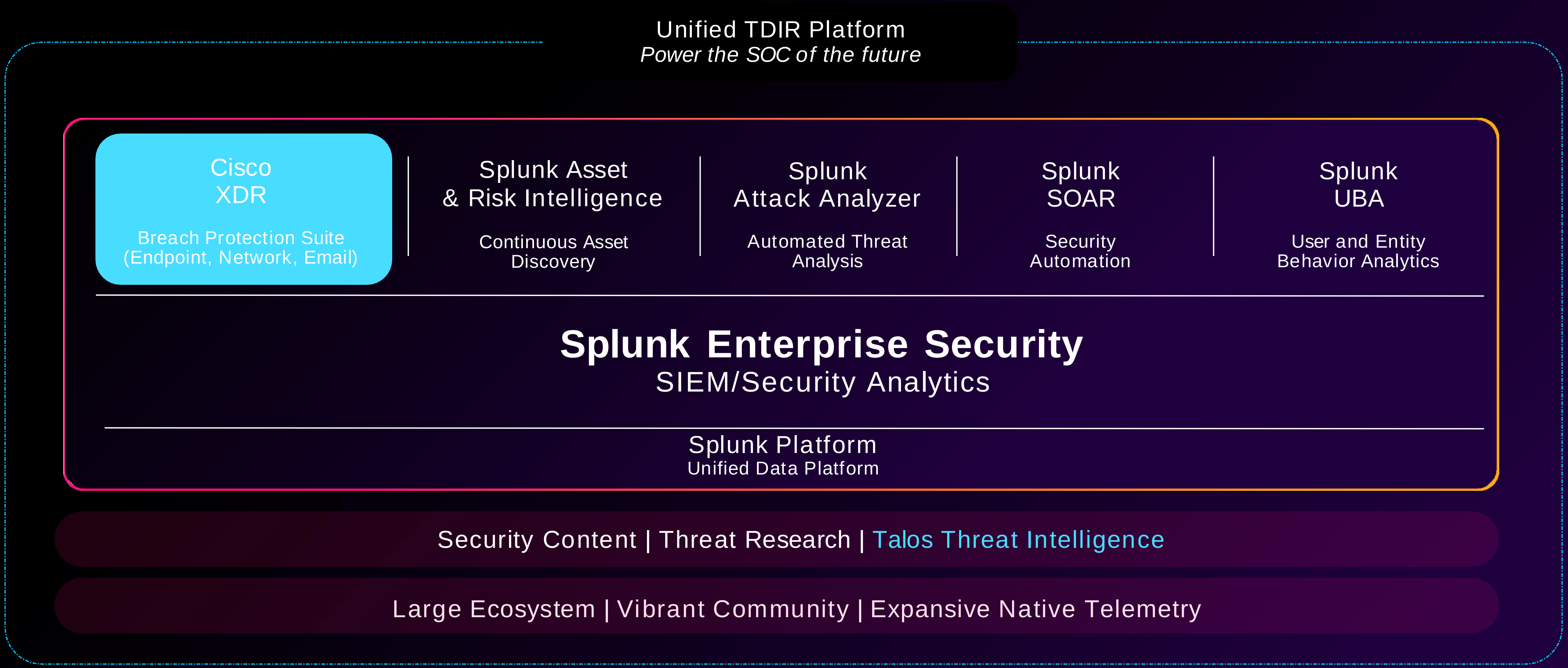
Flexible platform

Enterprise-scale deployment flexibility across hybrid, cloud and on-premises.

© 2024 SPLUNK LLC

A comprehensive security portfolio powering Unified TDIR

Splunk + Cisco



Unified TDIR Platform
Power the SOC of the future

Cisco XDR
Breach Protection Suite (Endpoint, Network, Email)

Splunk Asset & Risk Intelligence
Continuous Asset Discovery

Splunk Attack Analyzer
Automated Threat Analysis

Splunk SOAR
Security Automation

Splunk UBA
User and Entity Behavior Analytics

Splunk Enterprise Security
SIEM/Security Analytics

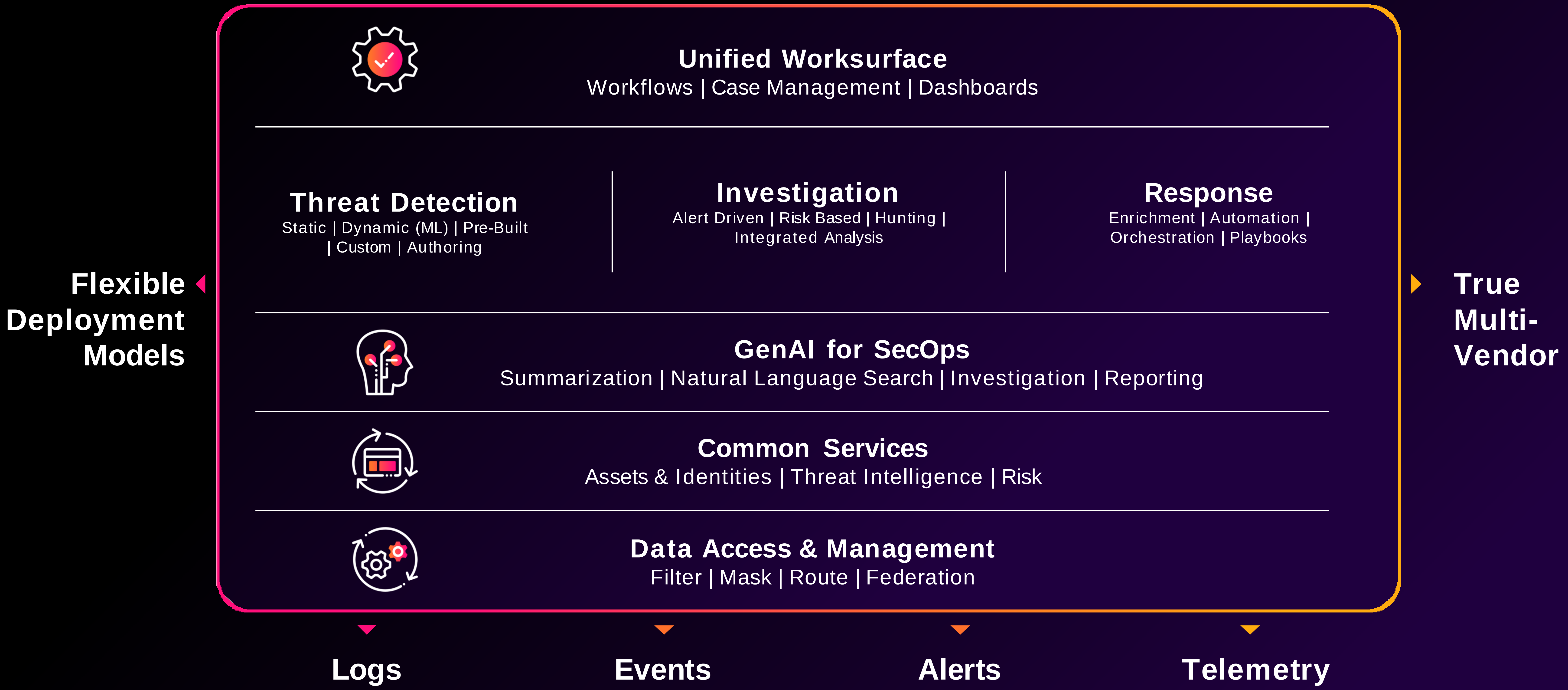
Splunk Platform
Unified Data Platform

Security Content | Threat Research | Talos Threat Intelligence

Large Ecosystem | Vibrant Community | Expansive Native Telemetry

© 2024 SPLUNK LLC

Delivering the essential elements of a Unified TDIR Platform



Flexible Deployment Models

Unified Worksurface
Workflows | Case Management | Dashboards

Threat Detection
Static | Dynamic (ML) | Pre-Built | Custom | Authoring

Investigation
Alert Driven | Risk Based | Hunting | Integrated Analysis

Response
Enrichment | Automation | Orchestration | Playbooks

GenAI for SecOps
Summarization | Natural Language Search | Investigation | Reporting

Common Services
Assets & Identities | Threat Intelligence | Risk

Data Access & Management
Filter | Mask | Route | Federation

True Multi-Vendor

Logs **Events** **Alerts** **Telemetry**

© 2024 SPLUNK LLC

Enabling critical capabilities for the SOC

Data Management & Federation

Effectively manage complex data management needs. Seamlessly access data stored across different data stores for search and analytics.

Transform Threat Detection

Support a range of detection methodologies. Effectively utilize detection as a code.

Reduce Risk Exposure

Unleash continuous asset discovery to enhance compliance posture and close gaps in security controls.

AI for Enhanced Security Operations

Augment with AI to help analysts with routine yet error-prone tasks such as writing investigative summaries.

Unified TDIR with Automated Workflows

Coordinate and collaborate across the TDIR lifecycle. Automate workflows across TDIR.

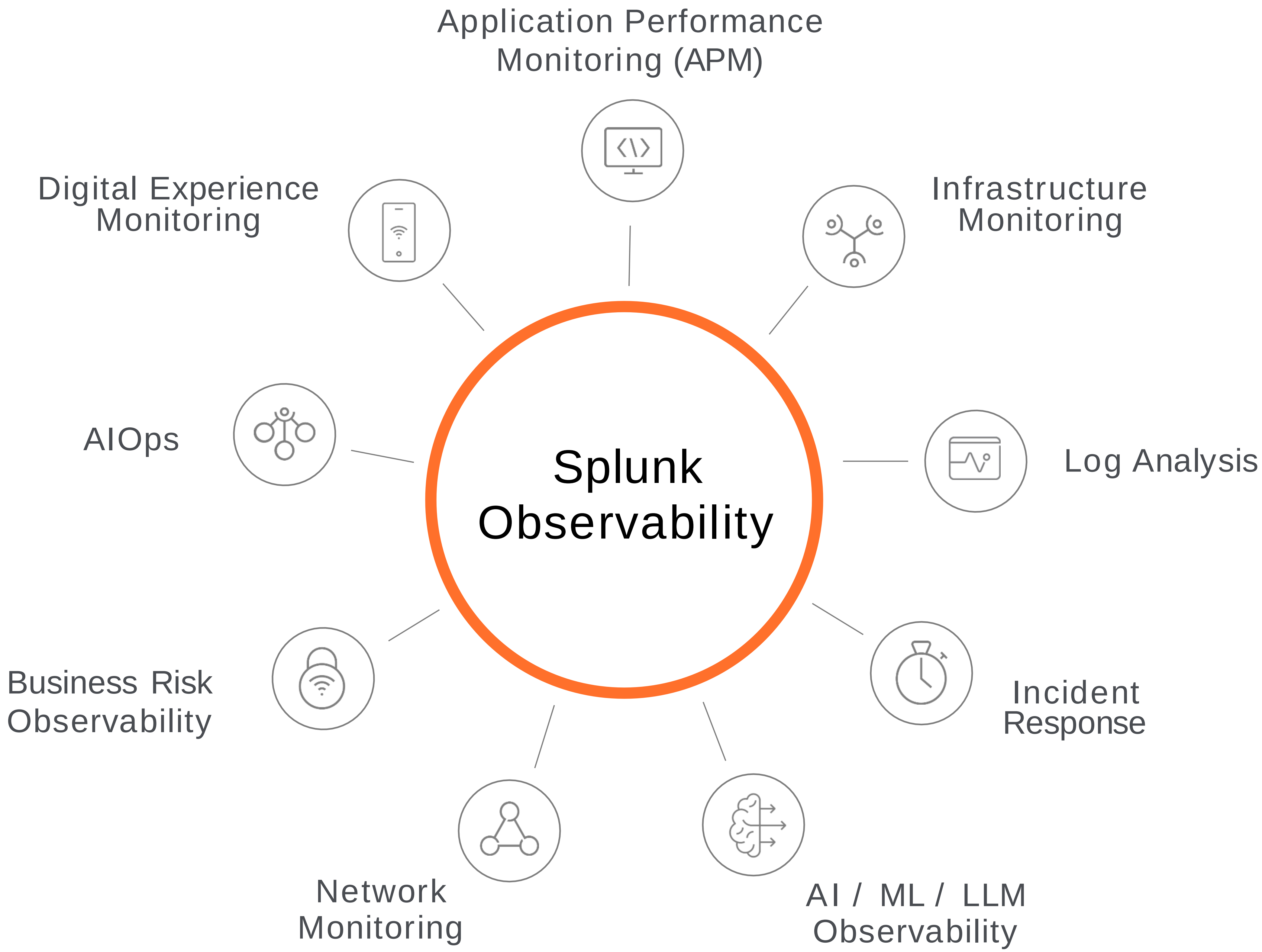
Power the SOC of the future

© 2024 SPLUNK LLC

Observability

© 2024 SPLUNK LLC

Splunk Observability portfolio


Application Performance Monitoring (APM)
Digital Experience Monitoring
Infrastructure Monitoring
AIOps
Splunk Observability
Log Analysis
Business Risk Observability
Incident Response
Network Monitoring
AI / ML / LLM Observability

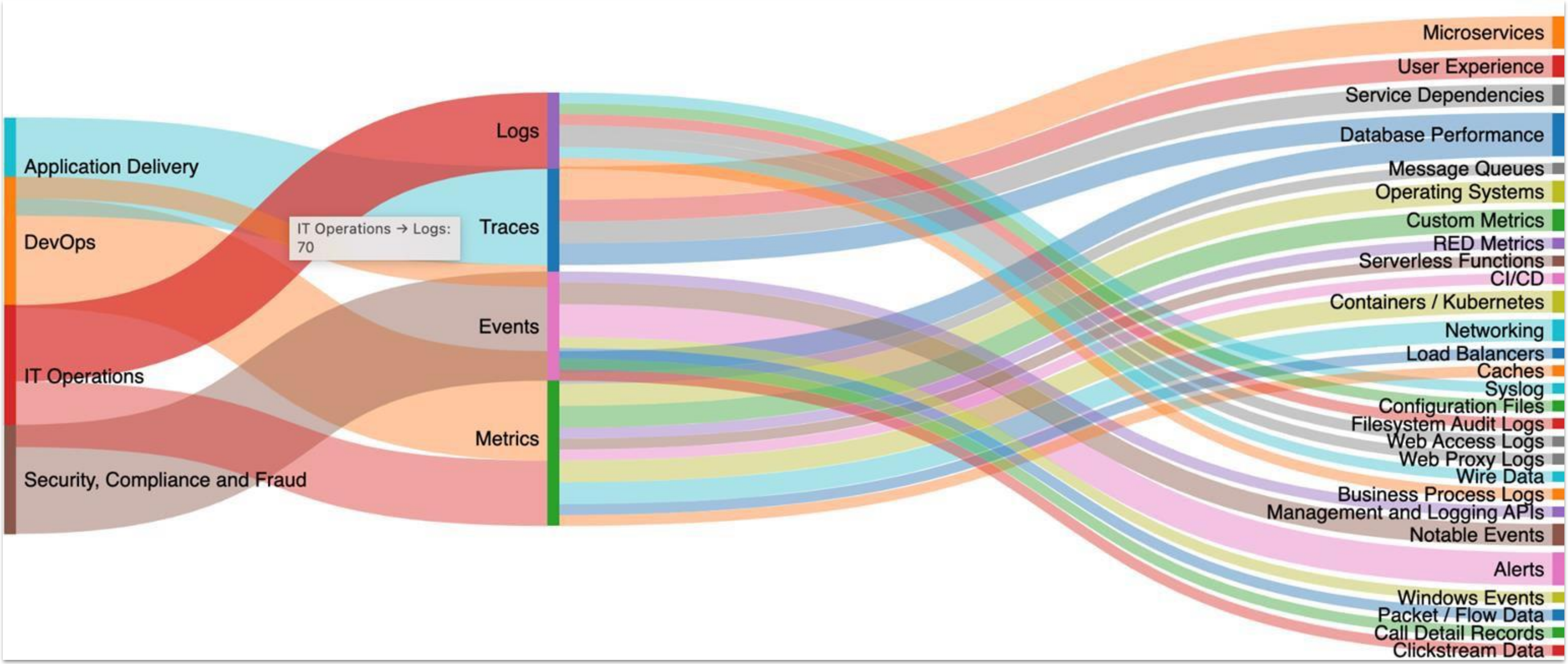
- Real-Time Insights
- AI Powered
- Enterprise Grade
- Open Telemetry Native
- Extensible
- Cross MELT
- Business Context

© 2024 SPLUNK LLC

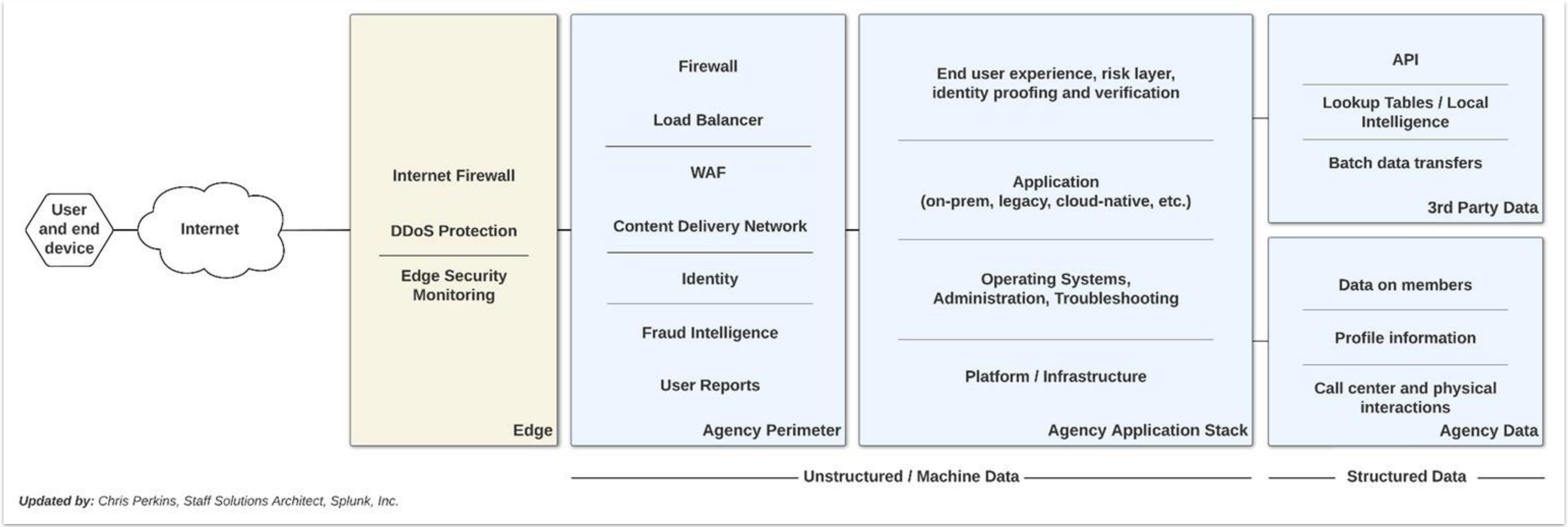
Data

© 2024 SPLUNK LLC

Common, Multi-Use Data



© 2024 SPLUNK INC.



User and end device

Internet

Internet Firewall

DDoS Protection

Edge Security Monitoring

Edge

Firewall

Load Balancer

WAF

Content Delivery Network

Identity

Fraud Intelligence

User Reports

Agency Perimeter

End user experience, risk layer, identity proofing and verification

Application (on-prem, legacy, cloud-native, etc.)

Operating Systems, Administration, Troubleshooting

Platform / Infrastructure

Agency Application Stack

API

Lookup Tables / Local Intelligence

Batch data transfers

3rd Party Data

Data on members

Profile information

Call center and physical interactions

Agency Data

Unstructured / Machine Data

Structured Data

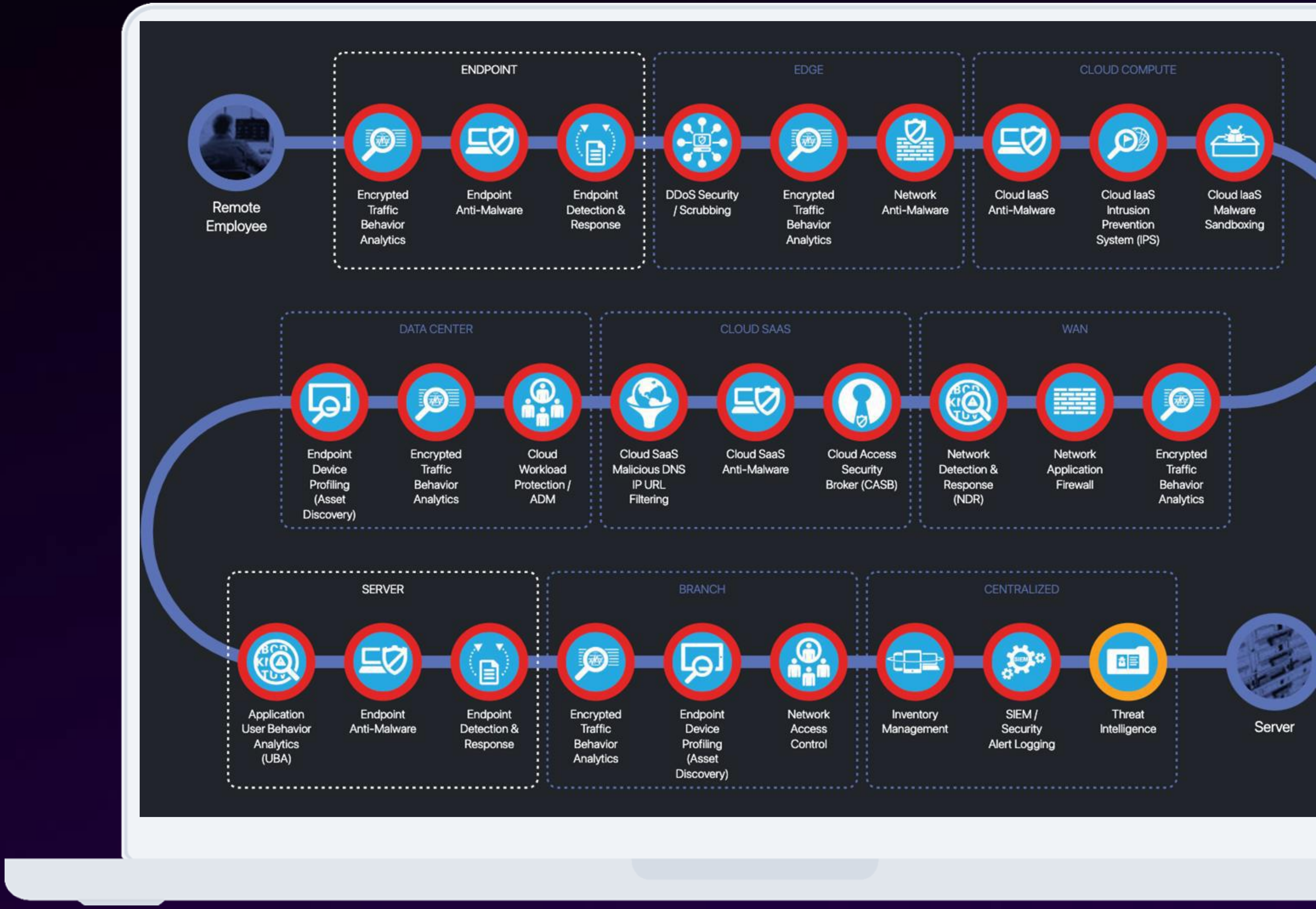
Updated by: *Chris Perkins, Staff Solutions Architect, Splunk, Inc.*

© 2024 SPLUNK INC.

Secure Architecture For the Enterprise

Main idea:

Blueprinting your IT Services.



Remote Employee

ENDPOINT

Encrypted Traffic Behavior Analytics

Endpoint Anti-Malware

Endpoint Detection & Response

EDGE

DDoS Security / Scrubbing

Encrypted Traffic Behavior Analytics

Network Anti-Malware

CLOUD COMPUTE

Cloud IaaS Anti-Malware

Cloud IaaS Intrusion Prevention System (IPS)

Cloud IaaS Malware Sandboxing

DATA CENTER

Endpoint Device Profiling (Asset Discovery)

Encrypted Traffic Behavior Analytics

Cloud Workload Protection / ADM

CLOUD SAAS

Cloud SaaS Malicious DNS IP URL Filtering

Cloud SaaS Anti-Malware

Cloud Access Security Broker (CASB)

WAN

Network Detection & Response (NDR)

Network Application Firewall

Encrypted Traffic Behavior Analytics

SERVER

Application User Behavior Analytics (UBA)

Endpoint Anti-Malware

Endpoint Detection & Response

BRANCH

Encrypted Traffic Behavior Analytics

Endpoint Device Profiling (Asset Discovery)

Network Access Control

CENTRALIZED

Inventory Management

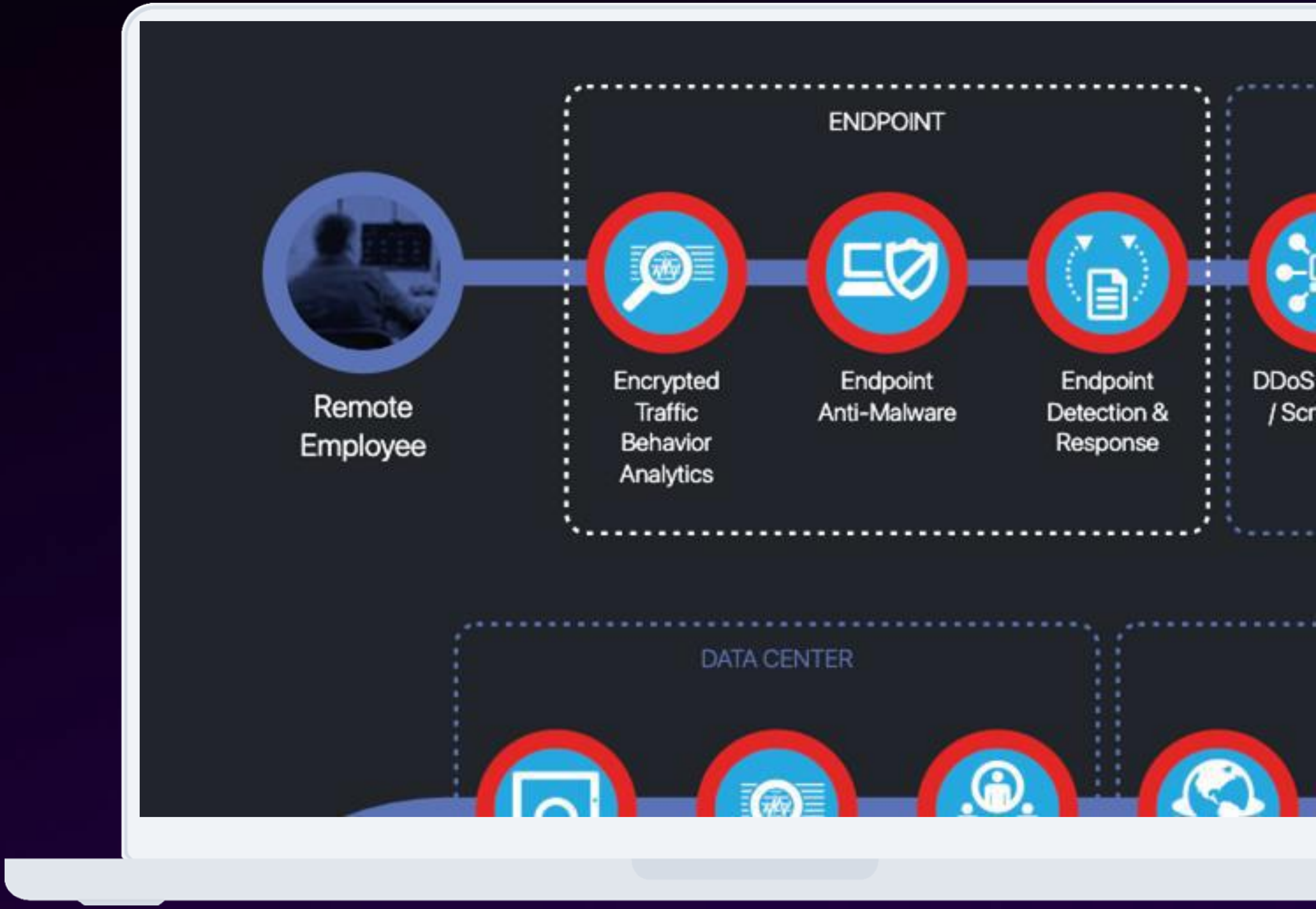
SIEM / Security Alert Logging

Threat Intelligence

Server

© 2024 SPLUNK INC.

