Impulse el SOC del futuro

Splunk Security

Alberto Zamora
Staff Partner Solutions Engineer

splunk> a cisco company

Ampliación de la superficie de ataque

Herramientas, equipos, datos y flujos de trabajo aislados

Innovación estancada

Mandatos de cumplimiento

Actores de amenazas sofisticados

Volúmenes de ataques crecientes

Escasez de talento y habilidades


95%
de los CISO informaron haber sufrido al menos un ataque disruptivo en su organización durante el último año.
Source: Splunk CISO Report
© 2024 SPLUNK LLC

El impacto

Pérdida de ingresos

Pérdida de reputación

Multas y sanciones

“El tiempo de inactividad en ciberseguridad es la forma más costosa de comprender el tiempo de inactividad en general”.

-Luca Panattoni, Head of IT and Digital Transformation, Carrefour


Es hora de
reimaginar
el SOC

El SOC
Del futuro

- ❑ Completa visibilidad
- ❑ Contexto y colaboración
- ❑ Camino claro hacia la resolución

Con TDIR unificando en el núcleo

- Consolidación de herramientas
- Eficiencias de flujos de trabajo
- Manejo de datos

El enfoque de la plataforma TDIR unificada de Splunk

Flexible Deployment Models

True Multi Vendor

Experiencia de analista unificado
Workflows | Case Management | Collaboration

Detección de amenazas ⟷ **Investigación** ⟷ **Respuesta**

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

Risk-Based Alerting | Threat Hunting | Integrated Analytics

Enrichment | Automation | Orchestration | Playbooks

GenAI para SecOps
Summarization | Natural Language Search | Reporting

Servicios Comunes
Assets & Identities | Threat Intelligence | Risk

Gestión y federación de datos
Filter | Mask | Route | Access

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

Libere capacidades de seguridad críticas

Data Management and Federation

Busque, analice y administre datos dondequiera que residan

Gestione eficazmente sus necesidades de gestión de datos complejos. Acceda sin problemas a los datos almacenados en diferentes almacenes de datos para búsquedas y análisis.

Transform Threat Detection

Abordar un panorama de amenazas en expansión

Diseñe y cree detecciones para respaldar una variedad de metodologías de detección e implementar de manera efectiva la detección como código.

Reduce Risk Exposure

Reduzca su exposición al riesgo y a las brechas de cumplimiento

Libere el descubrimiento continuo de activos para mejorar la postura de cumplimiento y cerrar brechas en los controles de seguridad.

Simplify SecOps with AI

Simplifique la experiencia del analista con IA

Aumente su equipo SOC con IA para ayudar a los analistas con tareas rutinarias pero propensas a errores, como la redacción de resúmenes de investigación.

Unify TDIR

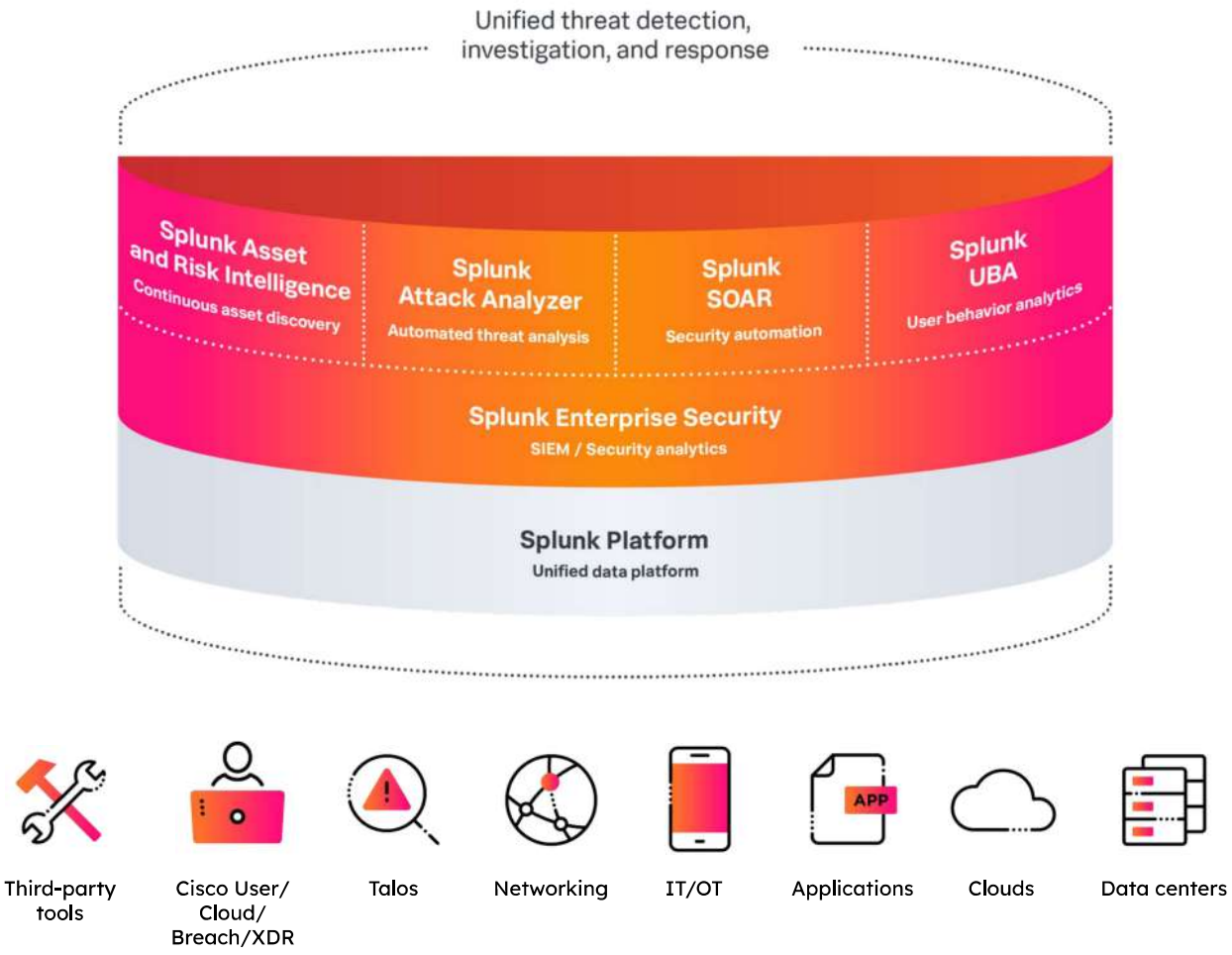
Unifique TDIR con flujos de trabajo automatizados