Secure Architecture For the Enterprise

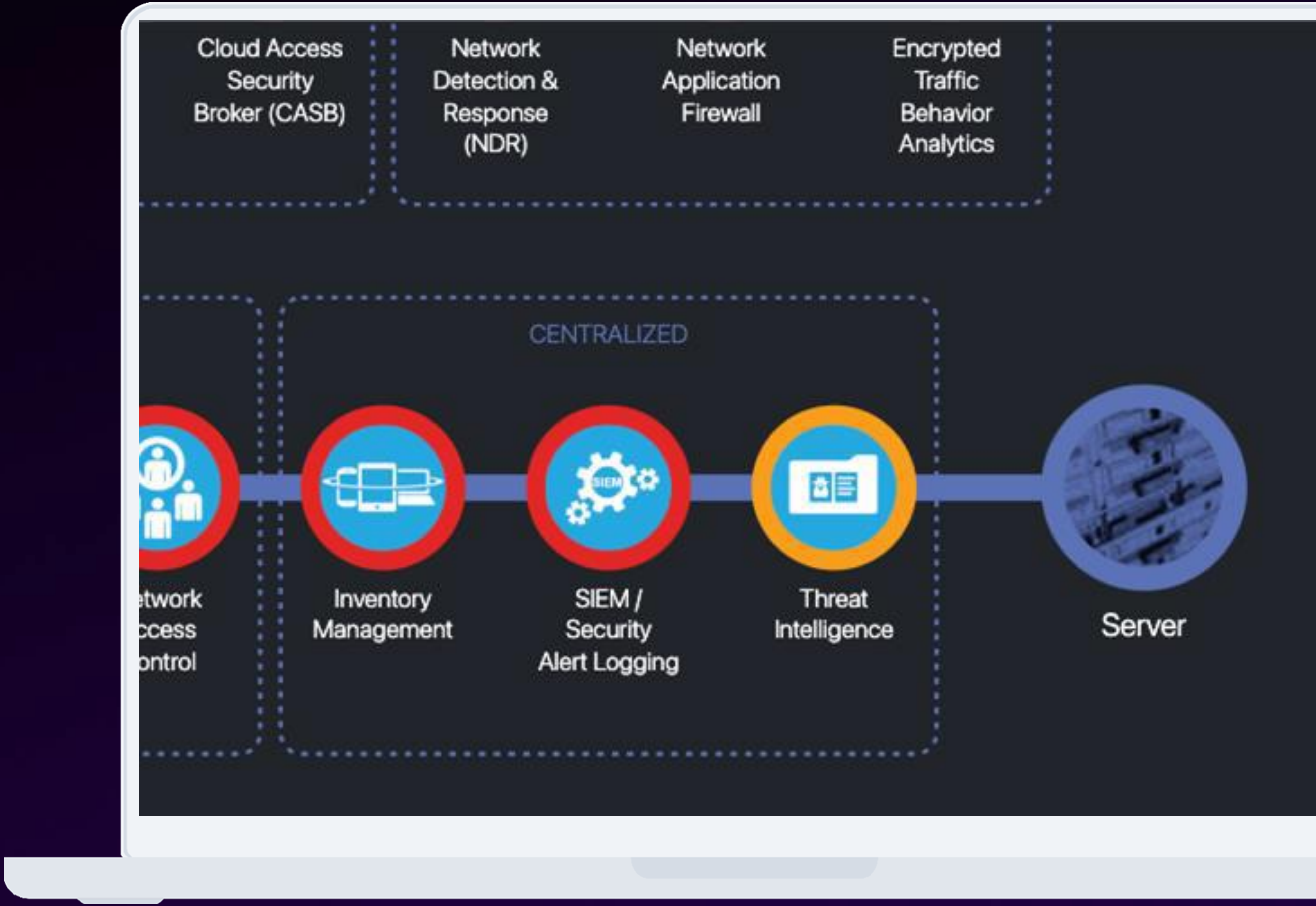

ENDPOINT
Remote Employee
Encrypted Traffic Behavior Analytics
Endpoint Anti-Malware
Endpoint Detection & Response
DDoS / Scr
DATA CENTER

Main idea:

Blueprinting your IT Services.

© 2024 SPLUNK INC.

Secure Architecture For the Enterprise


Cloud Access Security Broker (CASB)
Network Detection & Response (NDR)
Network Application Firewall
Encrypted Traffic Behavior Analytics
CENTRALIZED
SIEM
twork ccess ontrol
Inventory Management
SIEM / Security Alert Logging
Threat Intelligence
Server

Main idea:

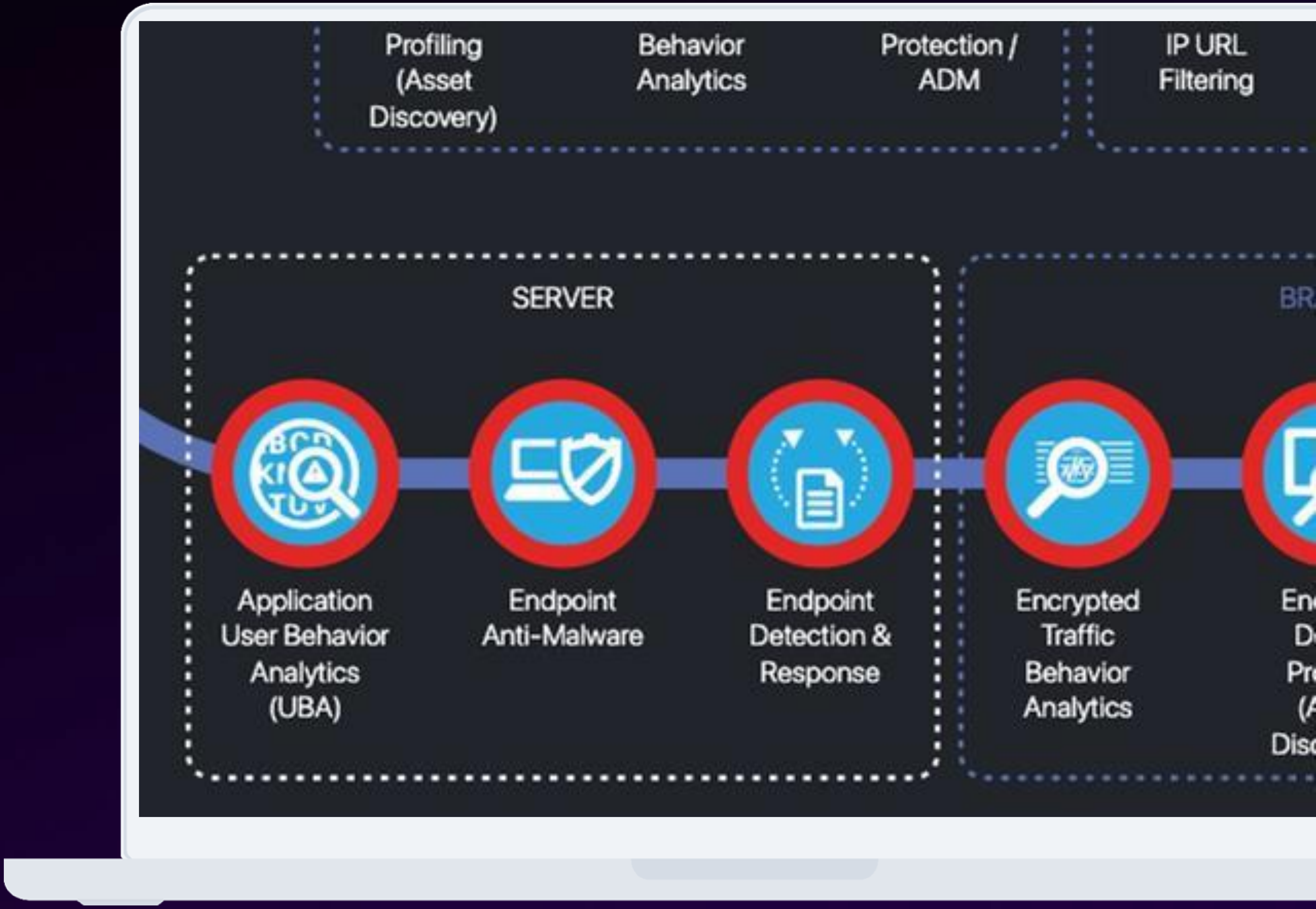
Blueprinting your IT Services.

© 2024 SPLUNK INC.

Secure Architecture For the Enterprise

Main idea:

Blueprinting your IT Services.


Profiling (Asset Discovery)
Behavior Analytics
Protection / ADM
IP URL Filtering
SERVER
BR
Application User Behavior Analytics (UBA)
Endpoint Anti-Malware
Endpoint Detection & Response
Encrypted Traffic Behavior Analytics
En
D
Pr
(A
Disc

© 2024 SPLUNK INC.

Use Cases, Capabilities and Tools

	IT Operations	Security	DevOps Observability
Automate			
Analyze			
Triage			
Monitor			
Store			
Collect	Universal Collection | Stream Processing | Real-time Alerting | Data Formatting | Data Routing | Data Labeling		

Use Cases, Capabilities and Tools

	IT Operations	Security	DevOps Observability
Automate			
Analyze			
Triage			
Monitor			
Store	Scalable Data Index | Full Fidelity No-Sample Metrics Store | Data Lake		
Collect	Universal Collection | Stream Processing | Real-time Alerting | Data Formatting | Data Routing | Data Labeling		

Use Cases, Capabilities and Tools

	IT Operations	Security	DevOps Observability
Automate			
Analyze			
Triage			
Monitor	Federated Search, Visualization, Reporting, Alerting		
Store	Scalable Data Index | Full Fidelity No-Sample Metrics Store | Data Lake		
Collect	Universal Collection | Stream Processing | Real-time Alerting | Data Formatting | Data Routing | Data Labeling		

Use Cases, Capabilities and Tools

	IT Operations	Security	DevOps Observability
Automate	Predictive ML Auto-Resolve On-Call Notification	SOAR Security Case Management	Self-healing Auto-scaling On-Call Notification
Analyze	Event Management AI Ops	Threat Intel Attack Analysis Risk-Based Alerting	Self-Service Observability Synthetics
Triage	Business Service Mapping KPI Monitoring	SIEM | UEBA Compliance	Infrastructure Monitoring RUM | DEM | APM | AppD
Monitor	Federated Search, Visualization, Reporting, Alerting		
Store	Scalable Data Index | Full Fidelity No-Sample Metrics Store | Data Lake		
Collect	Universal Collection | Stream Processing | Real-time Alerting | Data Formatting | Data Routing | Data Labeling		

Data Literacy

© 2024 SPLUNK LLC

“ The ability to take data –to be able to understand it, to process it, to extract value from it, to visualize it, to communicate it –that’s going to be a hugely important skill in the next decades.”

Hal Varian
Chief Economist at Google

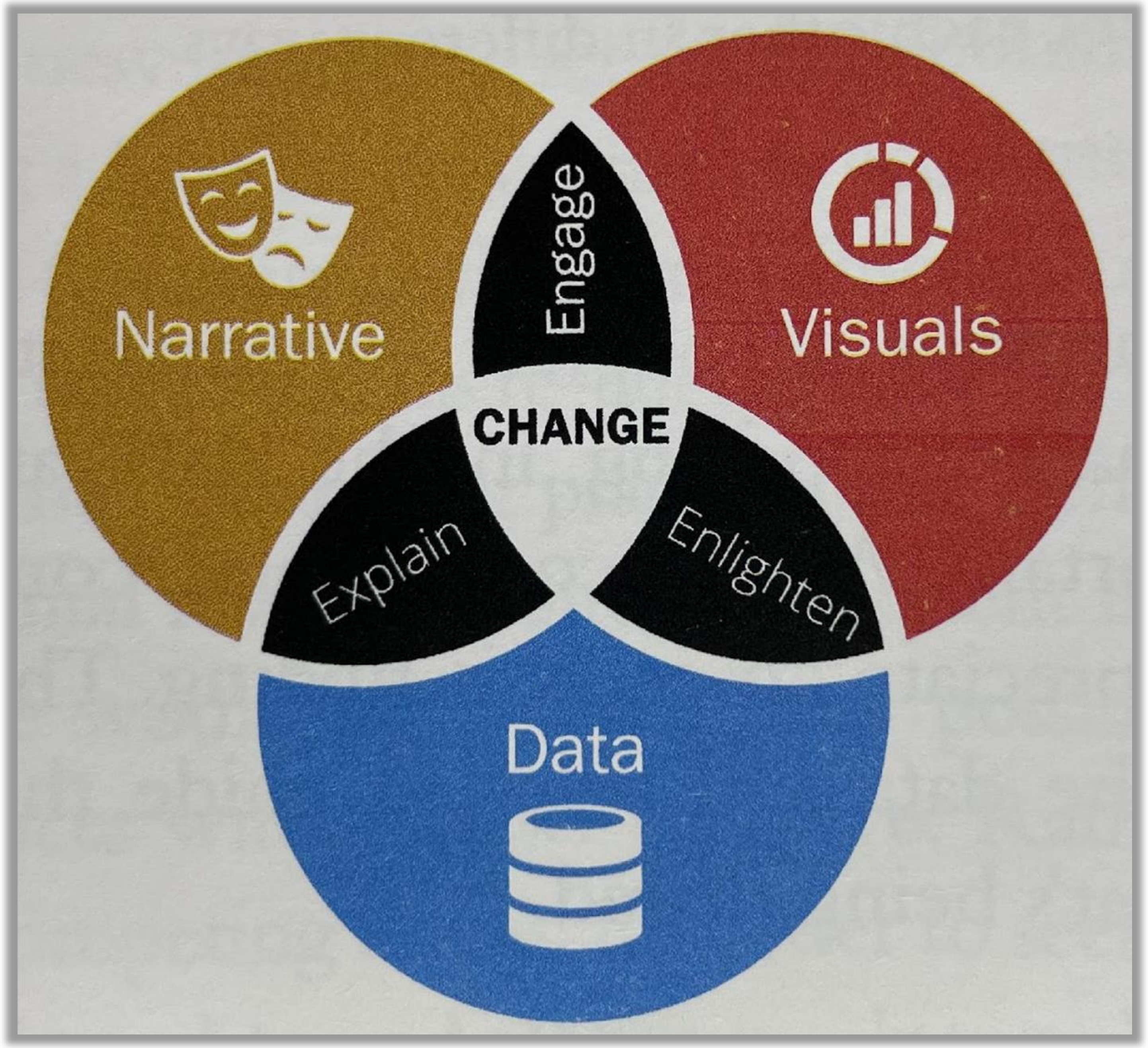
Data Literacy

To read, work with, analyze and communicate with data through storytelling, context and applicability.

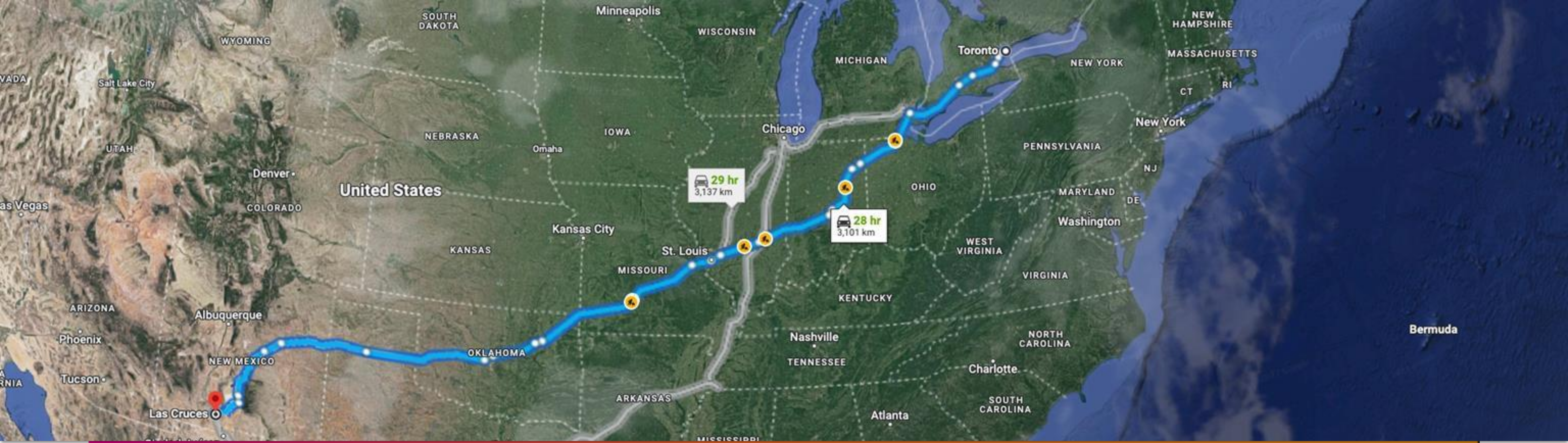
© 2021 SPLUNK INC.

Effective Data Stories Can Drive Change

When you combine the right data with the right narrative and visuals, you have a data story that can drive change.



Effective Data Storytelling, Brent Dykes



A Data Expedition

Charting our course through the three planes of data.

© 2023 SPLUNK INC.

Three Data Planes

Unfolding the layers of the universe (of data)

Signals

A foundation of raw data.

Semantics

The transformation into meaningful insights.

Logic

Generation of actionable insights.

© 2024 SPLUNK INC.

Three Data Planes

Unfolding the layers of the universe (of data)

- Machine data
- Metrics, events, logs, traces (**MELT**)
- Messy
- Not ready for analytics or ML, AI

- Aggregated and cleaned data
- Mapped and compliant (CIM)
- Objects fully mapped to business concepts

- Derived from the semantic layer
- Metrics or facts

© 2024 SPLUNK INC.

	Descriptive Analytics What is happening?	**Diagnostic Analytics** Why is it happening?	**Predictive Analytics** What could happen?	**Prescriptive Analytics** What should we do?
Signals Layer (Data Transmission)	Detecting unusual data movements or spikes in transaction activities.	Pinpointing anomalies in data transmissions that indicate fraud.	Utilizing past data signals to predict future fraud attempts.	Recommending immediate actions based on real-time data signals.
Semantics Layer (Data Interpretation)	Identifying the nature of the data, categorizing it as normal or potential fraud.	Analyzing the root cause of these anomalies – identifying specific fraud tactics.	Interpreting trends and patterns to forecast potential fraud activities.	Suggesting specific responses based on the data interpretation.
Logic Layer (Data Analysis and Decision-Making)	Summarizing current fraud trends based on historical data and recent activities.	Interpreting the reasons behind detected fraud patterns, using data correlations.	Developing strategies for preventing anticipated fraud scenarios.	Formulating comprehensive fraud prevention strategies based on data analysis.

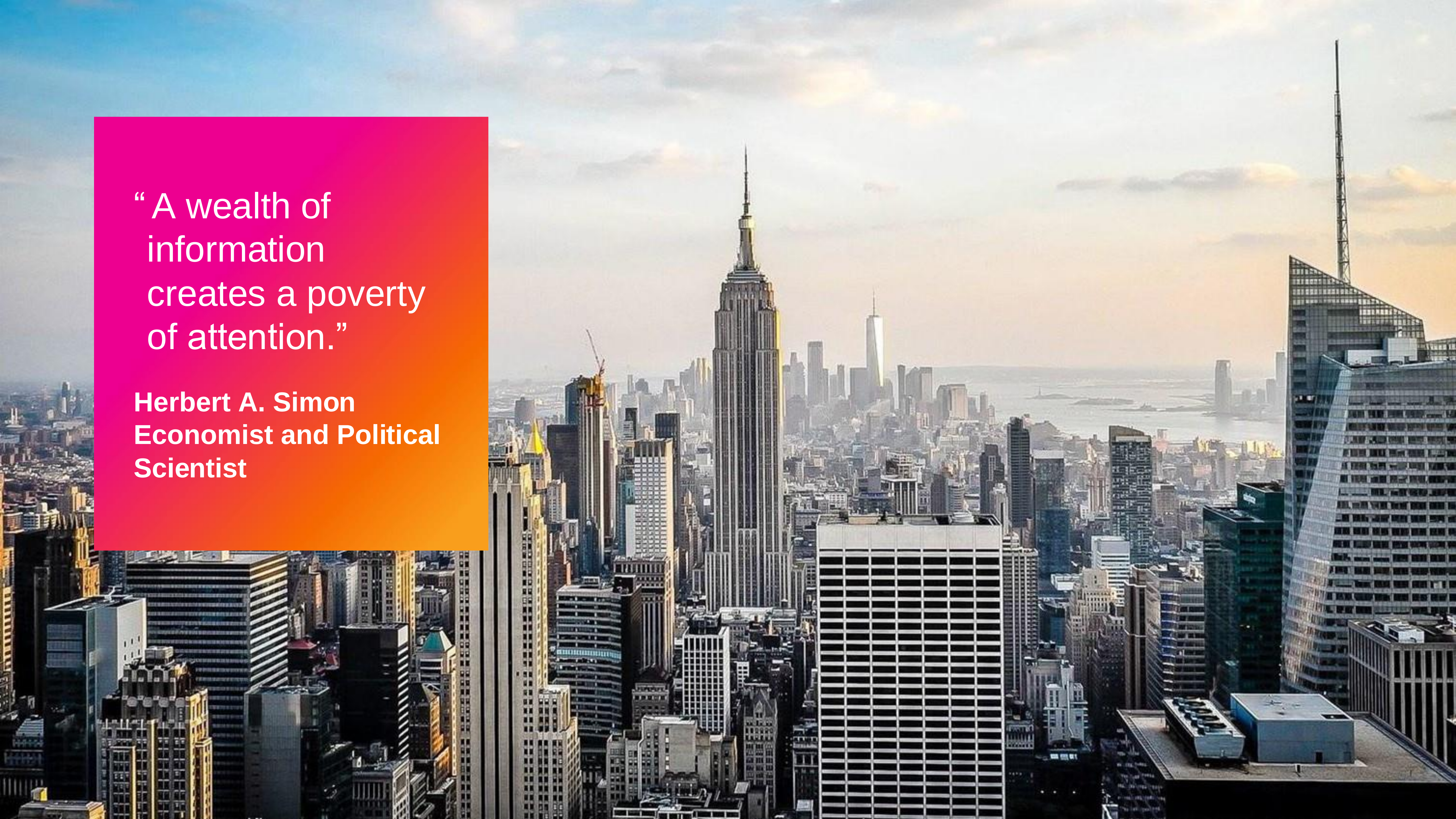
	Descriptive Analytics What is happening?	**Diagnostic Analytics** Why is it happening?	**Predictive Analytics** What could happen?	**Prescriptive Analytics** What should we do?
Signals Layer (Data Transmission)	Detecting unusual data movements or spikes in transaction activities.	Pinpointing anomalies in data transmissions that indicate fraud.	Utilizing past data signals to predict future fraud attempts.	Recommending immediate actions based on real-time data signals.
Semantics Layer (Data Interpretation)	Identifying the nature of the data, categorizing it as normal or potential fraud.	Analyzing the root cause of these anomalies – identifying specific fraud tactics.	Interpreting trends and patterns to forecast potential fraud activities.	Suggesting specific responses based on the data interpretation.
Logic Layer (Data Analysis and Decision-Making)	Summarizing current fraud trends based on historical data and recent activities.	Interpreting the reasons behind detected fraud patterns, using data correlations.	Developing strategies for preventing anticipated fraud scenarios.	Formulating comprehensive fraud prevention strategies based on data analysis.

	Descriptive Analytics What is happening?	**Diagnostic Analytics** Why is it happening?	**Predictive Analytics** What could happen?	**Prescriptive Analytics** What should we do?
Signals Layer (Data Transmission)	Detecting unusual data movements or spikes in transaction activities.	Pinpointing anomalies in data transmissions that indicate fraud.	Utilizing past data signals to predict future fraud attempts.	Recommending immediate actions based on real-time data signals.
Semantics Layer (Data Interpretation)	Identifying the nature of the data, categorizing it as normal or potential fraud.	Analyzing the root cause of these anomalies – identifying specific fraud tactics.	Interpreting trends and patterns to forecast potential fraud activities.	Suggesting specific responses based on the data interpretation.
Logic Layer (Data Analysis and Decision-Making)	Summarizing current fraud trends based on historical data and recent activities.	Interpreting the reasons behind detected fraud patterns, using data correlations.	Developing strategies for preventing anticipated fraud scenarios.	Formulating comprehensive fraud prevention strategies based on data analysis.

	Descriptive Analytics What is happening?	Diagnostic Analytics Why is it happening?	Predictive Analytics What could happen?	Prescriptive Analytics What should we do?
Signals Layer (Data Transmission)	Detecting unusual data movements or spikes in transaction activities.	Pinpointing anomalies in data transmissions that indicate fraud.	Utilizing past data signals to predict future fraud attempts.	Recommending immediate actions based on real-time data signals.
Semantics Layer (Data Interpretation)	Identifying the nature of the data, categorizing it as normal or potential fraud.	Analyzing the root cause of these anomalies – identifying specific fraud tactics.	Interpreting trends and patterns to forecast potential fraud activities.	Suggesting specific responses based on the data interpretation.
Logic Layer (Data Analysis and Decision-Making)	Summarizing current fraud trends based on historical data and recent activities.	Interpreting the reasons behind detected fraud patterns, using data correlations.	Developing strategies for preventing anticipated fraud scenarios.	Formulating comprehensive fraud prevention strategies based on data analysis.

	Descriptive Analytics What is happening?	Diagnostic Analytics Why is it happening?	Predictive Analytics What could happen?	Prescriptive Analytics What should we do?
Signals Layer (Data Transmission)	Detecting unusual data movements or spikes in transaction activities.	Pinpointing anomalies in data transmissions that indicate fraud.	Utilizing past data signals to predict future fraud attempts.	Recommending immediate actions based on real-time data signals.
Semantics Layer (Data Interpretation)	Identifying the nature of the data, categorizing it as normal or potential fraud.	Analyzing the root cause of these anomalies – identifying specific fraud tactics.	Interpreting trends and patterns to forecast potential fraud activities.	Suggesting specific responses based on the data interpretation.
Logic Layer (Data Analysis and Decision-Making)	Summarizing current fraud trends based on historical data and recent activities.	Interpreting the reasons behind detected fraud patterns, using data correlations.	Developing strategies for preventing anticipated fraud scenarios.	Formulating comprehensive fraud prevention strategies based on data analysis.

	Descriptive Analytics What is happening?	Diagnostic Analytics Why is it happening?	Predictive Analytics What could happen?	Prescriptive Analytics What should we do?
Signals Layer (Data Transmission)	Detecting unusual data movements or spikes in transaction activities.	Pinpointing anomalies in data transmissions that indicate fraud.	Utilizing past data signals to predict future fraud attempts.	Recommending immediate actions based on real-time data signals.
Semantics Layer (Data Interpretation)	Identifying the nature of the data, categorizing it as normal or potential fraud.	Analyzing the root cause of these anomalies – identifying specific fraud tactics.	Interpreting trends and patterns to forecast potential fraud activities.	Suggesting specific responses based on the data interpretation.
Logic Layer (Data Analysis and Decision-Making)	Summarizing current fraud trends based on historical data and recent activities.	Interpreting the reasons behind detected fraud patterns, using data correlations.	Developing strategies for preventing anticipated fraud scenarios.	Formulating comprehensive fraud prevention strategies based on data analysis.



> “ A wealth of information creates a poverty of attention.”

Herbert A. Simon
Economist and Political Scientist

Thank You

Fraud Analytics

© 2024 SPLUNK INC.

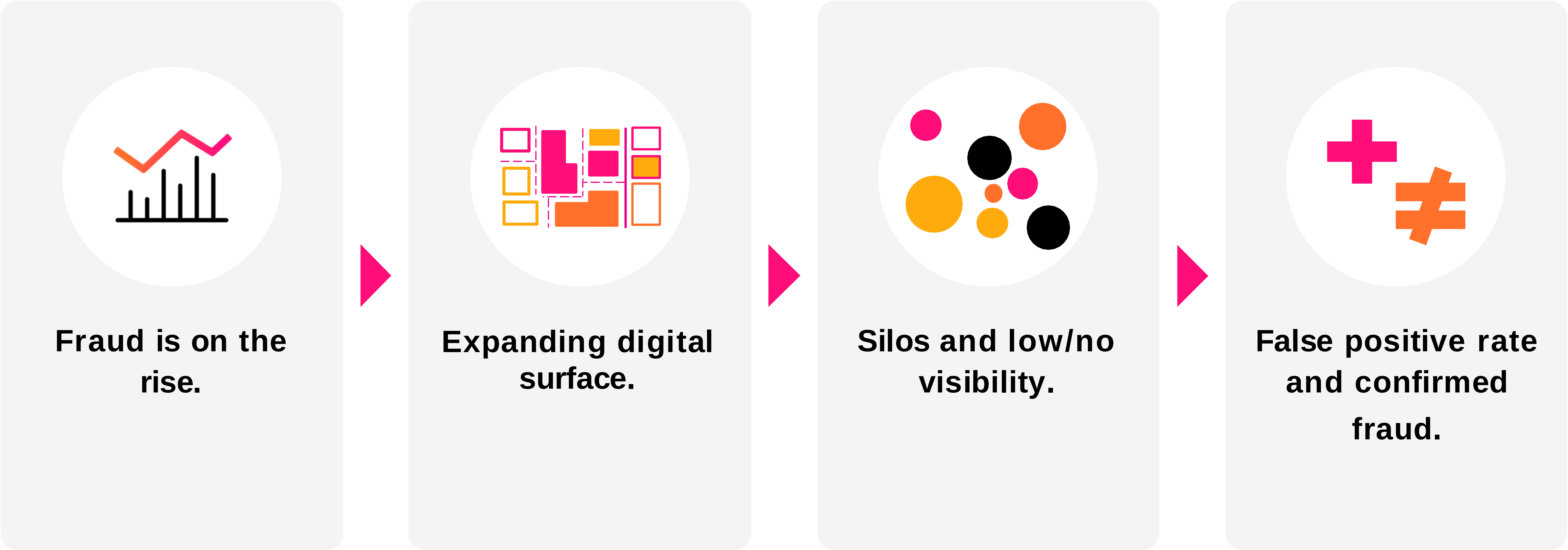
“Both improper payments and fraud result in significant financial and nonfinancial impacts to the integrity of programs. They erode public trust in government, waste taxpayer dollars, and hinder agencies’ efforts to execute their missions and program objectives effectively and efficiently.”

U.S. Government Accountability Office

Improper Payments and Fraud: How They are Related but Different

Challenges in Detecting Fraud

The size and complexity of the landscape is increasing



Fraud is on the rise.

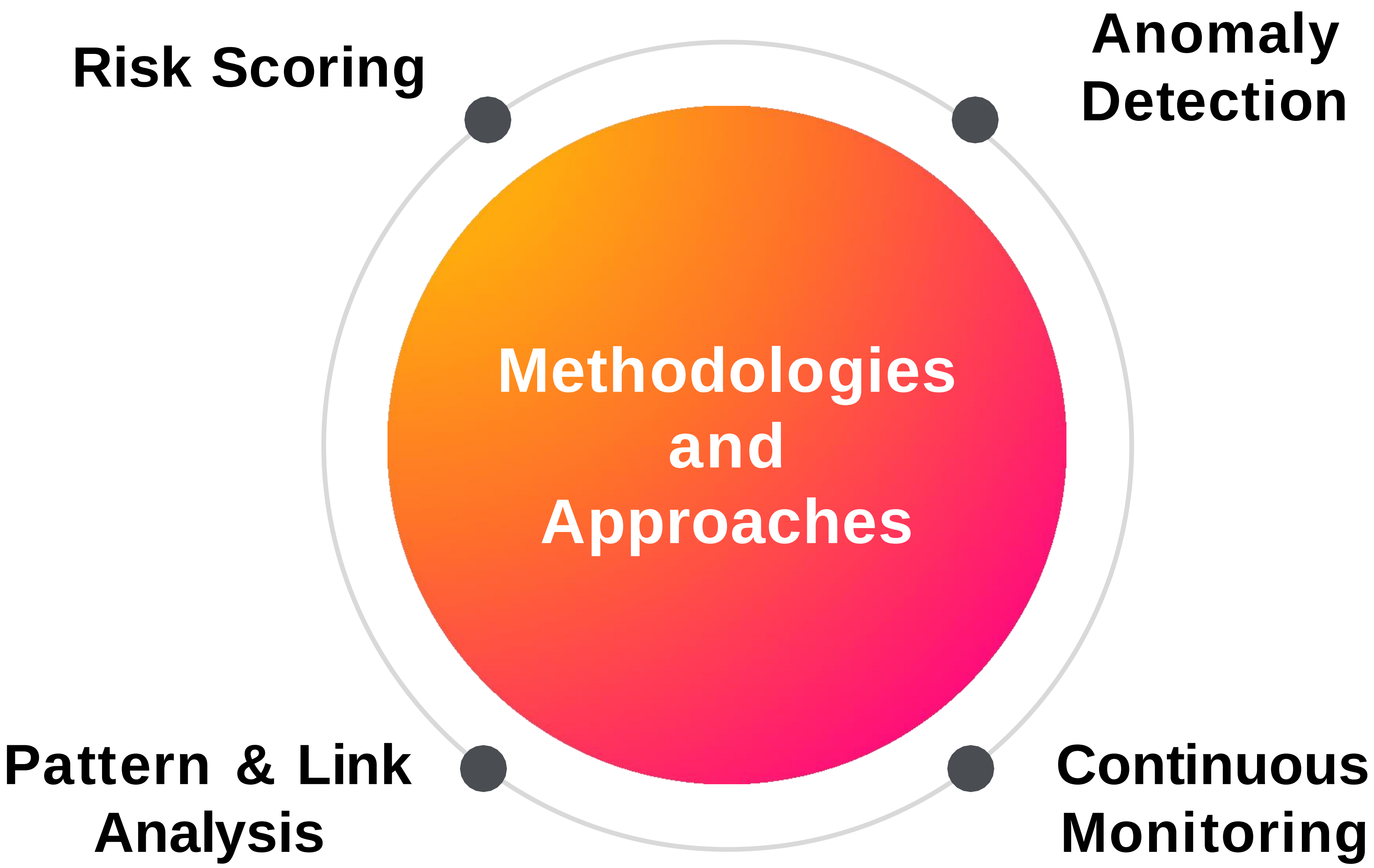
Expanding digital surface.

Silos and low/no visibility.

False positive rate and confirmed fraud.

© 2024 SPLUNK INC.

Fraud Use Case



Risk Scoring

Anomaly Detection

Methodologies and Approaches

Pattern & Link Analysis

Continuous Monitoring

© 2024 SPLUNK INC.

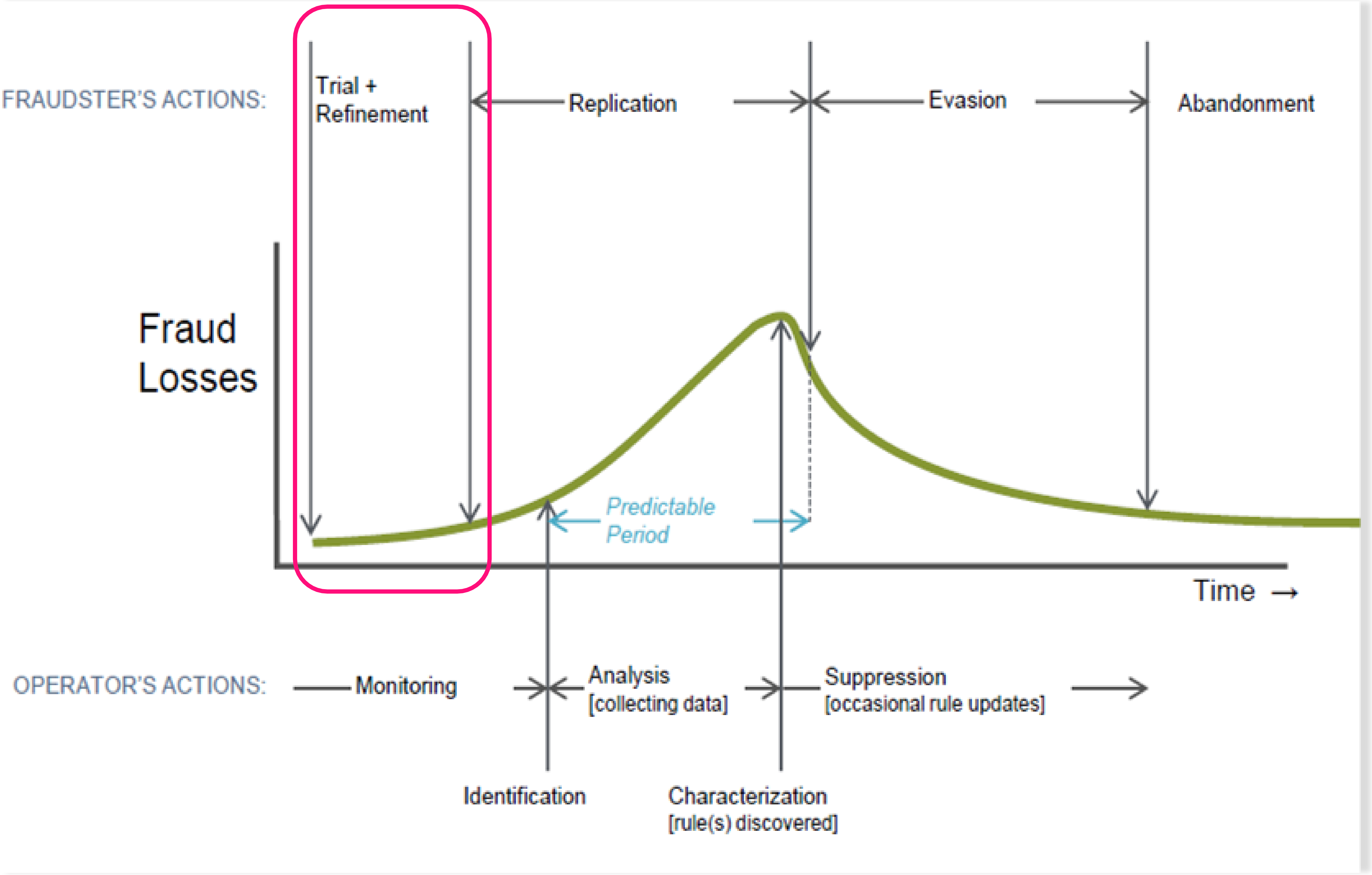
Centralized access to data such that monitoring, detection, investigations, reporting, and integration of learned insights are made actionable.

Monitor activity in the Trial + Refinement phase.

Monitor the identity of the user and machine.

&

Monitor the behavior of the user and the machine.



splunk>

© 2024 SPLUNK INC.

DOL

THE NEW JERSEY DEPARTMENT OF LABOR & WORKFORCE DEVELOPMENT

Fraud Actor Group	Primary Motivations	Typical Tactics	Behavior Patterns	Scale of Operations	Detection Difficulty	Impact
Individual Fraud Actors	Financial hardship / desperation, opportunity	Simple deception, basic identity theft	Impulsive, opportunistic, low/no OpSec	Small-scale, isolated incidents	Relatively easier to detect	Individually low, collectively significant
Opportunists	Exploiting weaknesses, financial need	Capitalizing on chaotic situations, identity theft, social engineering	Situational, reactionary, organized processes (patternistic)	Varies, often situation-specific	Varies from easy to moderately difficult to detect	Significant during vulnerable times, creates stress on the system
Organized Crime	Financial profit, funding illegal activities	Sophisticated schemes, money laundering, mule networks, bots	Highly organized, methodical, low n slow	Large-scale, international	High difficulty	Potentially massive, disruptive
Nation-State Actors	Financial profit, geopolitical influence, intelligence gathering	Advanced cyber operations, espionage	Strategic, long-term focus	Extensive, state-backed	Very high difficulty	Far-reaching, affects national security

© 2024 SPLUNK INC.

Fraud Actor Group	Primary Motivations	Typical Tactics	Behavior Patterns	Scale of Operations	Detection Difficulty	Impact
Individual Fraud Actors	Financial hardship / desperation, opportunity	Simple deception, basic identity theft	Impulsive, opportunistic, low/no OpSec	Small-scale, isolated incidents	Relatively easier to detect	**Individually low, collectively significant**
Opportunists	Exploiting weaknesses, financial need	Capitalizing on chaotic situations, identity theft, social engineering	Situational, reactionary, organized processes (patternistic)	Varies, often situation-specific	Varies from easy to moderately difficult to detect	**Significant during vulnerable times, creates stress on the system**
Organized Crime	Financial profit, funding illegal activities	Sophisticated schemes, money laundering, mule networks, bots	Highly organized, methodical, low n slow	Large-scale, international	High difficulty	Potentially massive, disruptive
Nation-State Actors	Financial profit, geopolitical influence, intelligence gathering	Advanced cyber operations, espionage	Strategic, long-term focus	Extensive, state-backed	Very high difficulty	Far-reaching, affects national security

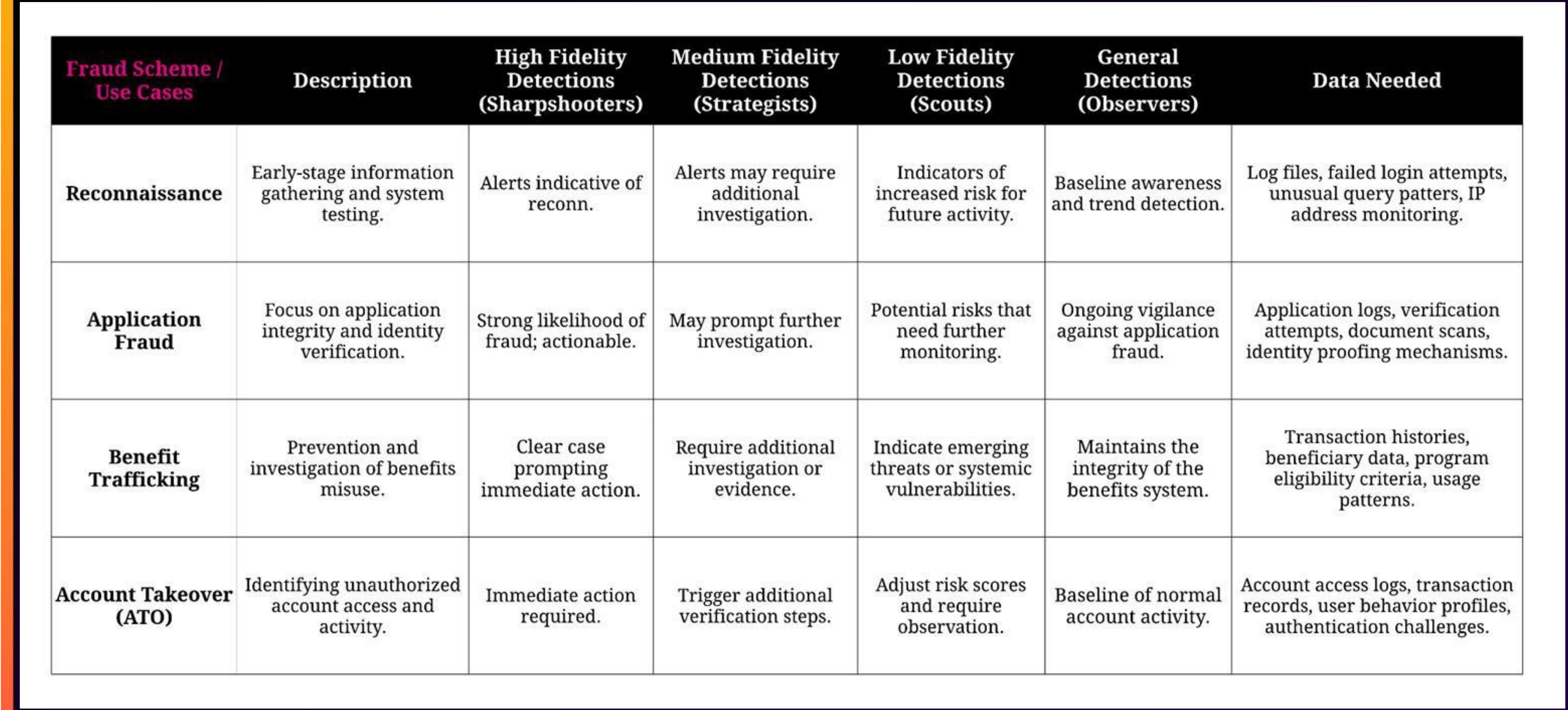
© 2024 SPLUNK INC.

Fraud Actor Group	Primary Motivations	Typical Tactics	Behavior Patterns	Scale of Operations	Detection Difficulty	Impact
Individual Fraud Actors	Financial hardship / desperation, opportunity	Simple deception, basic identity theft	Impulsive, opportunistic, low/no OpSec	Small-scale, isolated incidents	Relatively easier to detect	Individually low, collectively significant
Opportunists	Exploiting weaknesses, financial need	Capitalizing on chaotic situations, identity theft, social engineering	Situational, reactionary, organized processes (patternistic)	Varies, often situation-specific	Varies from easy to moderately difficult to detect	Significant during vulnerable times, creates stress on the system
Organized Crime	**Financial profit, funding illegal activities**	Sophisticated schemes, money laundering, mule networks, bots	Highly organized, methodical, low n slow	Large-scale, international	**High difficulty**	**Potentially massive, disruptive**
Nation-State Actors	**Financial profit, geopolitical influence, intelligence gathering**	Advanced cyber operations, espionage	Strategic, long-term focus	Extensive, state-backed	**Very high difficulty**	**Far-reaching, affects national security**

© 2024 SPLUNK INC.

Fraud Actor Group	Primary Motivations	Typical Tactics	Behavior Patterns	Scale of Operations	Detection Difficulty	Impact
Individual Fraud Actors	Financial hardship / desperation, opportunity	Simple deception, basic identity theft	Impulsive, opportunistic, low/no OpSec	Small-scale, isolated incidents	Relatively easier to detect	Individually low, collectively significant
Opportunists	Exploiting weaknesses, financial need	Capitalizing on chaotic situations, identity theft, social engineering	Situational, reactionary, organized processes (patternistic)	Varies, often situation-specific	Varies from easy to moderately difficult to detect	Significant during vulnerable times, creates stress on the system
Organized Crime	Financial profit, funding illegal activities	Sophisticated schemes, money laundering, mule networks, bots	Highly organized, methodical, low n slow	Large-scale, international	High difficulty	Potentially massive, disruptive
Nation-State Actors	Financial profit, geopolitical influence, intelligence gathering	Advanced cyber operations, espionage	Strategic, long-term focus	Extensive, state-backed	Very high difficulty	Far-reaching, affects national security

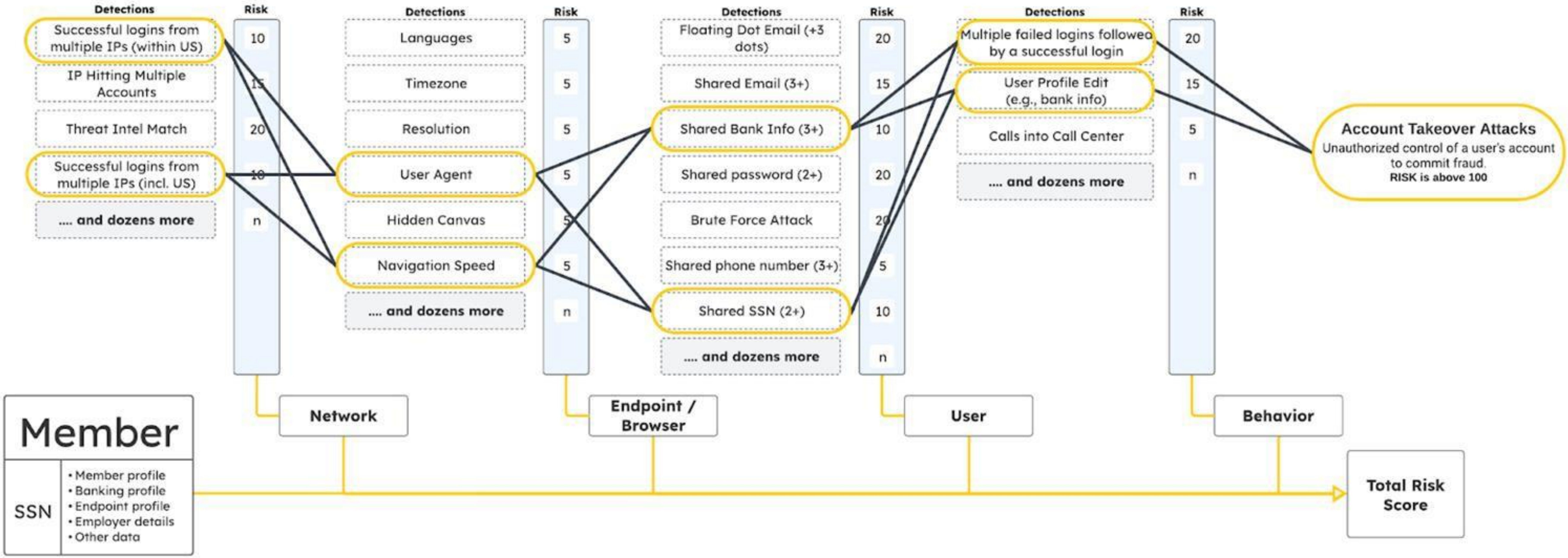
© 2024 SPLUNK INC.



Fraud Scheme / Use Cases	Description	High Fidelity Detections (Sharpshooters)	Medium Fidelity Detections (Strategists)	Low Fidelity Detections (Scouts)	General Detections (Observers)	Data Needed
Reconnaissance	Early-stage information gathering and system testing.	Alerts indicative of reconn.	Alerts may require additional investigation.	Indicators of increased risk for future activity.	Baseline awareness and trend detection.	Log files, failed login attempts, unusual query patters, IP address monitoring.
Application Fraud	Focus on application integrity and identity verification.	Strong likelihood of fraud; actionable.	May prompt further investigation.	Potential risks that need further monitoring.	Ongoing vigilance against application fraud.	Application logs, verification attempts, document scans, identity proofing mechanisms.
Benefit Trafficking	Prevention and investigation of benefits misuse.	Clear case prompting immediate action.	Require additional investigation or evidence.	Indicate emerging threats or systemic vulnerabilities.	Maintains the integrity of the benefits system.	Transaction histories, beneficiary data, program eligibility criteria, usage patterns.
Account Takeover (ATO)	Identifying unauthorized account access and activity.	Immediate action required.	Trigger additional verification steps.	Adjust risk scores and require observation.	Baseline of normal account activity.	Account access logs, transaction records, user behavior profiles, authentication challenges.

© 2024 SPLUNK INC.

Fraud Attack: ATO (account takeover)



Network

Detections	Risk
Successful logins from multiple IPs (within US)	10
IP Hitting Multiple Accounts	15
Threat Intel Match	20
Successful logins from multiple IPs (incl. US)	10
.... and dozens more	n

Endpoint / Browser

Detections	Risk
Languages	5
Timezone	5
Resolution	5
User Agent	5
Hidden Canvas	5
Navigation Speed	5
.... and dozens more	n

User

Detections	Risk
Floating Dot Email (+3 dots)	20
Shared Email (3+)	15
Shared Bank Info (3+)	10
Shared password (2+)	20
Brute Force Attack	20
Shared phone number (3+)	5
Shared SSN (2+)	10
.... and dozens more	n

Behavior

Detections	Risk
Multiple failed logins followed by a successful login	20
User Profile Edit (e.g., bank info)	15
Calls into Call Center	5
.... and dozens more	n

Account Takeover Attacks
Unauthorized control of a user's account to commit fraud.
RISK is above 100

Member

SSN

- Member profile
- Banking profile
- Endpoint profile
- Employer details
- Other data

Total Risk Score

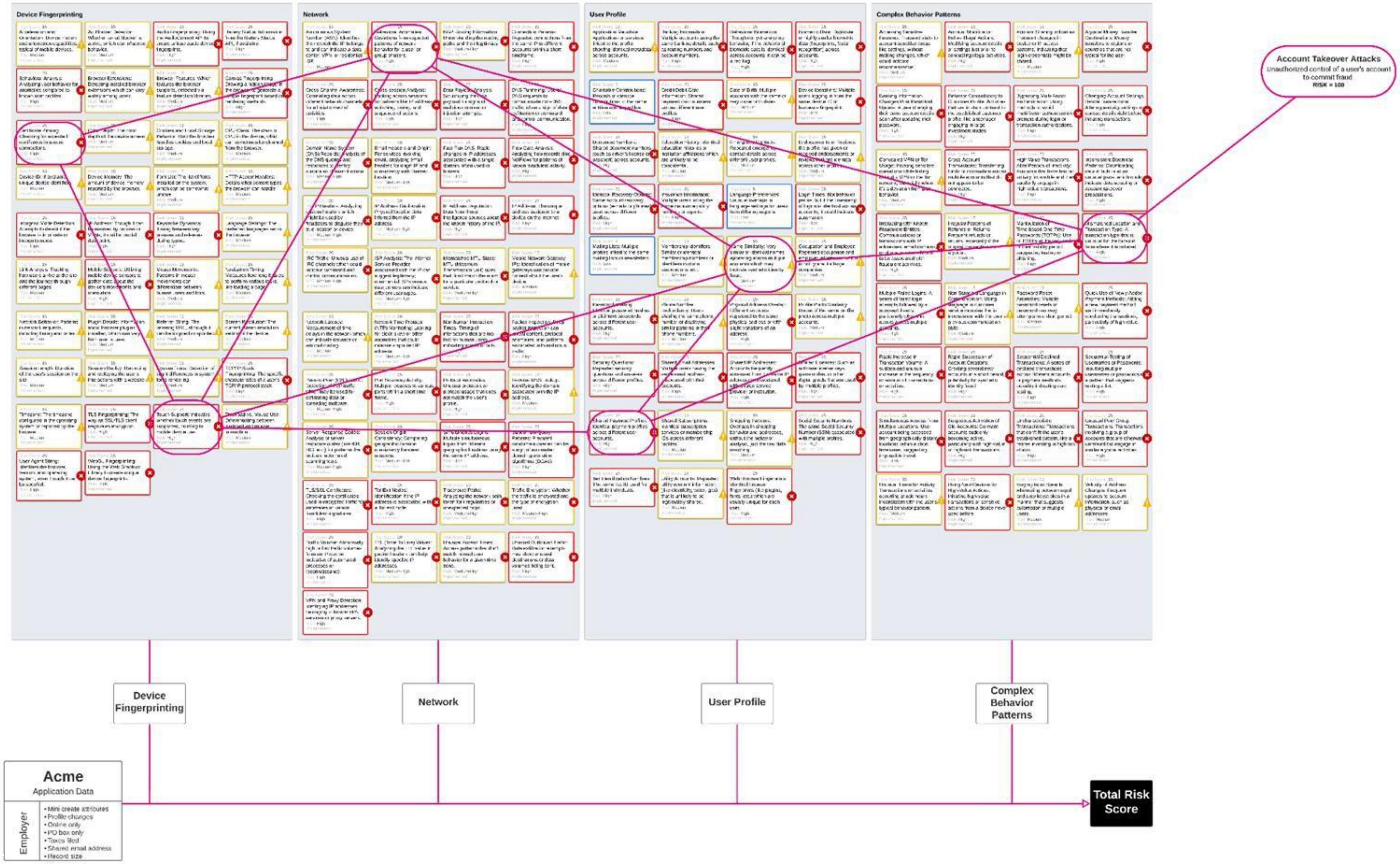
© 2024 SPLUNK INC.

Applied Analytics for Anomaly Detection and Fraud Prevention

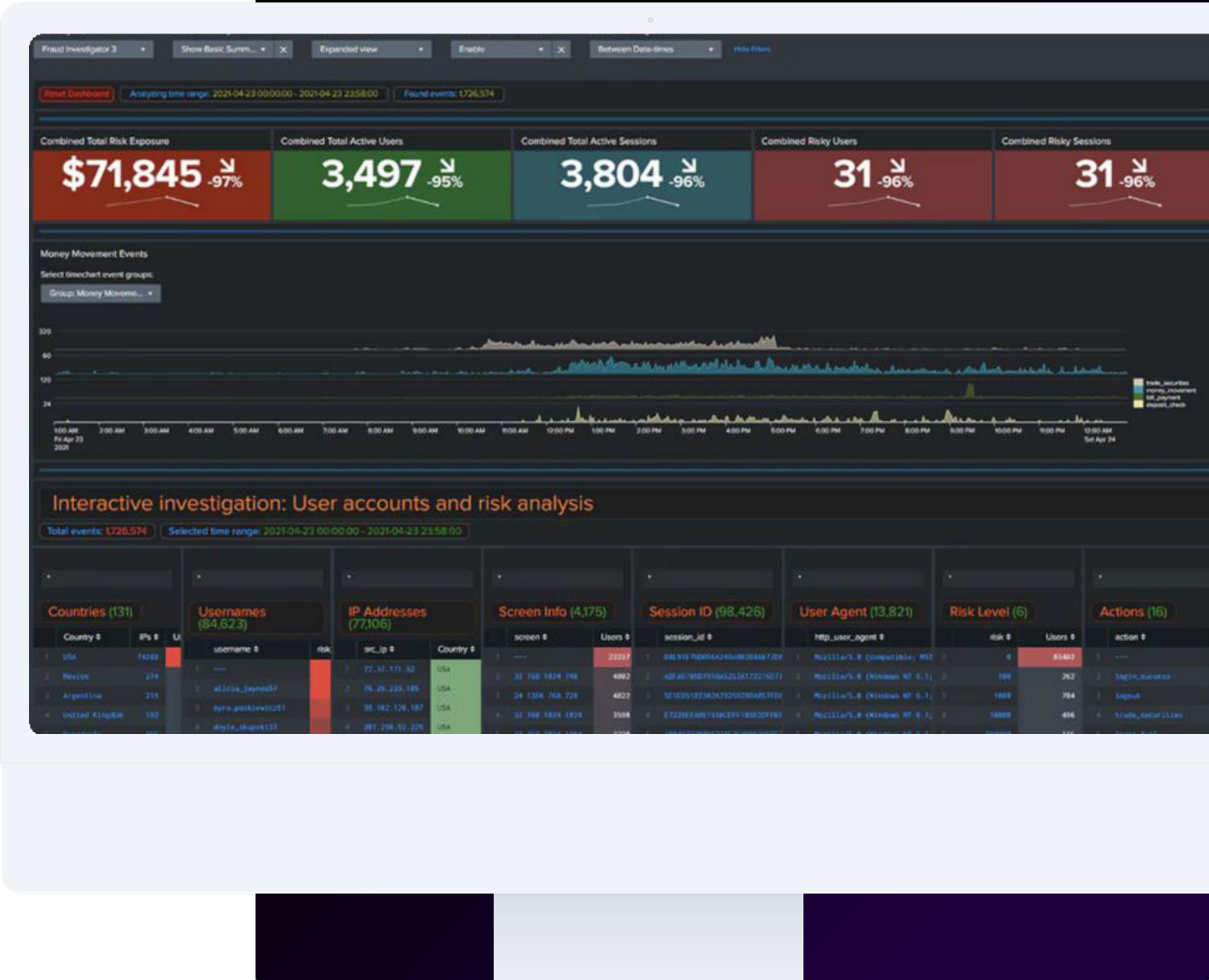
Updated: November 6th, 2023

Updated/Reviewed by: Chris Perkins (Splunk)

Fraud detection mechanisms using metadata and data analytics.



Splunk App for Fraud Analytics



Fraud Investigator 3 | Show Basic Summ... | Expanded view | Enable | Between Date-times | Hide Filters

Reset Dashboard | Analyzing time range: 2021-04-23 00:00:00 - 2021-04-23 23:58:00 | Found events: 1,726,574

Combined Total Risk Exposure	Combined Total Active Users	Combined Total Active Sessions	Combined Risky Users	Combined Risky Sessions
$71,845 -97%	3,497 -95%	3,804 -96%	31 -96%	31 -96%

Money Movement Events

Select timechart event groups:

Group: Money Moveme...

Interactive investigation: User accounts and risk analysis

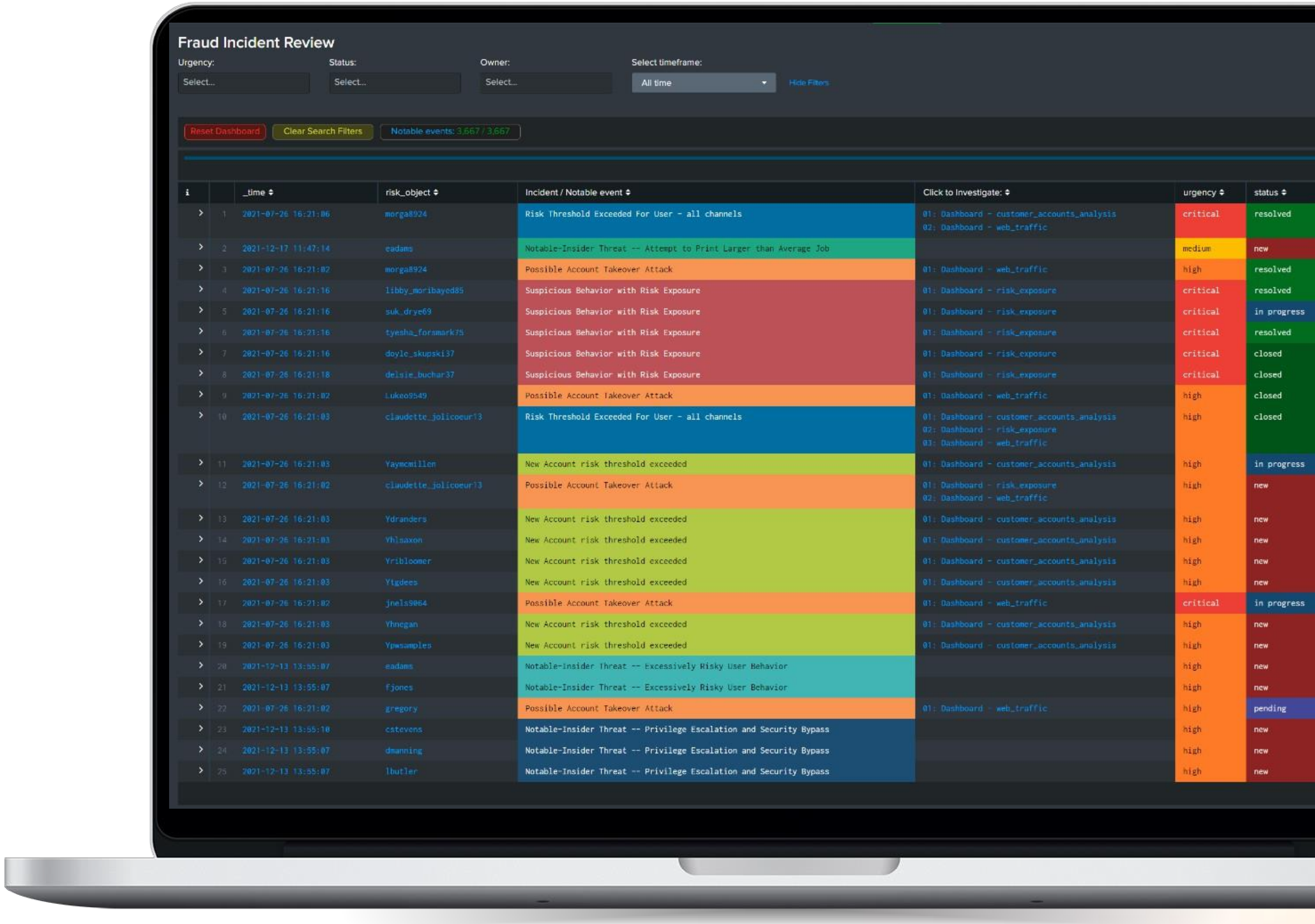
Total events: 1,726,574 | Selected time range: 2021-04-23 00:00:00 - 2021-04-23 23:58:00

Countries (131) | Usernames (84,623) | IP Addresses (77,106) | Screen Info (4,175) | Session ID (98,426) | User Agent (13,821) | Risk Level (6) | Actions (16)

Fraud Incident Review

In Depth Incident Analysis

- Summarizes all triggered alerts (notable events) with key actionable data points
- Shortcuts directly to relevant investigation dashboards are included within each alert.
- Preview risk contributors for each alert to improve efficiency of investigation
- Better organize investigations
- Track fraud over time
- Facilitate discovery of correlation and causation



Fraud Incident Review

Urgency: Select...

Status: Select...

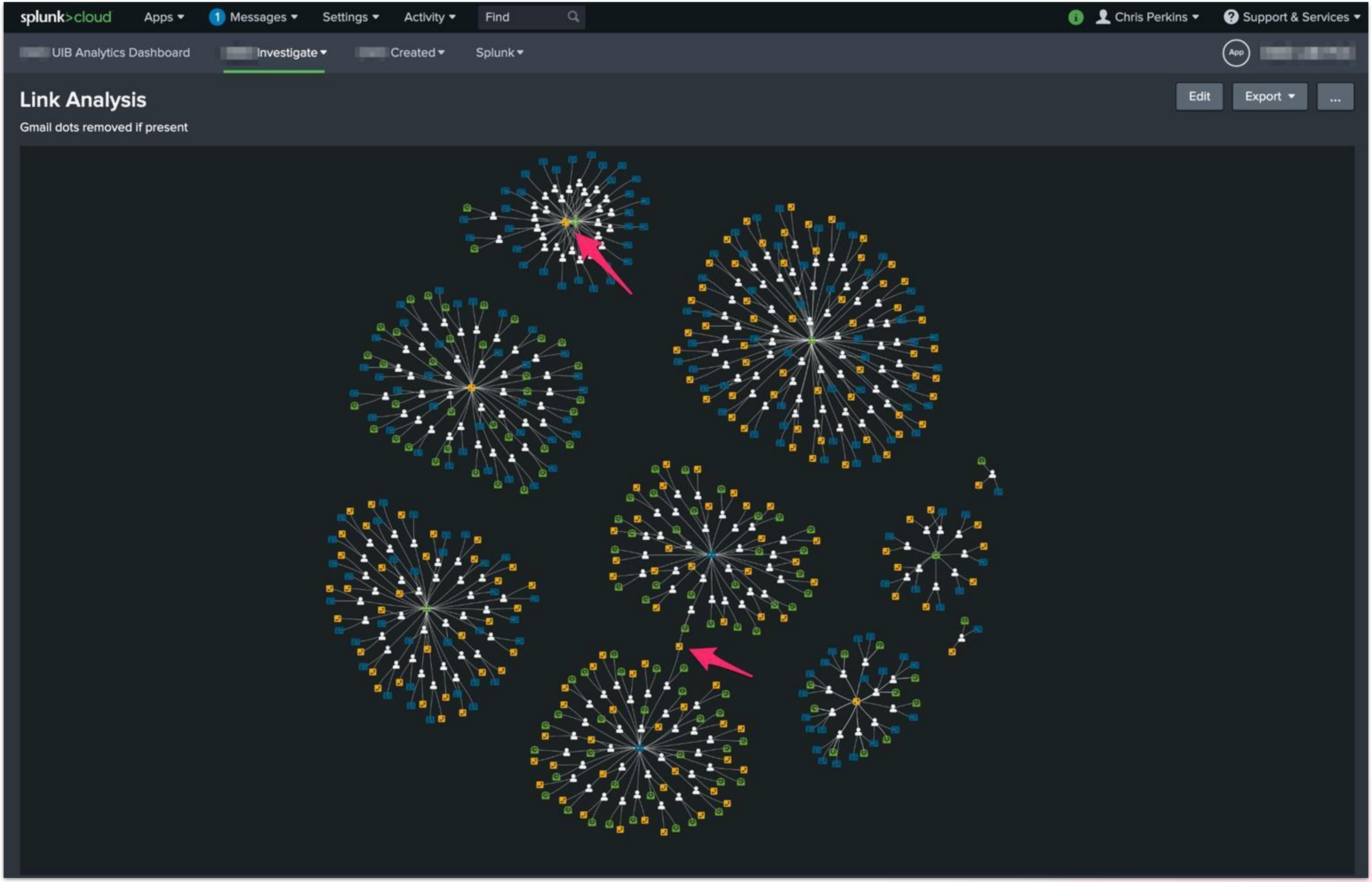
Owner: Select...

Select timeframe: All time

Notable events: 3,667 / 3,667

i		_time ⇕	risk_object ⇕	Incident / Notable event ⇕	Click to Investigate: ⇕	urgency ⇕	status ⇕
>	1	2021-07-26 16:21:06	morga8924	Risk Threshold Exceeded For User - all channels	01: Dashboard - customer_accounts_analysis 02: Dashboard - web_traffic	critical	resolved
>	2	2021-12-17 11:47:14	eadams	Notable-Insider Threat -- Attempt to Print Larger than Average Job		medium	new
>	3	2021-07-26 16:21:02	morga8924	Possible Account Takeover Attack	01: Dashboard - web_traffic	high	resolved
>	4	2021-07-26 16:21:16	libby_moribayed85	Suspicious Behavior with Risk Exposure	01: Dashboard - risk_exposure	critical	resolved
>	5	2021-07-26 16:21:16	suk_drye69	Suspicious Behavior with Risk Exposure	01: Dashboard - risk_exposure	critical	in progress
>	6	2021-07-26 16:21:16	tyesha_forsmark75	Suspicious Behavior with Risk Exposure	01: Dashboard - risk_exposure	critical	resolved
>	7	2021-07-26 16:21:16	doyle_skupski37	Suspicious Behavior with Risk Exposure	01: Dashboard - risk_exposure	critical	closed
>	8	2021-07-26 16:21:18	delsie_buchar37	Suspicious Behavior with Risk Exposure	01: Dashboard - risk_exposure	critical	closed
>	9	2021-07-26 16:21:02	Lukeo9549	Possible Account Takeover Attack	01: Dashboard - web_traffic	high	closed
>	10	2021-07-26 16:21:03	claudette_jolicoeur13	Risk Threshold Exceeded For User - all channels	01: Dashboard - customer_accounts_analysis 02: Dashboard - risk_exposure 03: Dashboard - web_traffic	high	closed
>	11	2021-07-26 16:21:03	Yaymcmillen	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	in progress
>	12	2021-07-26 16:21:02	claudette_jolicoeur13	Possible Account Takeover Attack	01: Dashboard - risk_exposure 02: Dashboard - web_traffic	high	new
>	13	2021-07-26 16:21:03	Ydranders	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	new
>	14	2021-07-26 16:21:03	Yhlsaxon	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	new
>	15	2021-07-26 16:21:03	Yribloomer	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	new
>	16	2021-07-26 16:21:03	Ytgdees	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	new
>	17	2021-07-26 16:21:02	jnels9064	Possible Account Takeover Attack	01: Dashboard - web_traffic	critical	in progress
>	18	2021-07-26 16:21:03	Yhnegan	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	new
>	19	2021-07-26 16:21:03	Ypwsamples	New Account risk threshold exceeded	01: Dashboard - customer_accounts_analysis	high	new
>	20	2021-12-13 13:55:07	eadams	Notable-Insider Threat -- Excessively Risky User Behavior		high	new
>	21	2021-12-13 13:55:07	fjones	Notable-Insider Threat -- Excessively Risky User Behavior		high	new
>	22	2021-07-26 16:21:02	gregory	Possible Account Takeover Attack	01: Dashboard - web_traffic	high	pending
>	23	2021-12-13 13:55:10	cstevens	Notable-Insider Threat -- Privilege Escalation and Security Bypass		high	new
>	24	2021-12-13 13:55:07	dmanning	Notable-Insider Threat -- Privilege Escalation and Security Bypass		high	new
>	25	2021-12-13 13:55:07	lbutler	Notable-Insider Threat -- Privilege Escalation and Security Bypass		high	new

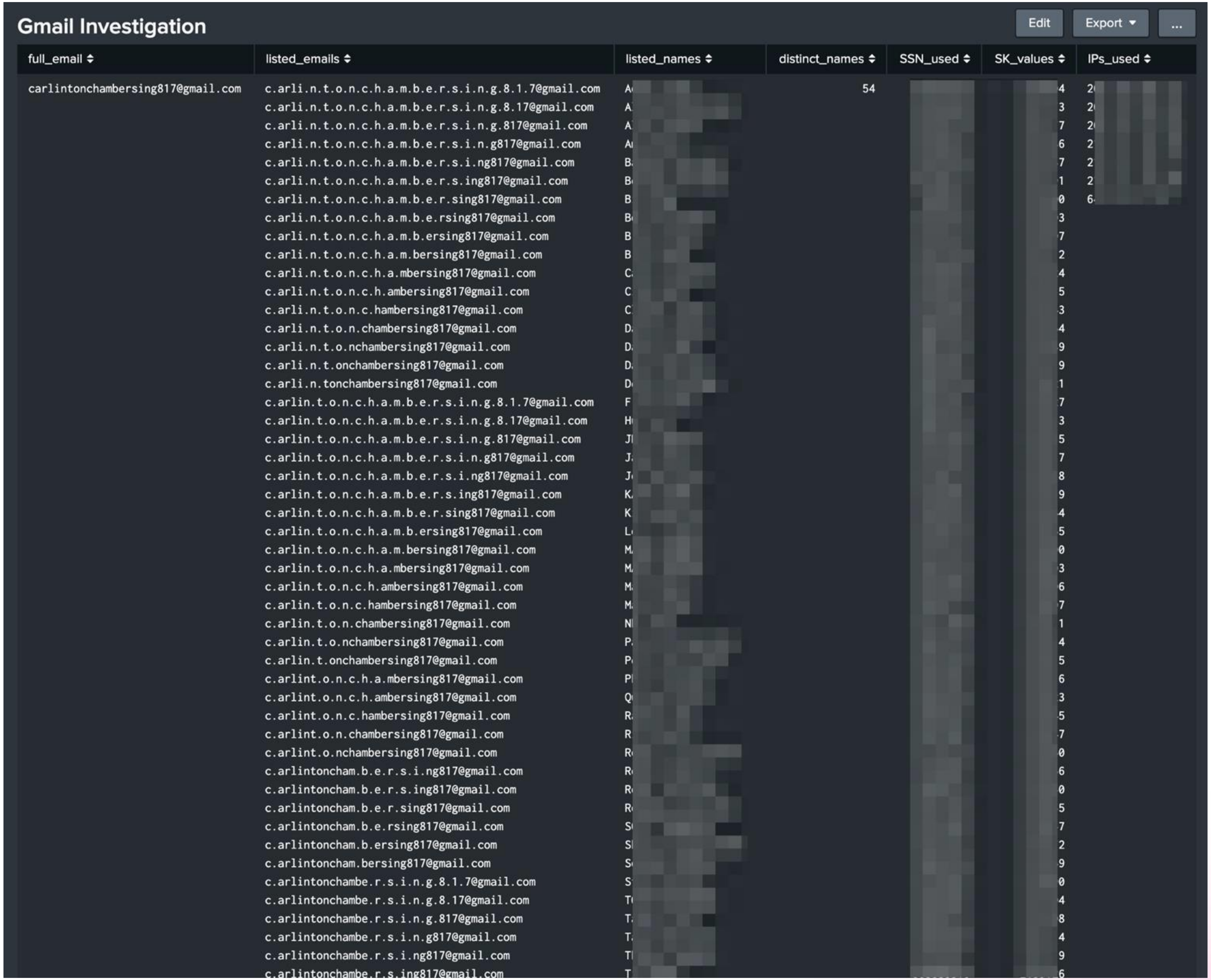
© 2024 SPLUNK INC.



Link Analysis

Gmail dots removed if present

© 2024 SPLUNK INC.

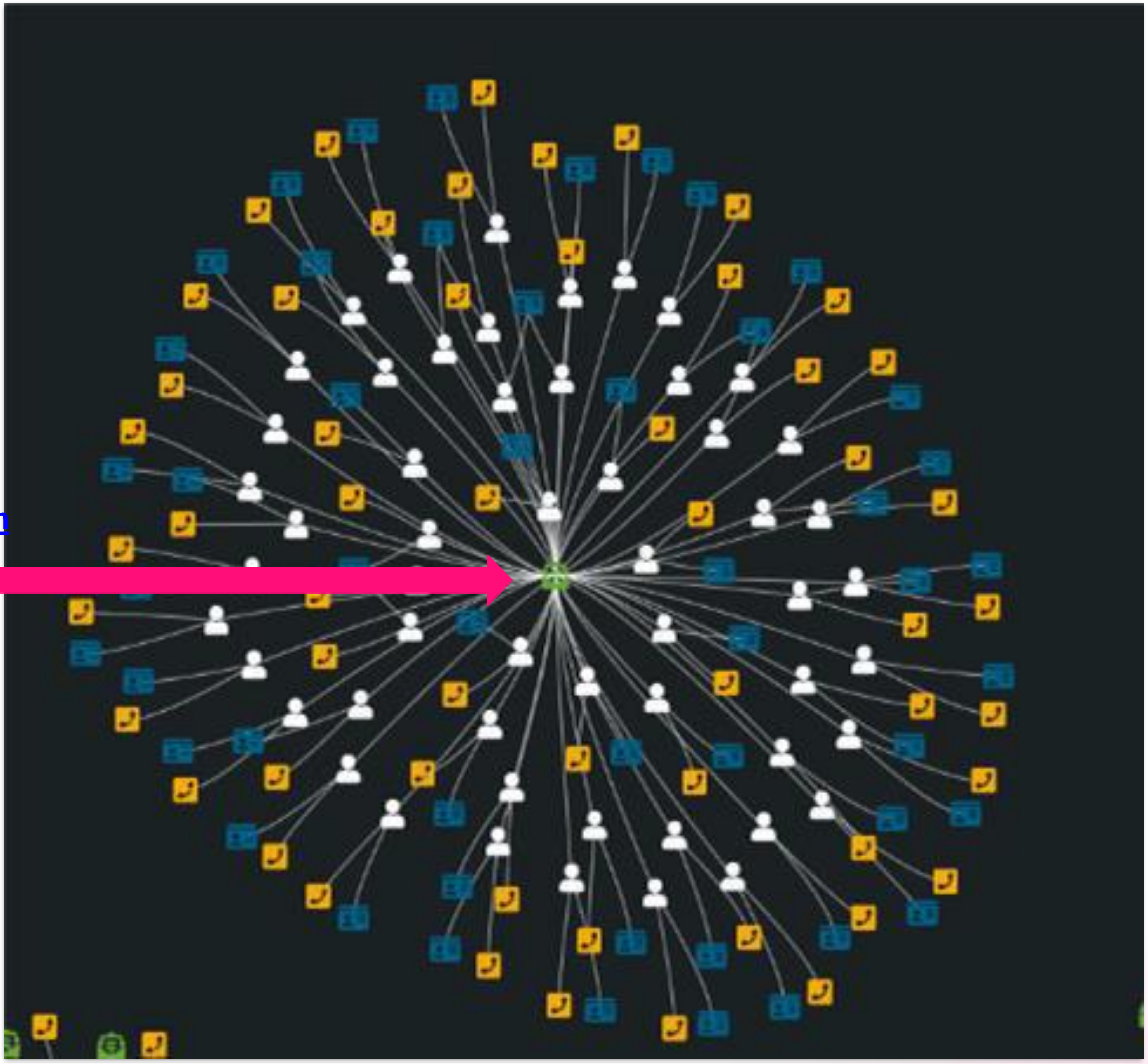


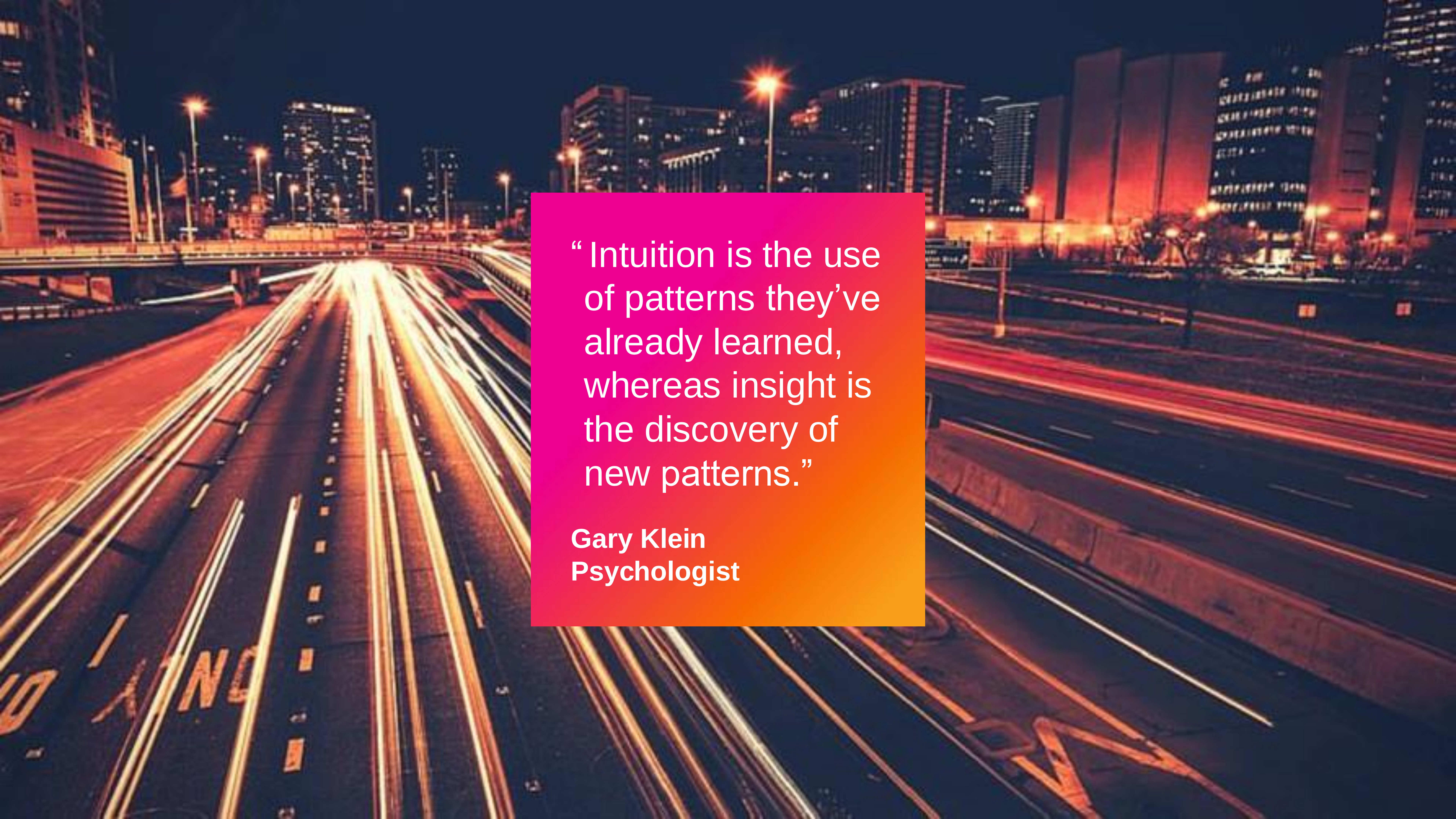
Gmail Investigation

full_email	listed_emails	listed_names	distinct_names	SSN_used	SK_values	IPs_used
carlintonchambersing817@gmail.com	c.arli.n.t.o.n.c.h.a.m.b.e.r.s.i.n.g.8.1.7@gmail.com	[redacted]	54	[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.r.s.i.n.g.8.17@gmail.com	[redacted]		[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.r.s.i.n.g.817@gmail.com	[redacted]		[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.r.s.i.n.g817@gmail.com	[redacted]		[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.r.s.i.ng817@gmail.com	[redacted]		[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.r.s.ing817@gmail.com	[redacted]		[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.r.sing817@gmail.com	[redacted]		[redacted]	[redacted]	[redacted]
	c.arli.n.t.o.n.c.h.a.m.b.e.rsing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.n.c.h.a.m.b.ersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.n.c.h.a.m.bersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.n.c.h.a.mbersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.n.c.h.ambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.n.c.hambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.n.chambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.o.nchambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.t.onchambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arli.n.tonchambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.s.i.n.g.8.1.7@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.s.i.n.g.8.17@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.s.i.n.g.817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.s.i.n.g817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.s.i.ng817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.s.ing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.e.r.sing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.b.ersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.m.bersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.a.mbersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.h.ambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.c.hambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.n.chambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.o.nchambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlin.t.onchambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlint.o.n.c.h.a.mbersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlint.o.n.c.h.ambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlint.o.n.c.hambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlint.o.n.chambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlint.o.nchambersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintoncham.b.e.r.s.i.ng817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintoncham.b.e.r.s.ing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintoncham.b.e.r.sing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintoncham.b.e.rsing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintoncham.b.ersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintoncham.bersing817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintonchambe.r.s.i.n.g.8.1.7@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintonchambe.r.s.i.n.g.8.17@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintonchambe.r.s.i.n.g.817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintonchambe.r.s.i.n.g817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintonchambe.r.s.i.ng817@gmail.com	[redacted]		[redacted]	[redacted]	
	c.arlintonchambe.r.s.ing817@gmail.com	[redacted]		[redacted]	[redacted]	

© 2024 SPLUNK INC.

Carlingtonchambersing187@gmail.com





> “ Intuition is the use of patterns they’ve already learned, whereas insight is the discovery of new patterns.”

Gary Klein
Psychologist

The mechanics of fraud prevention using Splunk

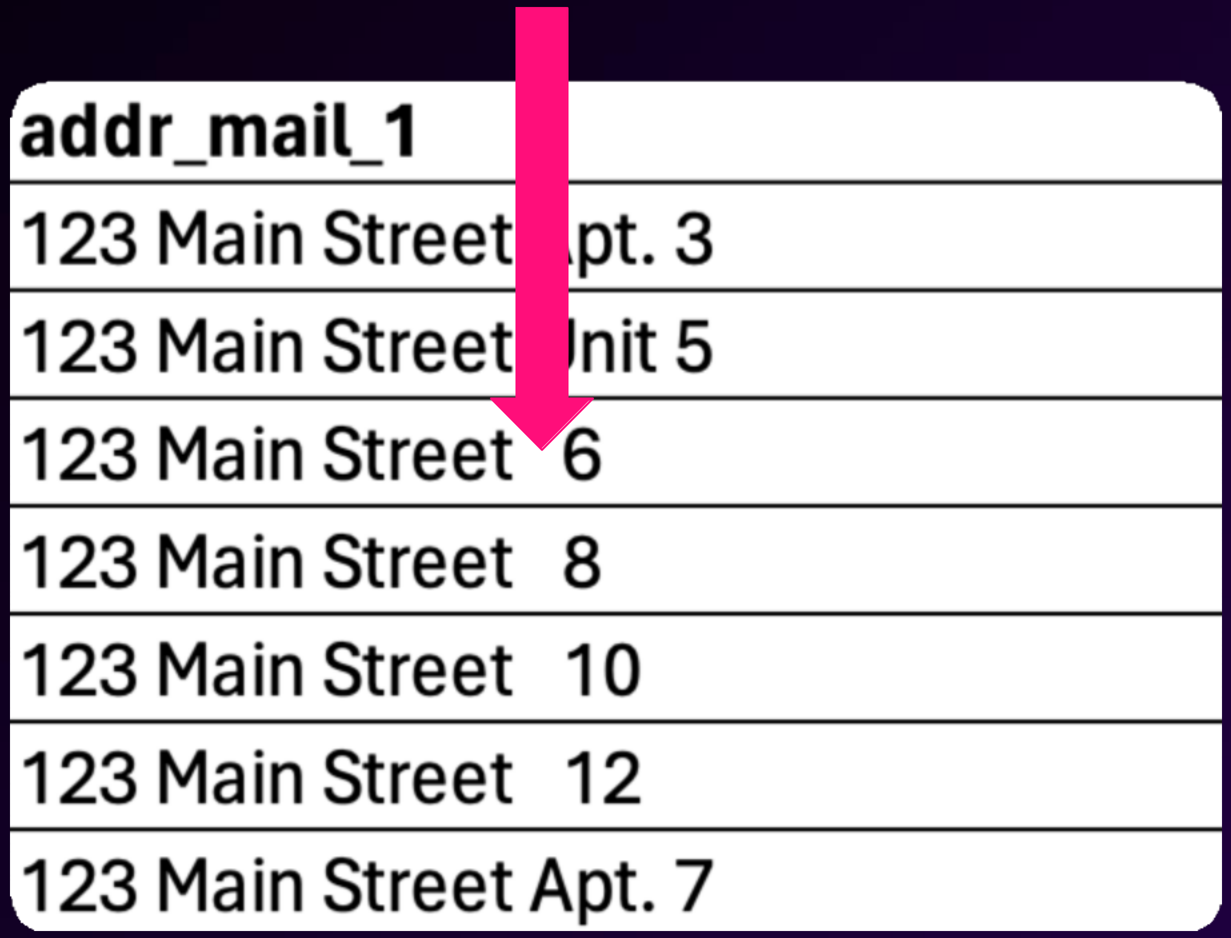
© 2024 SPLUNK INC.

/ how RBA works for cybersecurity in ES

© 2024 SPLUNK INC.

Risk Indicator Found

Claim records contained two spaces in the physical address field



Two Spaces

addr_mail_1
123 Main Street Apt. 3
123 Main Street Unit 5
123 Main Street 6
123 Main Street 8
123 Main Street 10
123 Main Street 12
123 Main Street Apt. 7

© 2024 SPLUNK INC.

Risk Indicator Found

Claim records contained two spaces in the physical address field

merical risk values per Social
(SSN) to quickly identify
etermine how many claims
same fraud indicator.

What does this mean?

Unusual patterns or usage of the system can be used to increment risk for given claims or identities.

The impact is:

- Lower fraud loss.
- Lower false positive rate.
  More efficient, centralized data analytics.
- Make decisions quicker during investigations.

© 2024 SPLUNK INC.

Data Sources

© 2024 SPLUNK INC.

Data Sources

FraudRiskRule-AnomalousLogin FraudRiskRule-DottedGmail FraudRiskRule-SharedSSN FraudRiskRule-SharedBankAccount FraudRiskRule-LandSpeedViolation FraudRiskRule-DisposableEmailDomain FraudRiskRule-ThreatIntelMatchIP FraudRiskRule-BotBehavior FraudRiskRule-ProfileEdit FraudRiskRule-WatchListedAccount

.

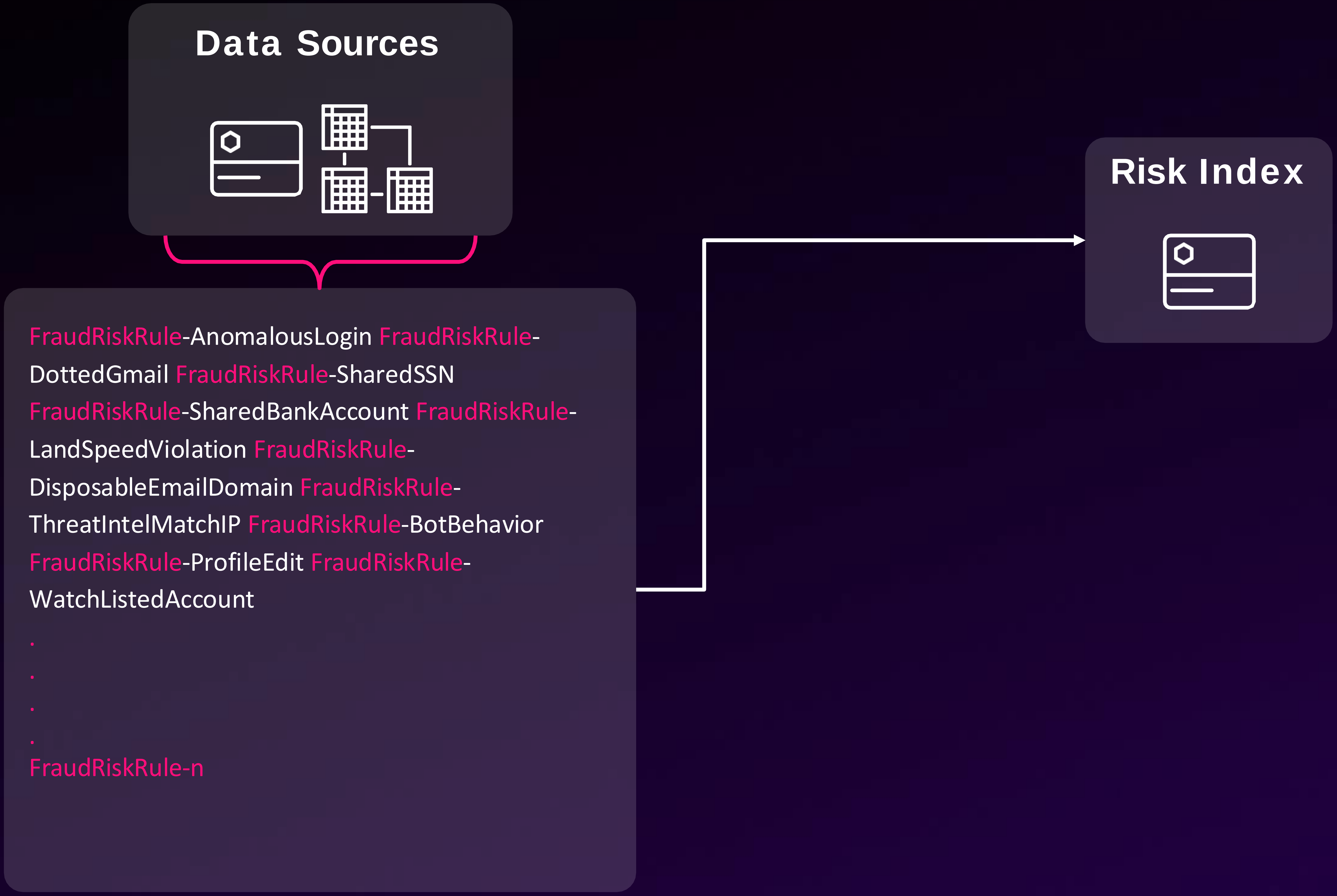
.

.

.

FraudRiskRule-n

© 2024 SPLUNK INC.



Data Sources

FraudRiskRule-AnomalousLogin FraudRiskRule-DottedGmail FraudRiskRule-SharedSSN FraudRiskRule-SharedBankAccount FraudRiskRule-LandSpeedViolation FraudRiskRule-DisposableEmailDomain FraudRiskRule-ThreatIntelMatchIP FraudRiskRule-BotBehavior FraudRiskRule-ProfileEdit FraudRiskRule-WatchListedAccount

.

.

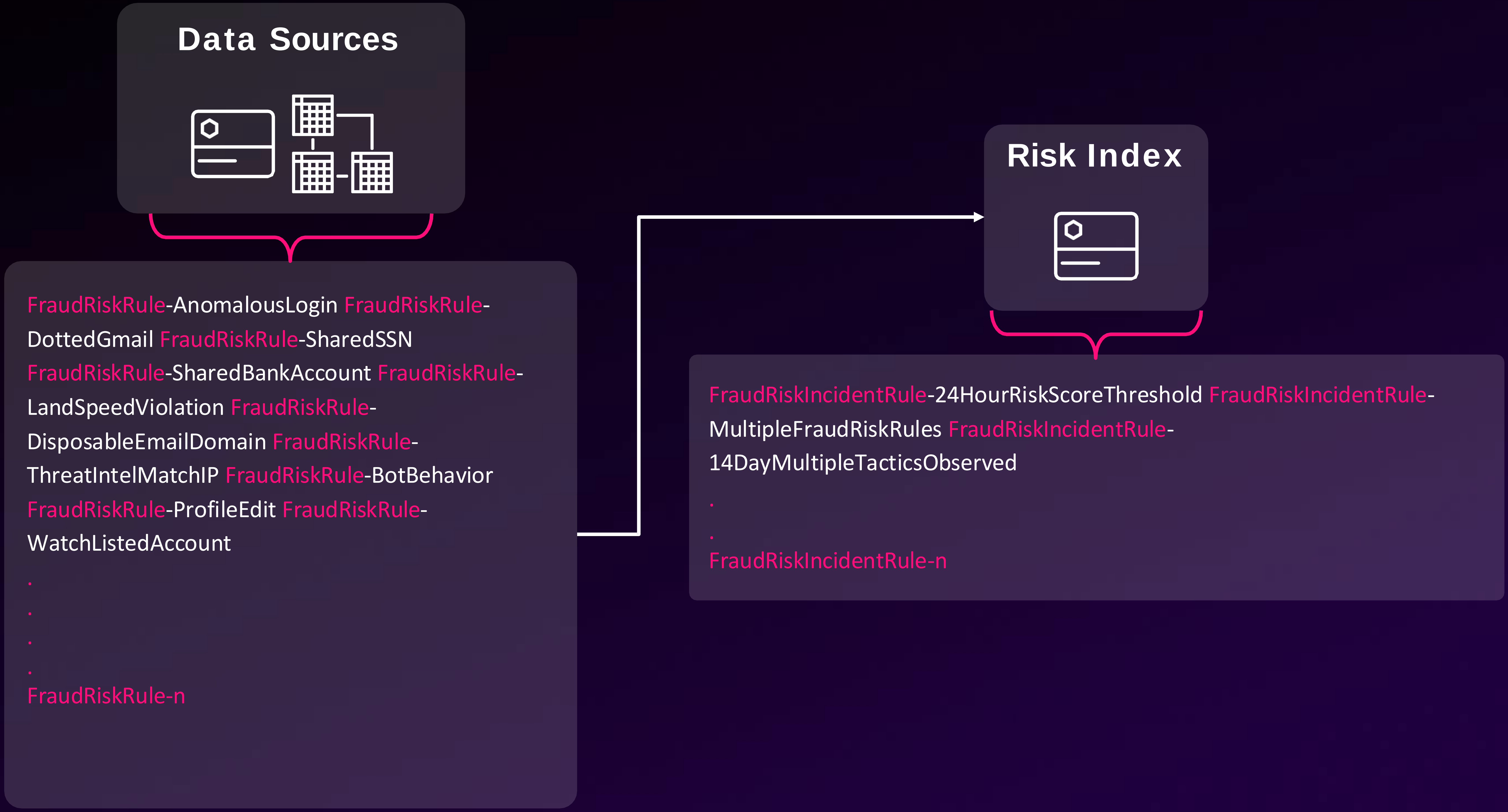
.

.

FraudRiskRule-n

Risk Index

© 2024 SPLUNK INC.



Data Sources

FraudRiskRule-AnomalousLogin FraudRiskRule-DottedGmail FraudRiskRule-SharedSSN FraudRiskRule-SharedBankAccount FraudRiskRule-LandSpeedViolation FraudRiskRule-DisposableEmailDomain FraudRiskRule-ThreatIntelMatchIP FraudRiskRule-BotBehavior FraudRiskRule-ProfileEdit FraudRiskRule-WatchListedAccount

.

.

.

.

FraudRiskRule-n

Risk Index

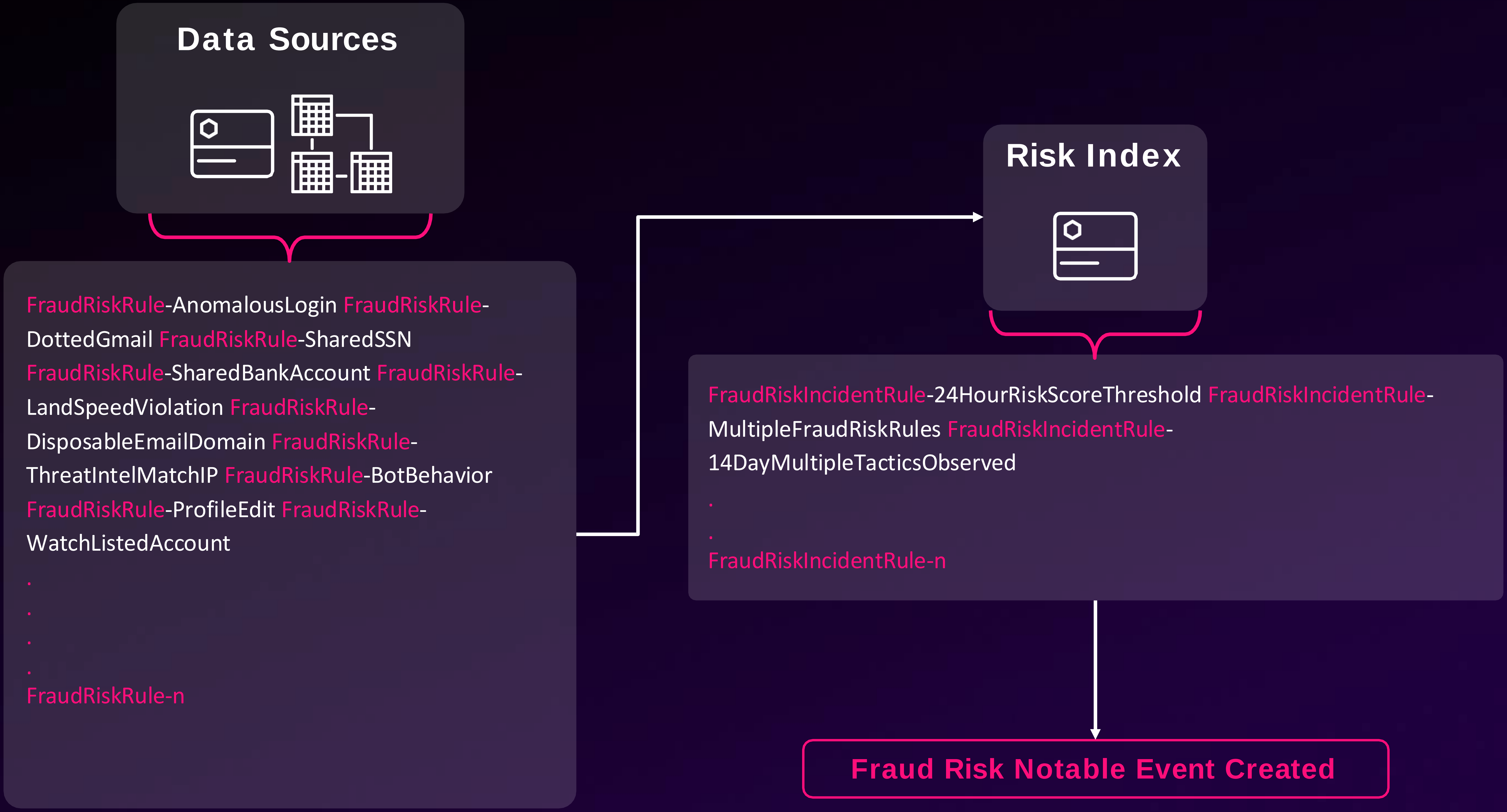
FraudRiskIncidentRule-24HourRiskScoreThreshold FraudRiskIncidentRule-MultipleFraudRiskRules FraudRiskIncidentRule-14DayMultipleTacticsObserved

.

.

FraudRiskIncidentRule-n

© 2024 SPLUNK INC.



Data Sources

FraudRiskRule-AnomalousLogin FraudRiskRule-DottedGmail FraudRiskRule-SharedSSN FraudRiskRule-SharedBankAccount FraudRiskRule-LandSpeedViolation FraudRiskRule-DisposableEmailDomain FraudRiskRule-ThreatIntelMatchIP FraudRiskRule-BotBehavior FraudRiskRule-ProfileEdit FraudRiskRule-WatchListedAccount

.

.

.

.

FraudRiskRule-n

Risk Index

FraudRiskIncidentRule-24HourRiskScoreThreshold FraudRiskIncidentRule-MultipleFraudRiskRules FraudRiskIncidentRule-14DayMultipleTacticsObserved

.

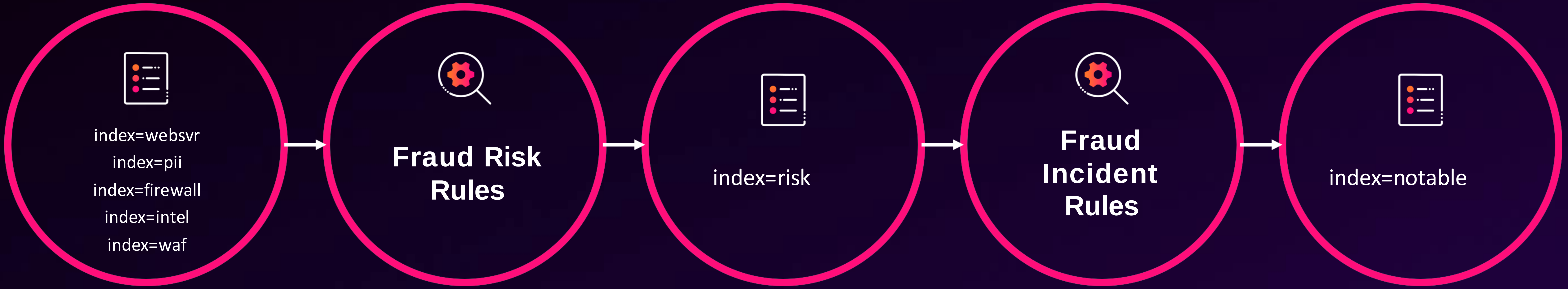
.

FraudRiskIncidentRule-n

Fraud Risk Notable Event Created

© 2024 SPLUNK INC.

Risk-Based Alert (RBA) Pipeline



index=websvr
index=pii
index=firewall
index=intel
index=waf

Fraud Risk Rules

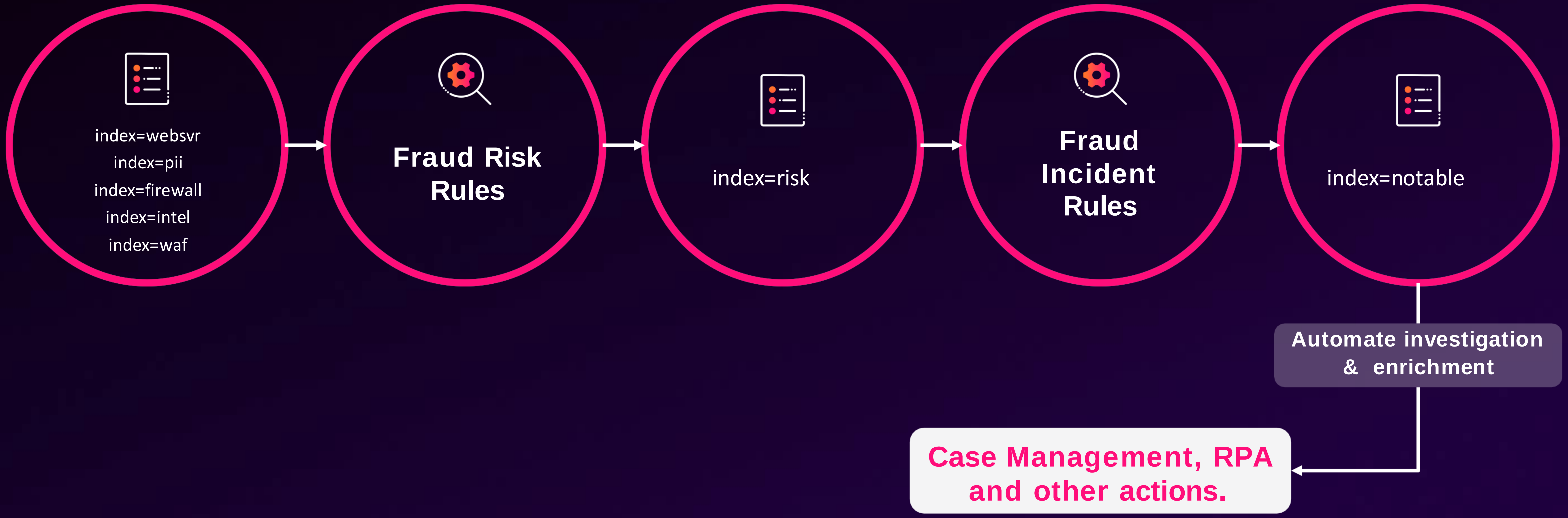
index=risk

Fraud Incident Rules

index=notable

© 2024 SPLUNK INC.

Risk-Based Alert (RBA) Pipeline



index=websvr
index=pii
index=firewall
index=intel
index=waf

Fraud Risk Rules

index=risk

Fraud Incident Rules

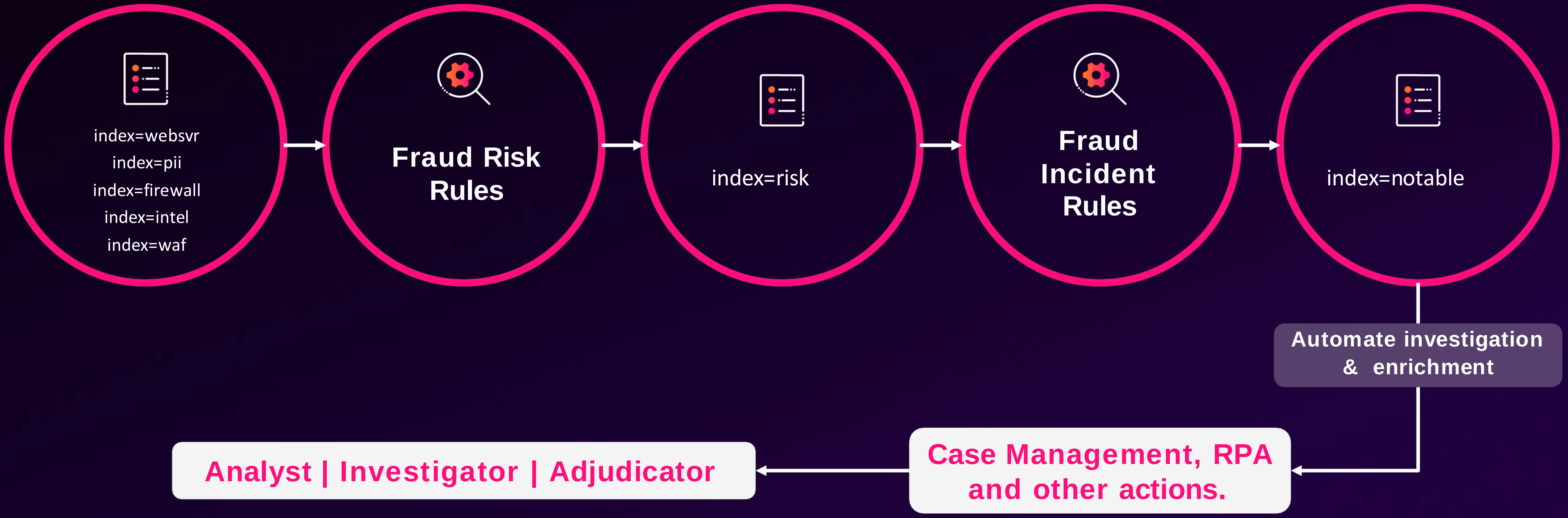
index=notable

Automate investigation & enrichment

Case Management, RPA and other actions.

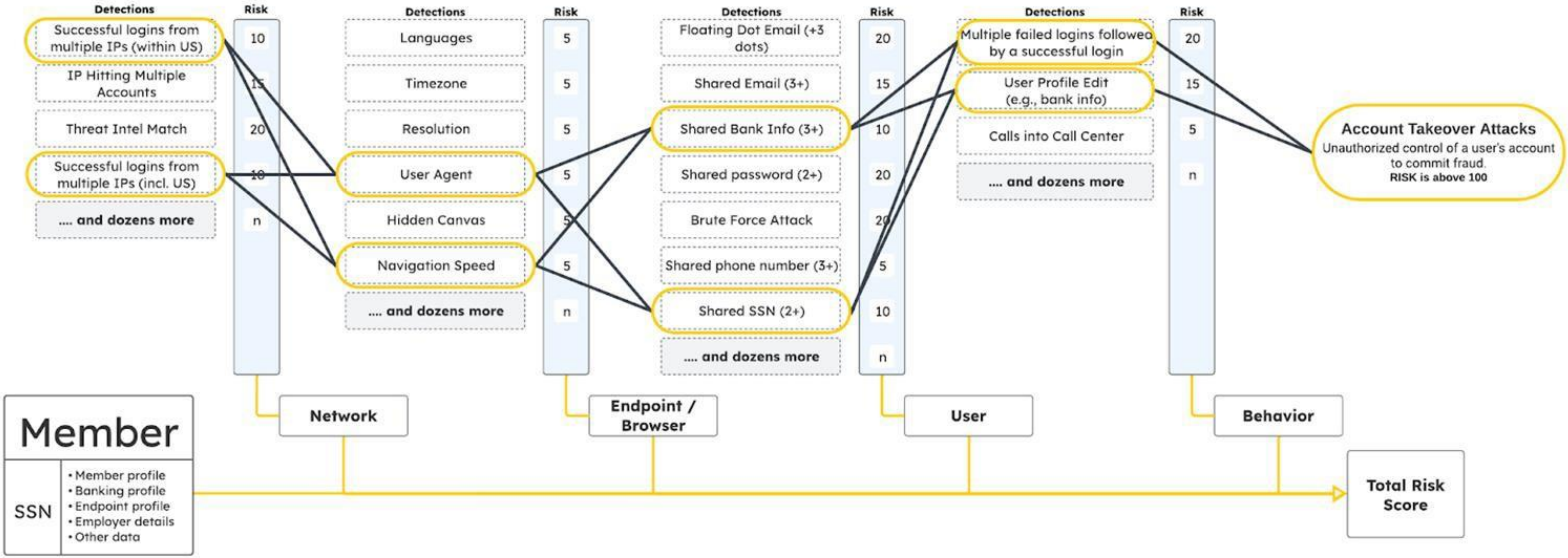
© 2024 SPLUNK INC.

Risk-Based Alert (RBA) Pipeline



© 2024 SPLUNK INC.

Fraud Attack: ATO (account takeover)



Detections	Risk
Successful logins from multiple IPs (within US)	10
IP Hitting Multiple Accounts	15
Threat Intel Match	20
Successful logins from multiple IPs (incl. US)	10
.... and dozens more	n

Network

Detections	Risk
Languages	5
Timezone	5
Resolution	5
User Agent	5
Hidden Canvas	5
Navigation Speed	5
.... and dozens more	n

Endpoint / Browser

Detections	Risk
Floating Dot Email (+3 dots)	20
Shared Email (3+)	15
Shared Bank Info (3+)	10
Shared password (2+)	20
Brute Force Attack	20
Shared phone number (3+)	5
Shared SSN (2+)	10
.... and dozens more	n

User

Detections	Risk
Multiple failed logins followed by a successful login	20
User Profile Edit (e.g., bank info)	15
Calls into Call Center	5
.... and dozens more	n

Behavior

Account Takeover Attacks
Unauthorized control of a user's account to commit fraud.
RISK is above 100

Member

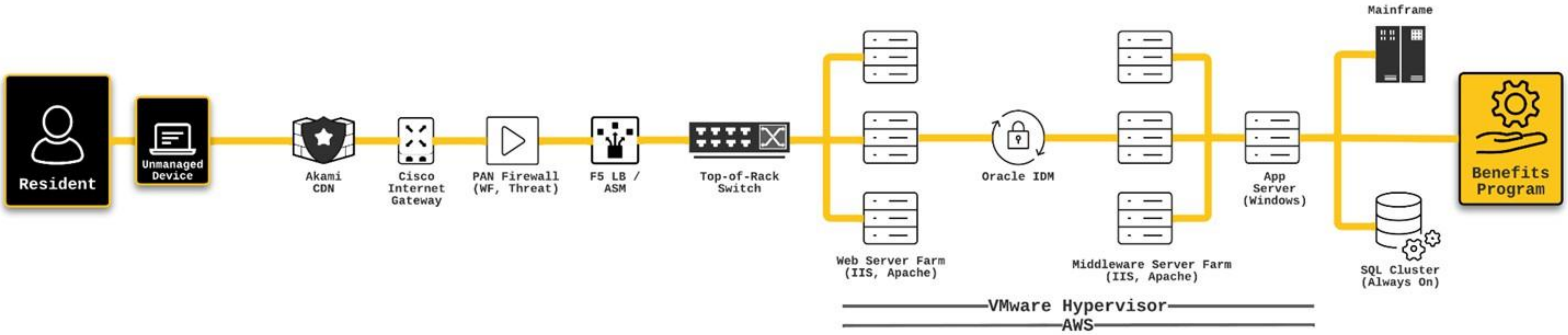
SSN

- Member profile
- Banking profile
- Endpoint profile
- Employer details
- Other data

Total Risk Score

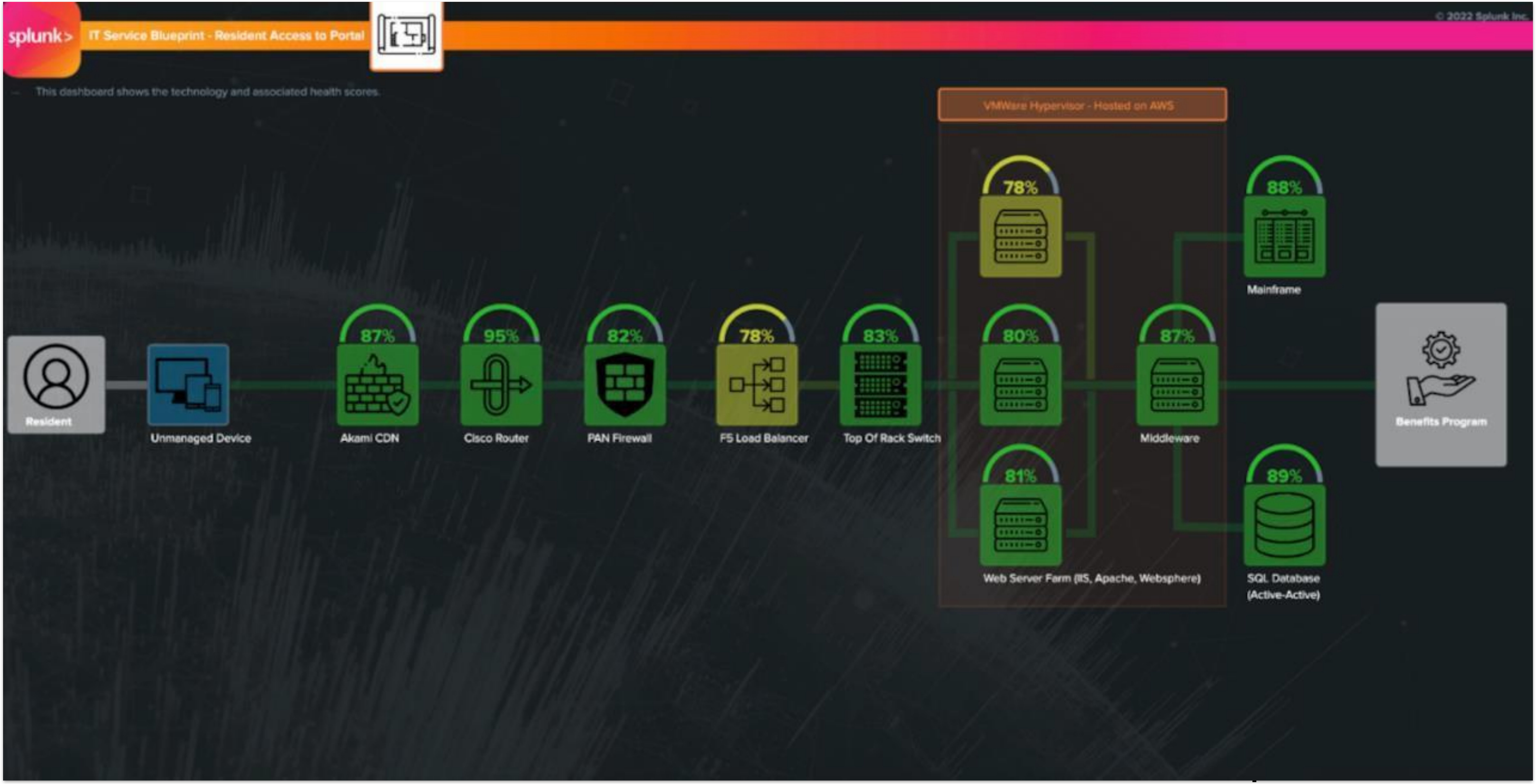
© 2021 SPLUNK INC.

IT Service Blueprint - Resident Access to the State's Unemployment Insurance Benefits (UIB) portal.



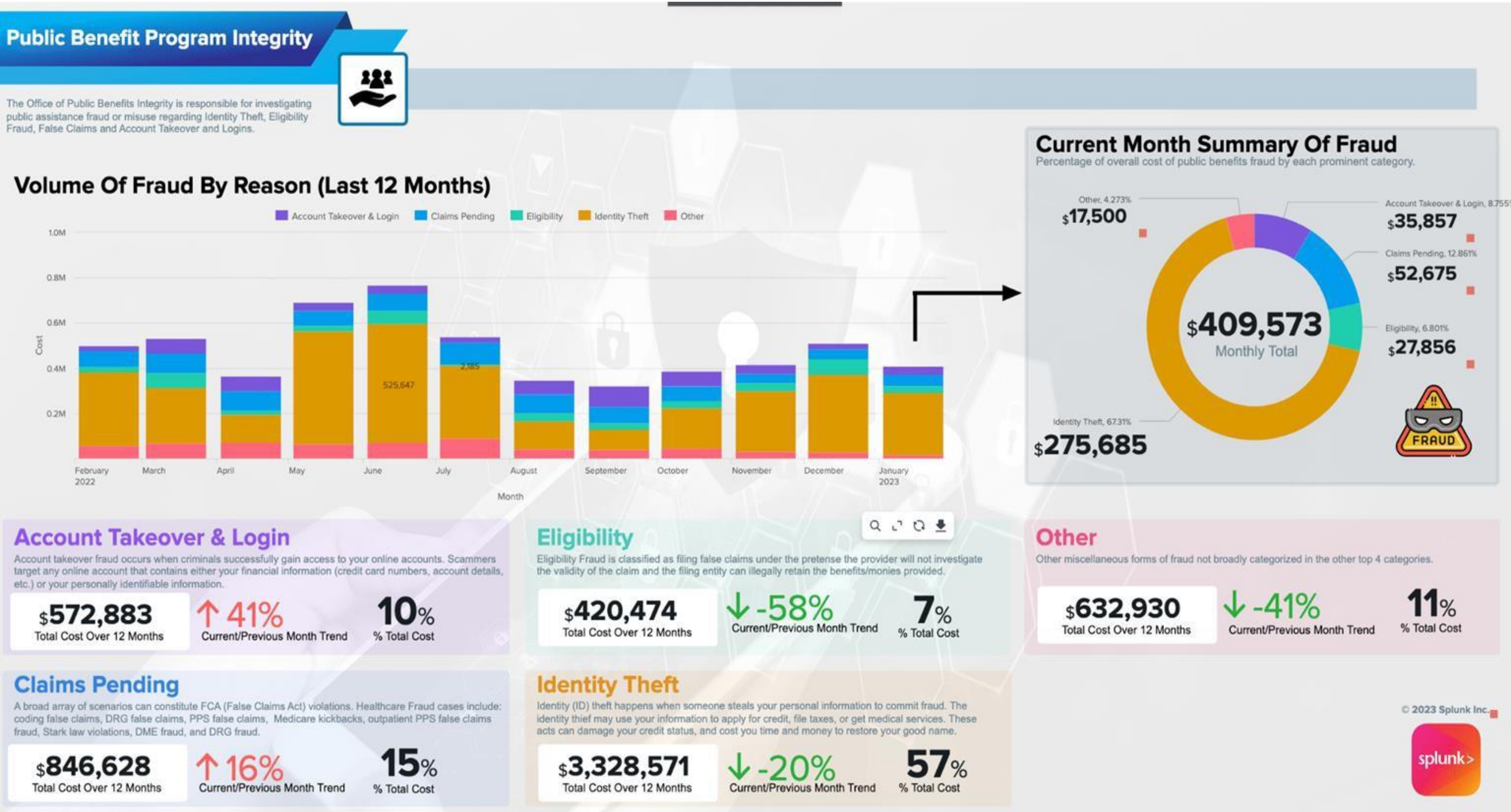
Splunk's Operationalizing Data Analytics Methodology (ODAM)

© 2021 SPLUNK INC.



IT Service Blueprint - Resident Access to Portal

This dashboard shows the technology and associated health scores.



Public Benefit Program Integrity

The Office of Public Benefits Integrity is responsible for investigating public assistance fraud or misuse regarding Identity Theft, Eligibility Fraud, False Claims and Account Takeover and Logins.

Volume Of Fraud By Reason (Last 12 Months)

Current Month Summary Of Fraud

Percentage of overall cost of public benefits fraud by each prominent category.

Account Takeover & Login

Account takeover fraud occurs when criminals successfully gain access to your online accounts. Scammers target any online account that contains either your financial information (credit card numbers, account details, etc.) or your personally identifiable information.

$572,883 Total Cost Over 12 Months

↑ 41% Current/Previous Month Trend

10% % Total Cost

Eligibility

Eligibility Fraud is classified as filing false claims under the pretense the provider will not investigate the validity of the claim and the filing entity can illegally retain the benefits/monies provided.

$420,474 Total Cost Over 12 Months

↓ -58% Current/Previous Month Trend

7% % Total Cost

Other

Other miscellaneous forms of fraud not broadly categorized in the other top 4 categories.

$632,930 Total Cost Over 12 Months

↓ -41% Current/Previous Month Trend

11% % Total Cost

Claims Pending

A broad array of scenarios can constitute FCA (False Claims Act) violations. Healthcare Fraud cases include: coding false claims, DRG false claims, PPS false claims, Medicare kickbacks, outpatient PPS false claims fraud, Stark law violations, DME fraud, and DRG fraud.

$846,628 Total Cost Over 12 Months

↑ 16% Current/Previous Month Trend

15% % Total Cost

Identity Theft

Identity (ID) theft happens when someone steals your personal information to commit fraud. The identity thief may use your information to apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name.

$3,328,571 Total Cost Over 12 Months

↓ -20% Current/Previous Month Trend

57% % Total Cost

© 2023 Splunk Inc.

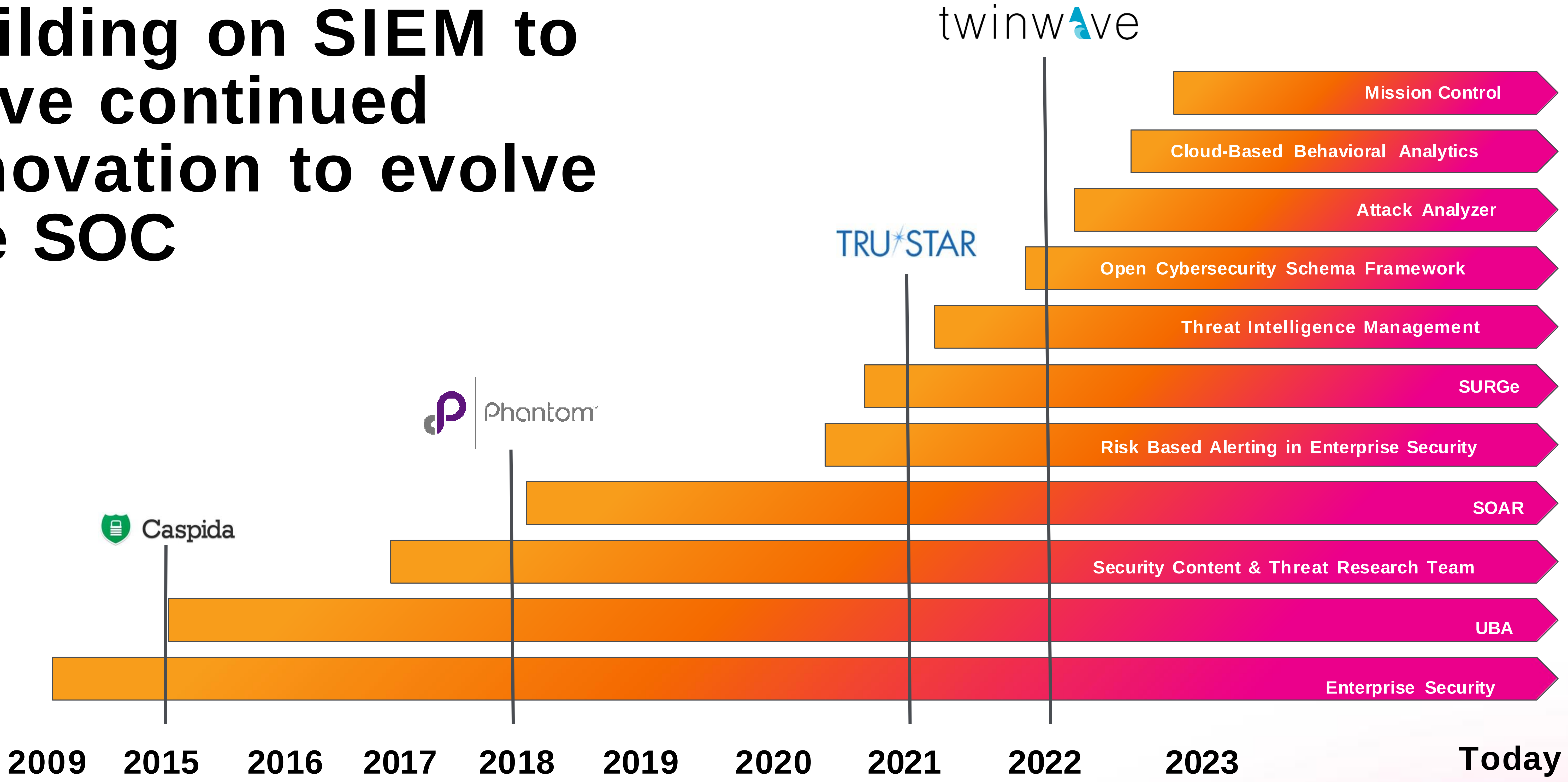
Cybersecurity

© 2024 SPLUNK LLC

Deep Dive on Critical Capabilities

© 2024 SPLUNK LLC

Building on SIEM to drive continued innovation to evolve the SOC



© 2024 SPLUNK INC.

The data landscape is changing for the SOC

How do you effectively manage data for the SOC of the future?

Data is growing exponentially.

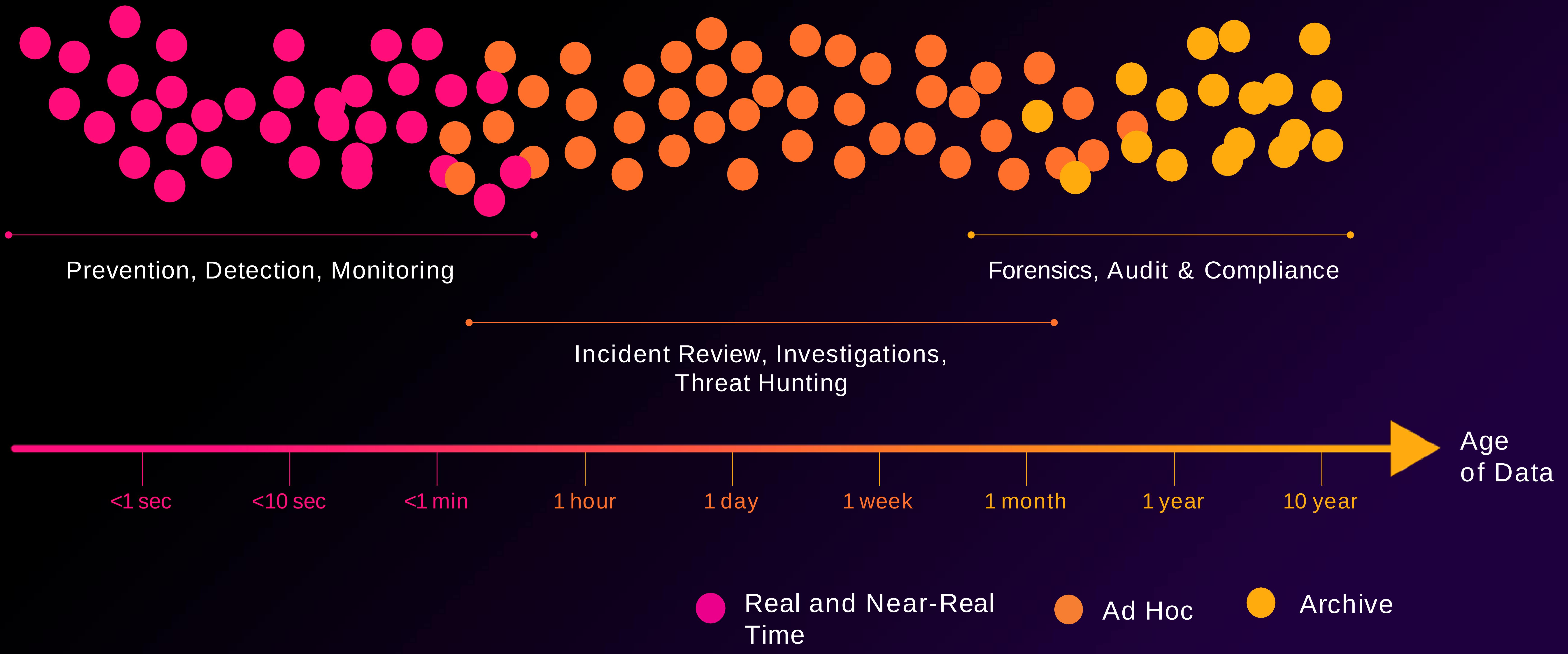
All data is not created equal.

Data may not be able to be moved within a time frame or at all.

© 2024 SPLUNK LLC

Effectively prioritize data based on use cases for your SOC

Manage your data to deliver a stronger security posture



Prevention, Detection, Monitoring

Forensics, Audit & Compliance

Incident Review, Investigations, Threat Hunting

● Real and Near-Real Time

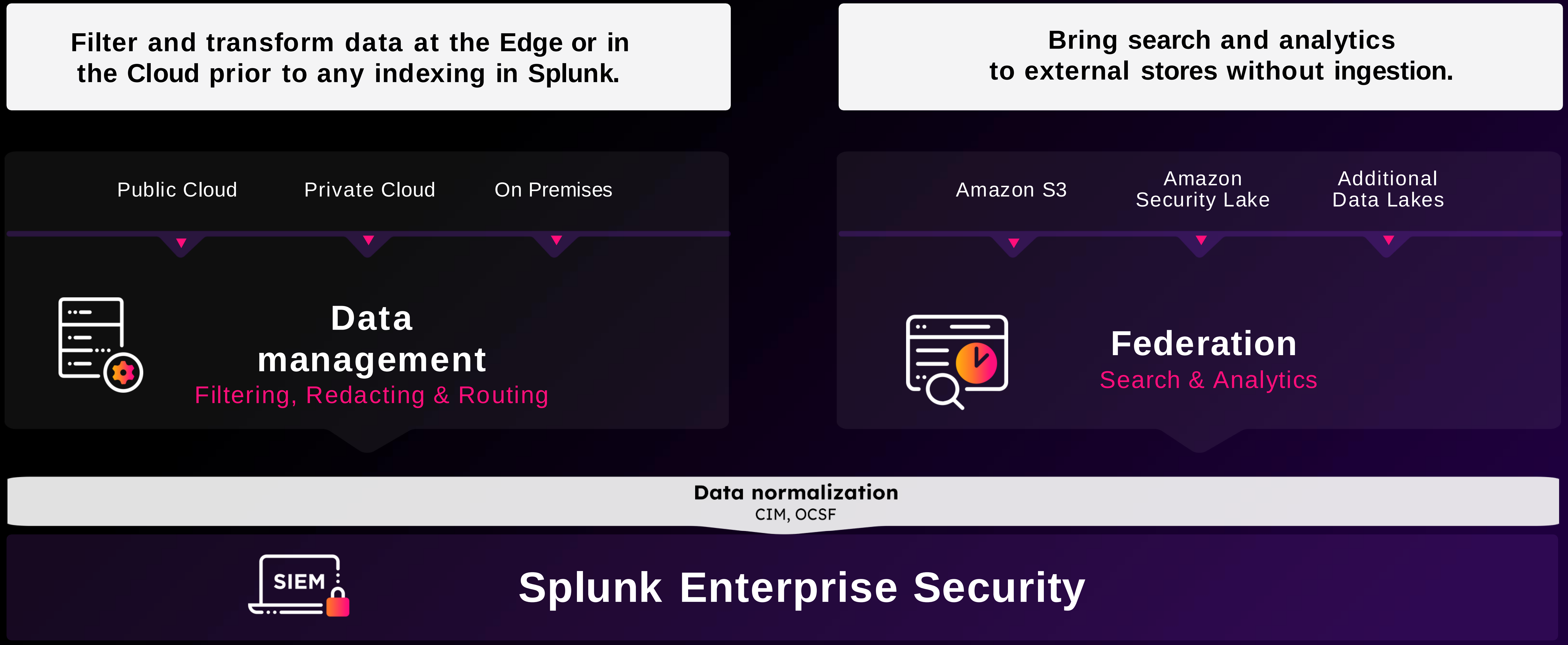
● Ad Hoc

● Archive

© 2024 SPLUNK LLC

Manage SOC data your way

Flexibility to manage, find and analyze actionable data in your SOC.



Filter and transform data at the Edge or in the Cloud prior to any indexing in Splunk.

Bring search and analytics to external stores without ingestion.

Public Cloud

Private Cloud

On Premises

Data management

Filtering, Redacting & Routing

Amazon S3

Amazon Security Lake

Additional Data Lakes

Federation

Search & Analytics

Data normalization

CIM, OCSF

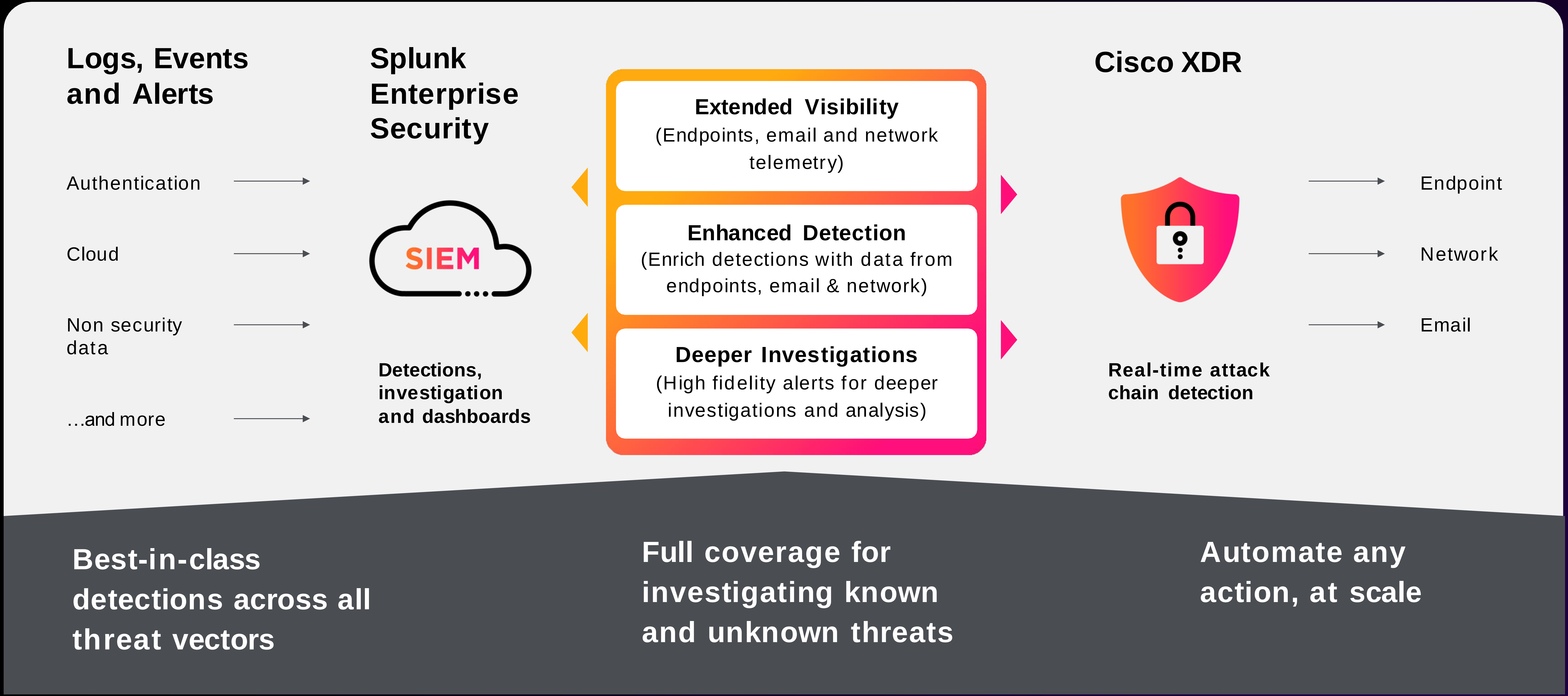
Splunk Enterprise Security

© 2024 SPLUNK LLC

Unified TDIR with automated workflows

Expand detection surface and context

Cisco XDR integration with Splunk ES



Logs, Events and Alerts

- Authentication
- Cloud
- Non security data
- …and more

Splunk Enterprise Security

Detections, investigation and dashboards

Extended Visibility
(Endpoints, email and network telemetry)

Enhanced Detection
(Enrich detections with data from endpoints, email & network)

Deeper Investigations
(High fidelity alerts for deeper investigations and analysis)

Cisco XDR

- Endpoint
- Network
- Email

Real-time attack chain detection

Best-in-class detections across all threat vectors

Full coverage for investigating known and unknown threats

Automate any action, at scale

© 2024 SPLUNK LLC

Transform threat detection

The expanding landscape of cyberthreats

Ransomware attacks

Malware

Phishing attacks

Advanced persistent attacks

Insider threats

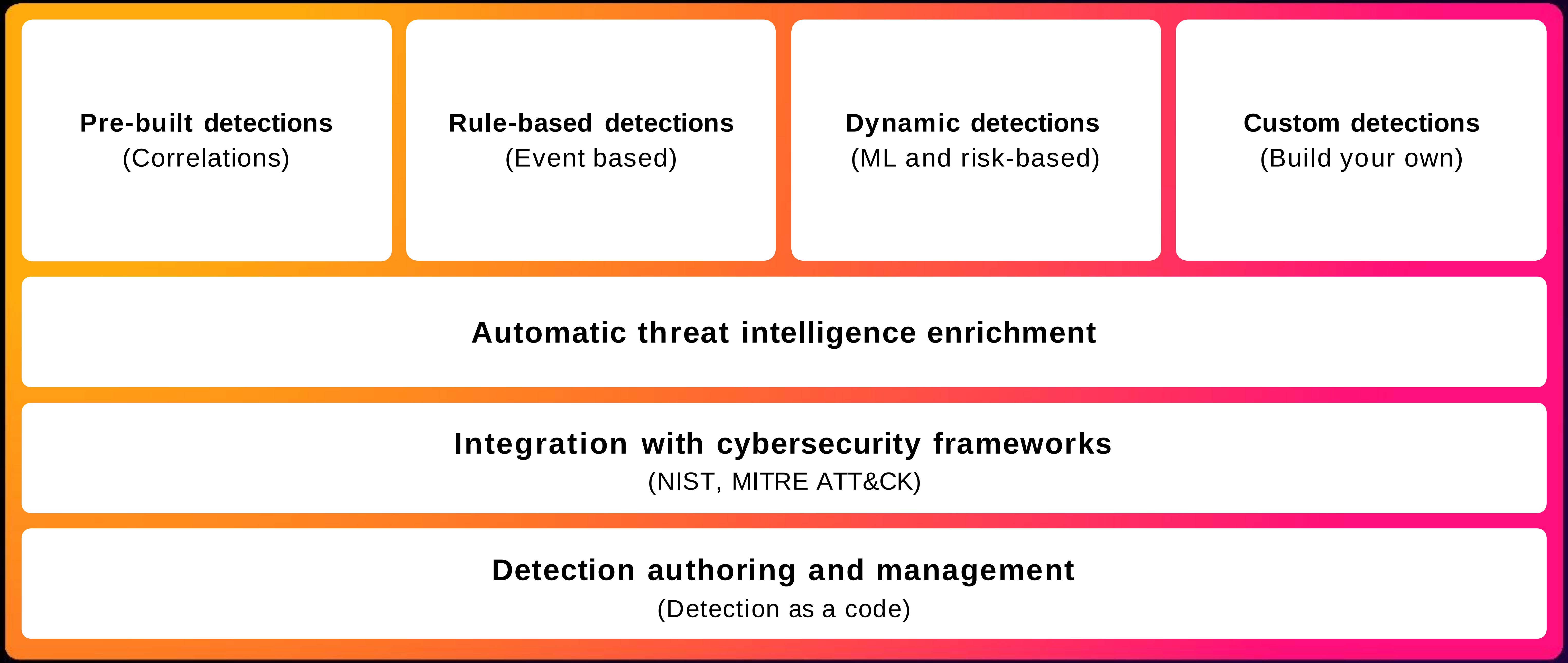
Zero day exploits

AI-Driven attacks

© 2024 SPLUNK LLC

At the core of a TDIR platform are detections

A comprehensive approach is needed to tackle the expanding landscape of cyberthreats



Pre-built detections
(Correlations)

Rule-based detections
(Event based)

Dynamic detections
(ML and risk-based)

Custom detections
(Build your own)

Automatic threat intelligence enrichment

Integration with cybersecurity frameworks
(NIST, MITRE ATT&CK)

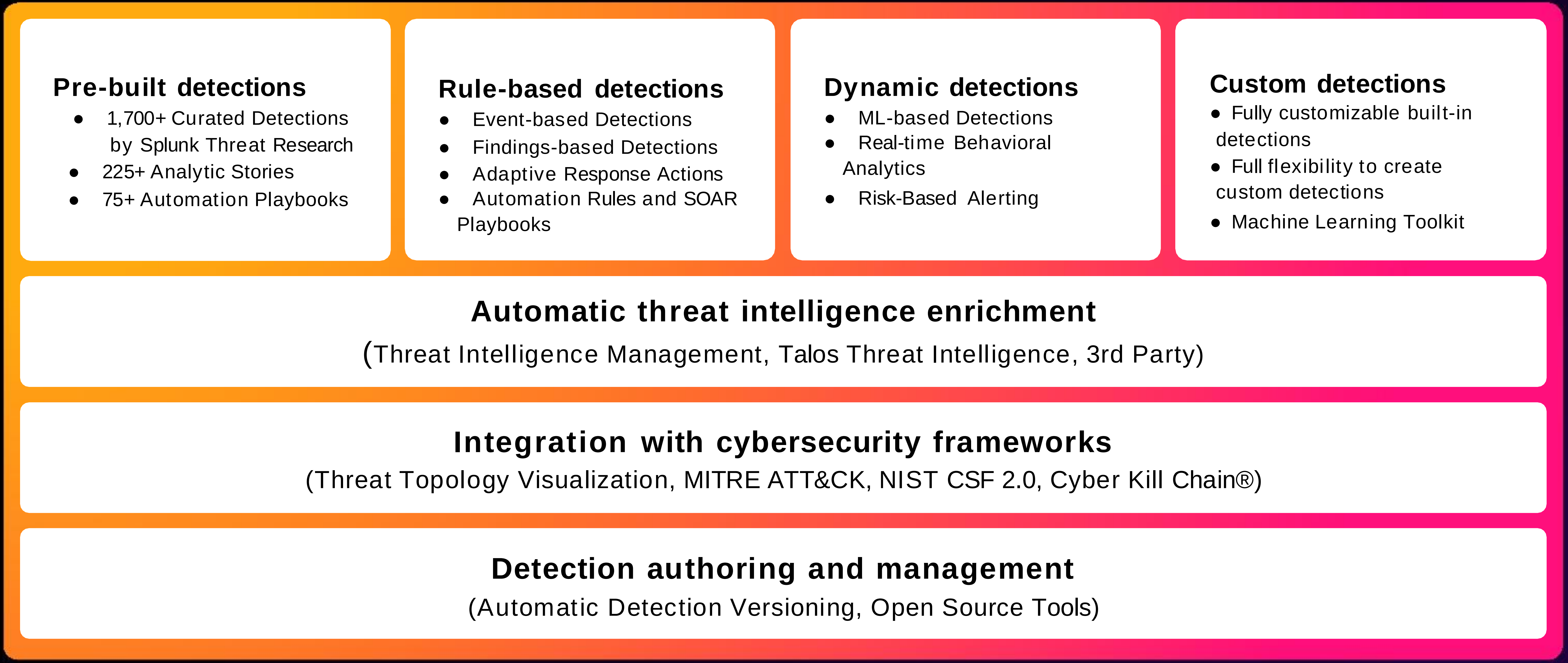
Detection authoring and management
(Detection as a code)

© 2024 SPLUNK LLC

Transform threat detection

Splunk Security delivering a comprehensive approach

World class detection approach for the SOC of the future



Pre-built detections

- 1,700+ Curated Detections by Splunk Threat Research
- 225+ Analytic Stories
- 75+ Automation Playbooks

Rule-based detections

- Event-based Detections
- Findings-based Detections
- Adaptive Response Actions
- Automation Rules and SOAR Playbooks

Dynamic detections

- ML-based Detections
- Real-time Behavioral Analytics
- Risk-Based Alerting

Custom detections

- Fully customizable built-in detections
- Full flexibility to create custom detections
- Machine Learning Toolkit

Automatic threat intelligence enrichment

(Threat Intelligence Management, Talos Threat Intelligence, 3rd Party)

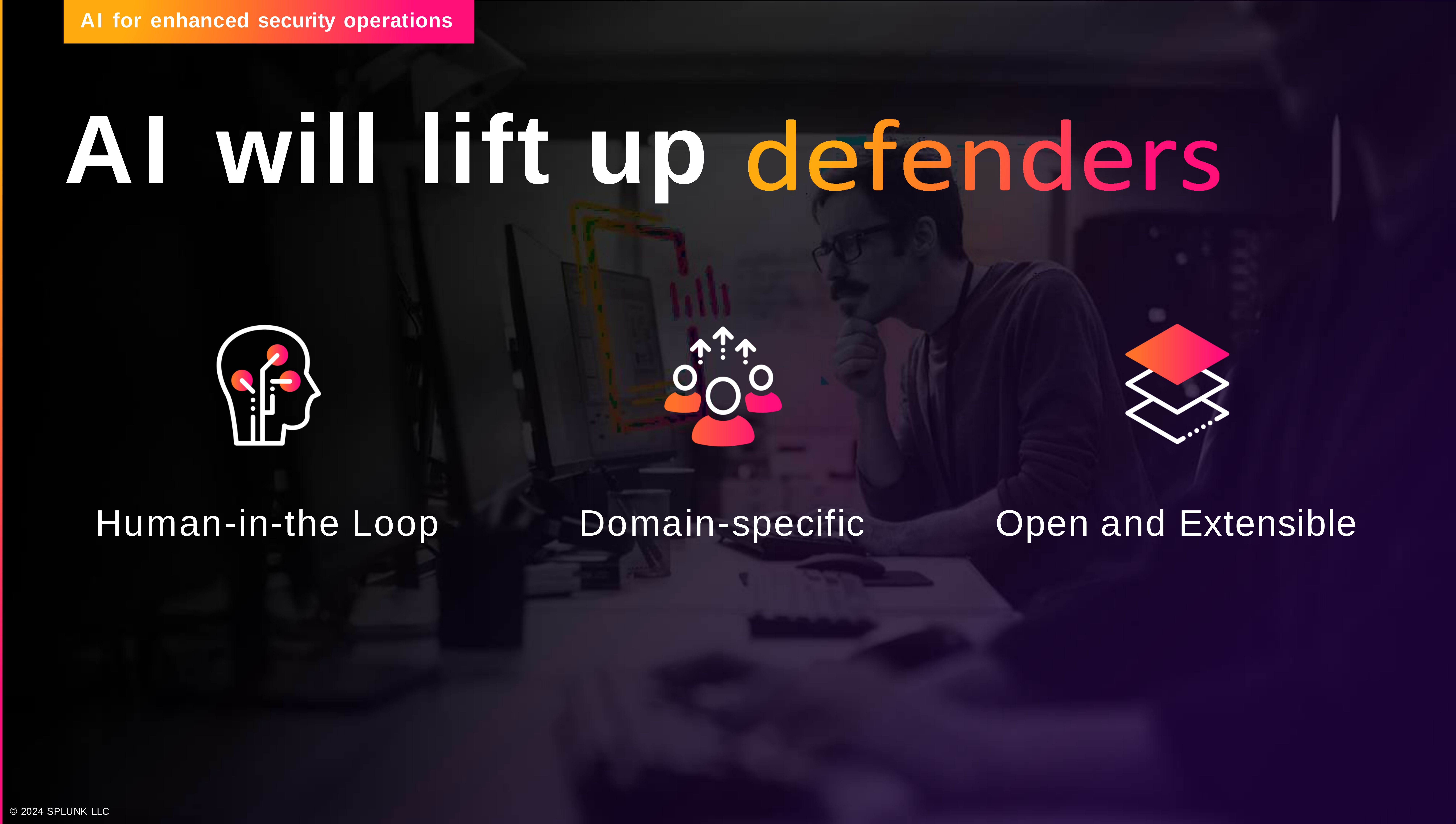
Integration with cybersecurity frameworks

(Threat Topology Visualization, MITRE ATT&CK, NIST CSF 2.0, Cyber Kill Chain®)

Detection authoring and management

(Automatic Detection Versioning, Open Source Tools)

© 2024 SPLUNK LLC



AI will lift up defenders

Human-in-the Loop

Domain-specific

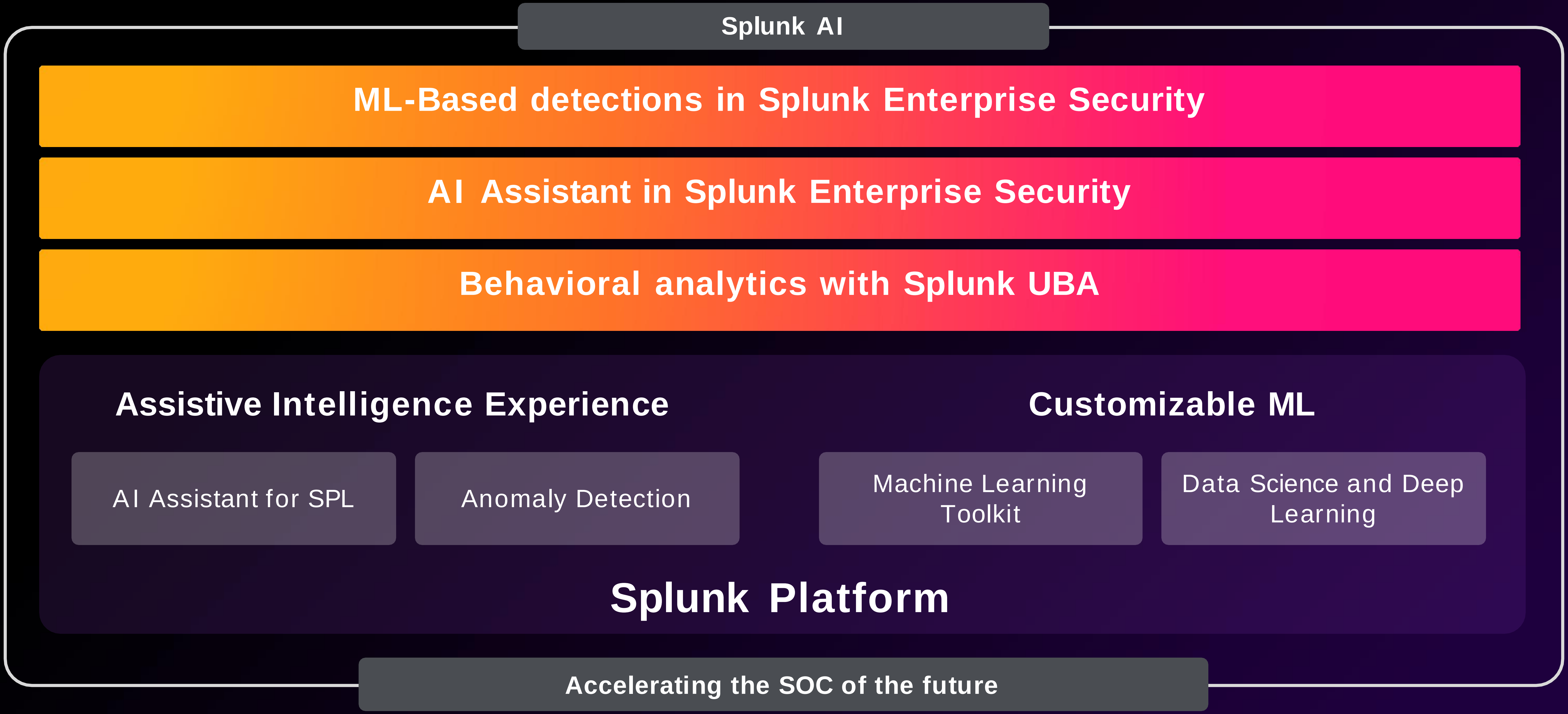
Open and Extensible

© 2024 SPLUNK LLC

AI for enhanced security operations

Driving a new wave of maturity for the SOC

Powered by Splunk AI



Splunk AI

ML-Based detections in Splunk Enterprise Security

AI Assistant in Splunk Enterprise Security

Behavioral analytics with Splunk UBA

Assistive Intelligence Experience

- AI Assistant for SPL
- Anomaly Detection

Customizable ML

- Machine Learning Toolkit
- Data Science and Deep Learning

Splunk Platform

Accelerating the SOC of the future

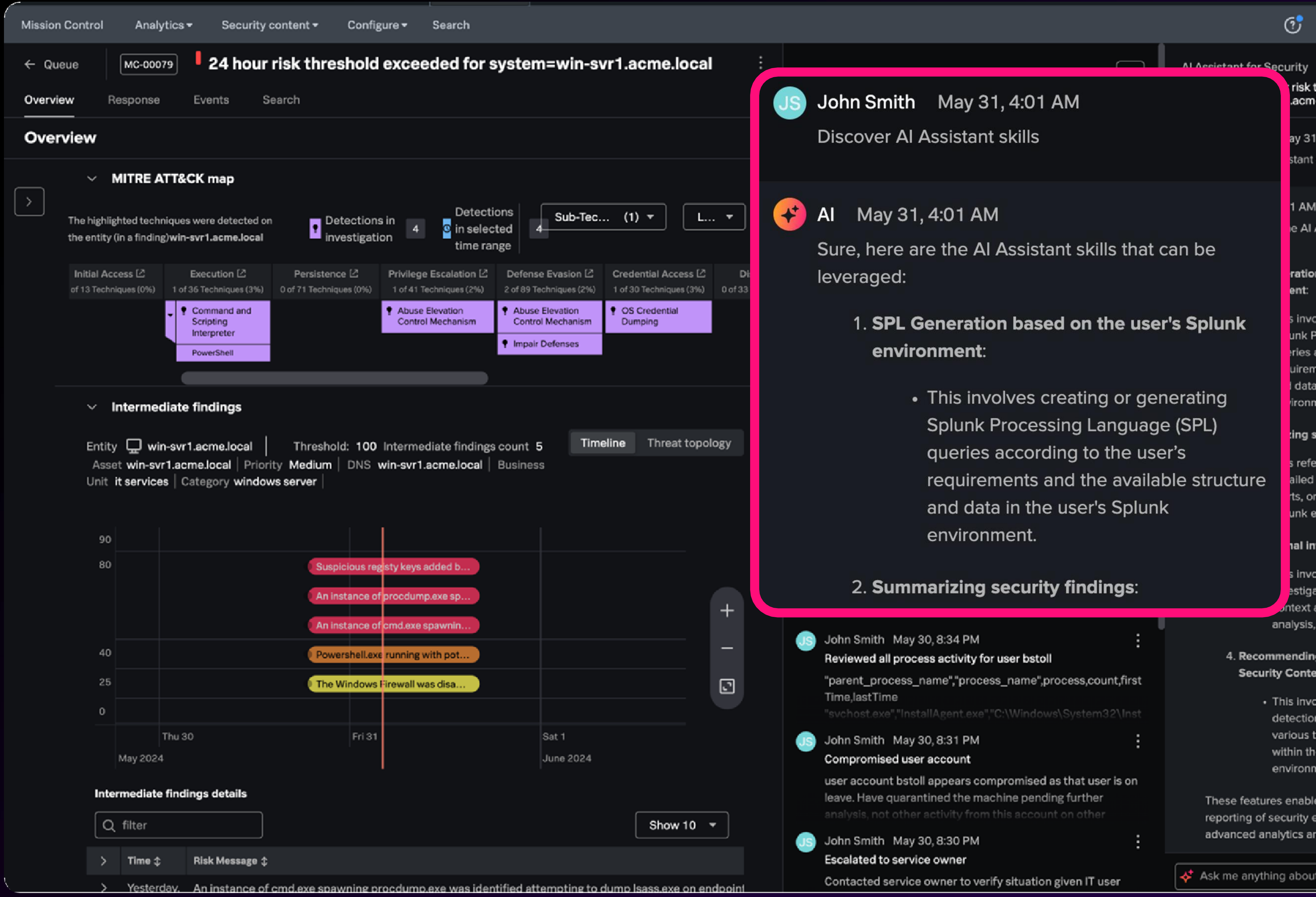
© 2024 SPLUNK LLC

AI for enhanced security operations

AI Assistant

Guided Security workflows where you do your work

- Answer analyst questions to guide daily workflows
- Save time while addressing threats more rapidly
- Use natural language queries to get answers during investigations



24 hour risk threshold exceeded for system=win-svr1.acme.local

Overview

MITRE ATT&CK map

The highlighted techniques were detected on the entity (in a finding)win-svr1.acme.local

Detections in investigation 4

Detections in selected time range 4

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Di
of 13 Techniques (0%)	1 of 36 Techniques (3%)	0 of 71 Techniques (0%)	1 of 41 Techniques (2%)	2 of 89 Techniques (2%)	1 of 30 Techniques (3%)	0 of 33
	Command and Scripting Interpreter PowerShell		Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism Impair Defenses	OS Credential Dumping	

Intermediate findings

Entity win-svr1.acme.local | Threshold: 100 Intermediate findings count 5
Asset win-svr1.acme.local | Priority Medium | DNS win-svr1.acme.local | Business Unit it services | Category windows server |

90
80
40
25
0
Suspicious registy keys added b...
An instance of procdump.exe sp...
An instance of cmd.exe spawnin...
Powershell.exe running with pot...
The Windows Firewall was disa...
Thu 30
Fri 31
Sat 1
May 2024
June 2024

Intermediate findings details

Time	Risk Message
Yesterday,	An instance of cmd.exe spawning procdump.exe was identified attempting to dump lsass.exe on endpoint

John Smith May 31, 4:01 AM
Discover AI Assistant skills

AI May 31, 4:01 AM
Sure, here are the AI Assistant skills that can be leveraged:

1. **SPL Generation based on the user's Splunk environment**:
   - This involves creating or generating Splunk Processing Language (SPL) queries according to the user's requirements and the available structure and data in the user's Splunk environment.
2. **Summarizing security findings**:

John Smith May 30, 8:34 PM
Reviewed all process activity for user bstoll
"parent_process_name","process_name",process,count,firstTime,lastTime
"svchost.exe","InstallAgent.exe","C:\Windows\System32\Inst

John Smith May 30, 8:31 PM
Compromised user account
user account bstoll appears compromised as that user is on leave. Have quarantined the machine pending further analysis, not other activity from this account on other

John Smith May 30, 8:30 PM
Escalated to service owner
Contacted service owner to verify situation given IT user

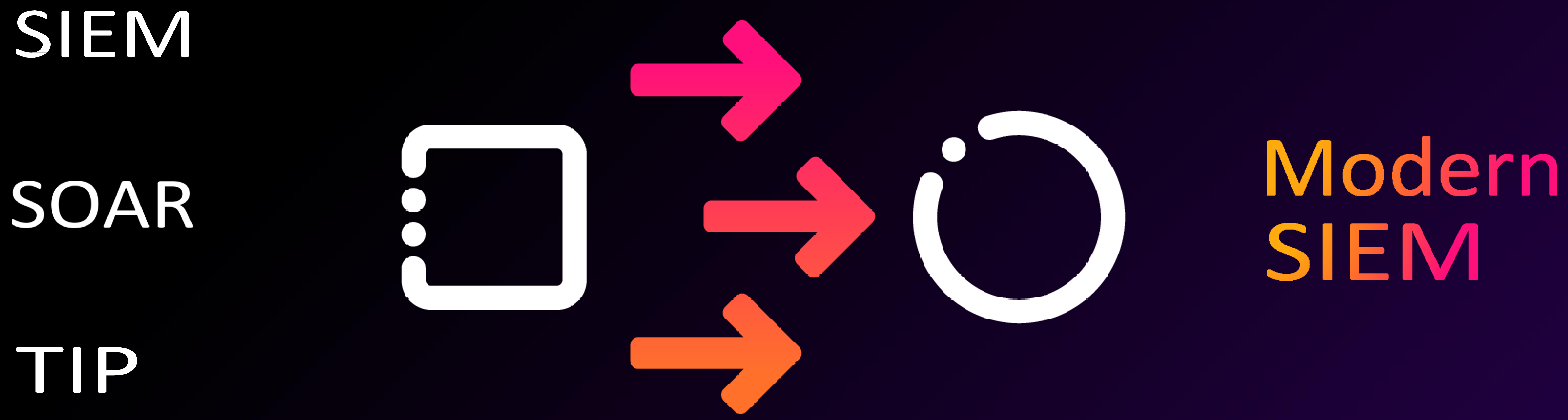
UI shown is for illustration; not final product.

© 2024 SPLUNK LLC

Unified TDIR with automated workflows

Unified TDIR is driving convergence

Simplify the use of critical tools for the SOC of the future



SIEM

SOAR

TIP

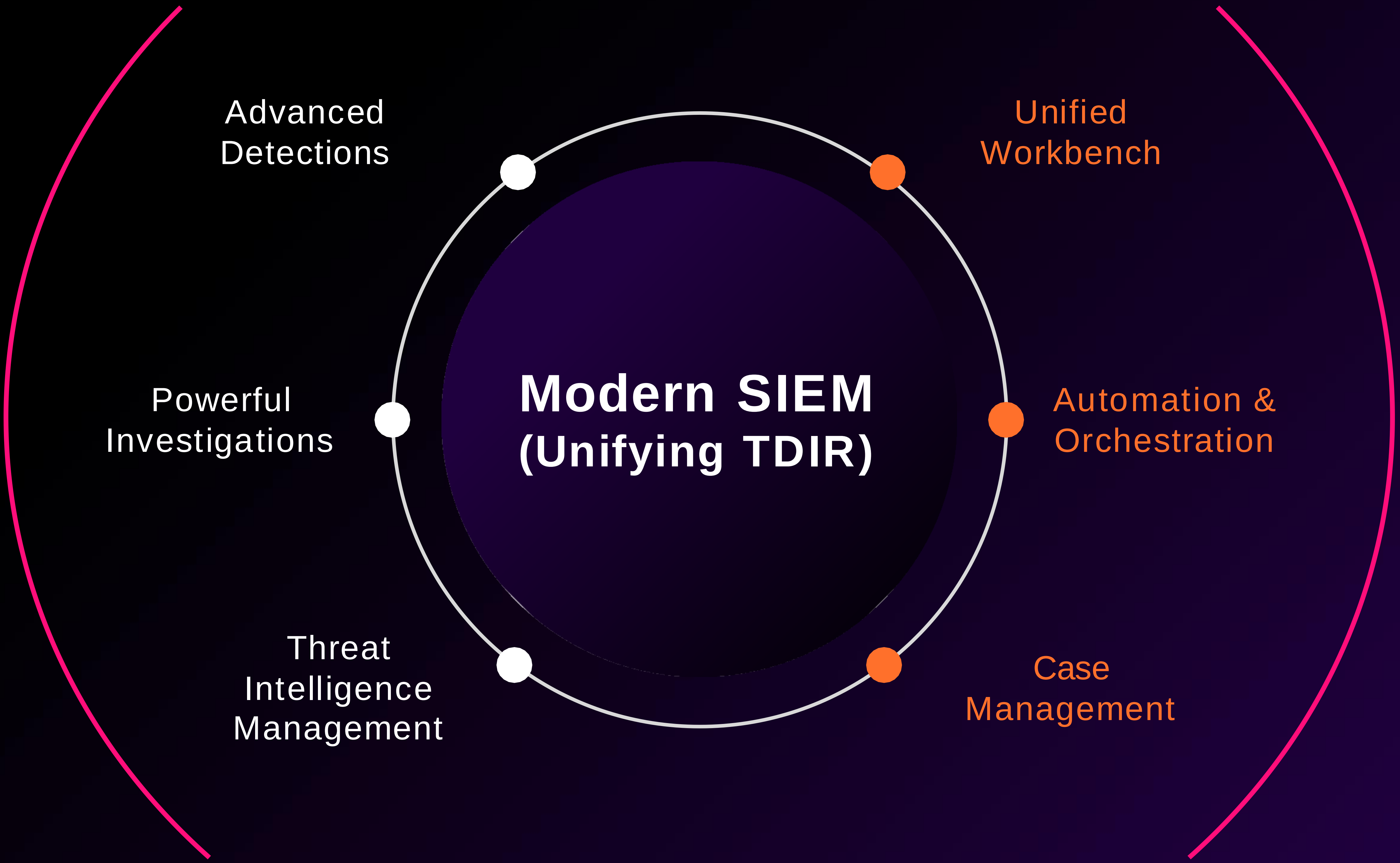
Modern SIEM

© 2024 SPLUNK LLC

Unified TDIR with automated workflows

Re-imagining the SIEM for the SOC of the future

Anchoring the Unified TDIR with automated workflows at the core of the SOC


Advanced Detections
Unified Workbench
Powerful Investigations
Modern SIEM (Unifying TDIR)
Automation & Orchestration
Threat Intelligence Management
Case Management

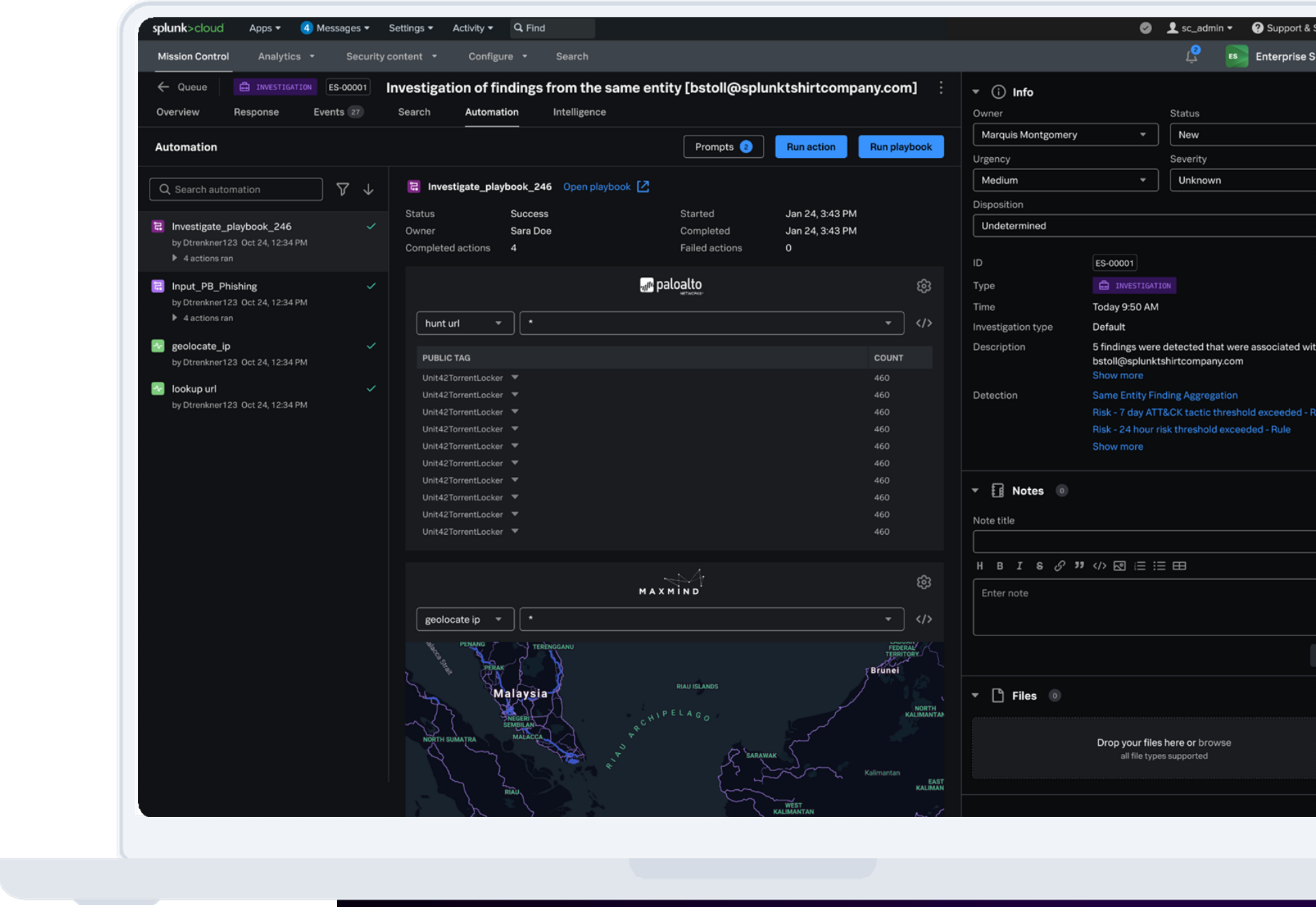
© 2024 SPLUNK LLC

Unified TDIR with automated workflows

Meet the modern SIEM

Powering the SOC of the future with ES 8.0

- Improved case management capabilities
- Native SOAR integration with a unified worksurface
- Enhanced detection engineering capabilities
- Simplified terminology for security analytics



INVESTIGATION ES-00001 Investigation of findings from the same entity [bstoll@splunktshirtcompany.com]

Automation

Investigate_playbook_246 ✓
by Dtrenkner123 Oct 24, 12:34 PM
4 actions ran

Input_PB_Phishing ✓
by Dtrenkner123 Oct 24, 12:34 PM
4 actions ran

geolocate_ip ✓
by Dtrenkner123 Oct 24, 12:34 PM

lookup url ✓
by Dtrenkner123 Oct 24, 12:34 PM

Investigate_playbook_246

Status	Success	Started	Jan 24, 3:43 PM
Owner	Sara Doe	Completed	Jan 24, 3:43 PM
Completed actions	4	Failed actions	0

PUBLIC TAG	COUNT
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460

Info

Owner: Marquis Montgomery
Status: New
Urgency: Medium
Severity: Unknown
Disposition: Undetermined

ID: ES-00001
Type: INVESTIGATION
Time: Today 9:50 AM
Investigation type: Default
Description: 5 findings were detected that were associated wit
bstoll@splunktshirtcompany.com
Show more
Detection: Same Entity Finding Aggregation
Risk - 7 day ATT&CK tactic threshold exceeded - R
Risk - 24 hour risk threshold exceeded - Rule
Show more

Notes 0

Note title

Files 0

ES 8.0 UI shown is for illustration; not final product.

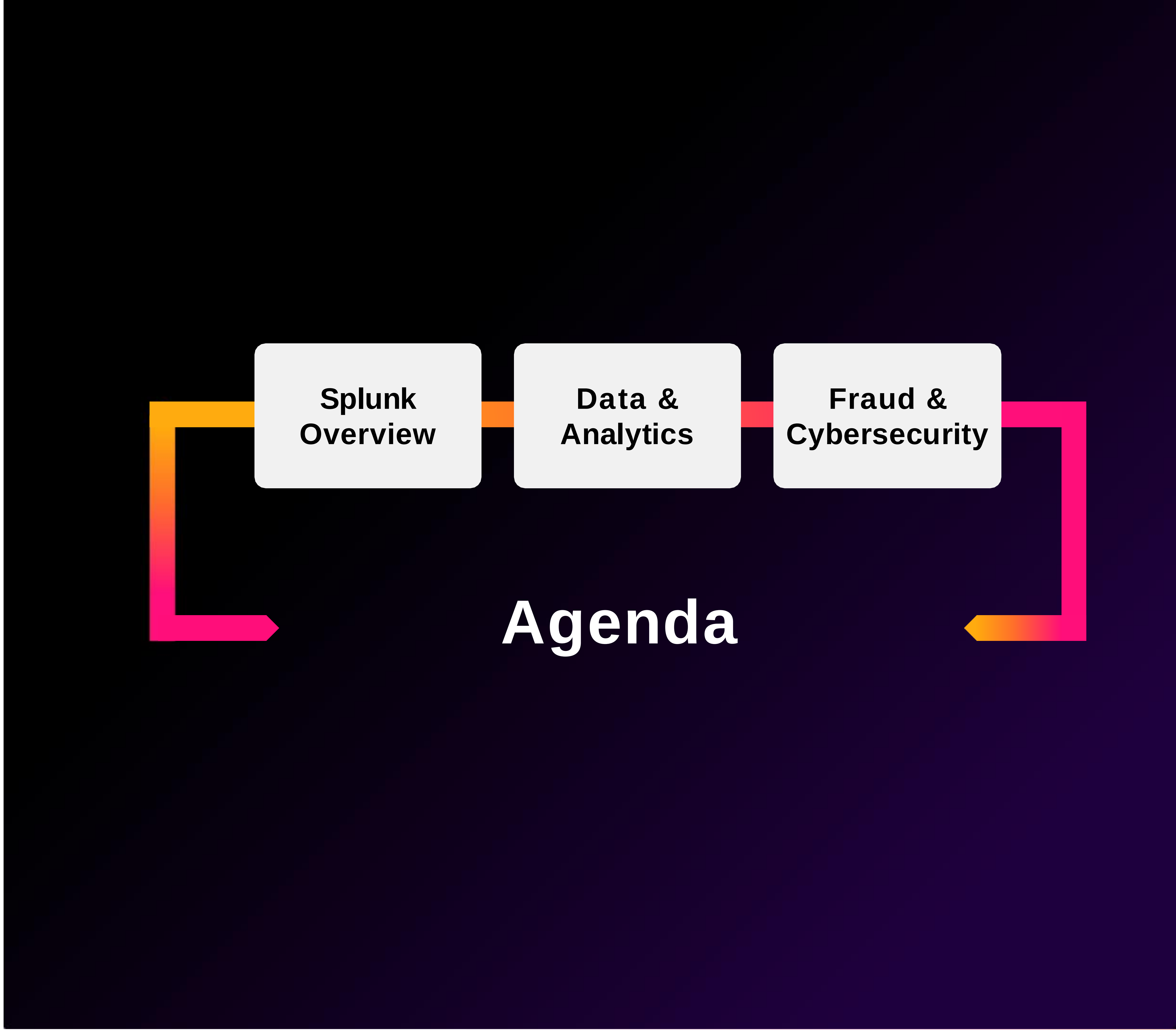
© 2024 SPLUNK LLC

Summary

- Splunk is a platform that can be used to extract value out of your data.
- Risk-Based Alerting (RBA) is a game-changer.
- Data storytelling is a key skill to cultivate.
- Splunk’s AI capabilities will change how you work.
- Blueprinting your IT Services is a great place to start.
- Signals, Semantics and Logic - the three layers of data.
- Descriptive, Diagnostic, Predictive and Prescriptive - the four levels of data analytics.

© 2024 SPLUNK INC.

How it started



Splunk Overview

Data & Analytics

Fraud & Cybersecurity

Agenda

© 2024 SPLUNK INC.

Thank You

Q & A

© 2024 SPLUNK INC.