Coordine y colabore en todo el ciclo de vida de TDIR con flujos de trabajo automatizados utilizando manuales SOAR personalizados.

Impulsar el SOC del futuro

Splunk Security

Impulsando el SOC del futuro con la solución líder TDIR



Ofrecemos resultados de misión crítica como One Cisco.

AI-ready
data centers

Future-proofed
workplaces

Digital resilience

Accelerated by Cisco AI

Construyendo un camino hacia la resiliencia digital

Modernizándose para construir el SOC del futuro

Visibilidad Fundacional

Ver a través de entornos

Busque, monitoree e investigue para obtener información en tiempo real.

Perspectivas guiadas

Detectar amenazas y problemas con contexto

Reduce el ruido, detecta más amenazas e identifica riesgos.

Respuesta proactiva

Adelántese a los problemas

Acelere las investigaciones y respuestas ante incidentes utilizando automatización y análisis avanzados.

Flujos de trabajo unificados

Colaborar sin problemas

Maximice la eficiencia del SOC con detección, investigación y respuesta ante amenazas integradas.

Acelerado con Splunk AI

Organizaciones que transforman su SOC con Splunk

Johnson Matthey
Inspiring science, enhancing life

- Increased alert fidelity by 30%
- Reduced case management time by 83%
- 61% of phishing close by automation with SOAR

Case Study

Novuna

- $500K cost savings (in 8 months)
- 80K security events managed, controlled and contained by Splunk SOAR
- Seamless cross-platform integration

Case Study

PROGRESSIVE

- $120 billion in market capitalization protected
- Reduced noise in SOC significantly with risk-based alerting

Case Study

Soriana
TESCO
CAL POLY
REI co-op
Carnival
SINGAPORE AIRLINES
Aflac
Bank of England
GE
ebay
Fannie Mae
intel
HYATT
LOCKHEED MARTIN
SIEMENS
REGENERON
Nasdaq
VOLKSWAGEN
AKTIENGESELLSCHAFT

Splunk es reconocido como un líder en ciberseguridad

Ofreciendo una posición incomparable para impulsar el SOC del futuro

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

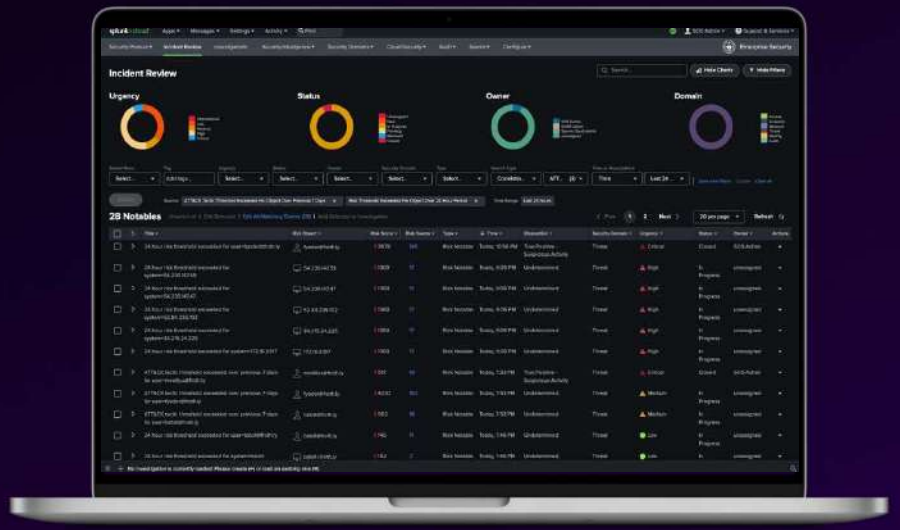
A leader in SOAR

Bring on the future.

Splunk Enterprise Security

Industry-defining security analytics solution trusted by SOCs globally

- **Gain comprehensive visibility** searching and analyzing any data at scale.
- **Get insights into risk** with customizable dashboards, visualizations, and reports.
- **Prioritize with context** using risk-based alerting to focus on imminent threats.
- **Detect threats faster** with over 1,700+ pre-built detections.
- **Effectively detect anomalies** and **unknown threats** with AI/ML.
- **Unify threat detection, investigation and response** using a modern work surface.
- **Build what you need** with custom apps and powerful integrations.



"Since implementing Splunk ES as the brain in our security nerve center, we have found Splunk to be the right solution to quickly and effectively create and implement security analytics across a wide array of data sources and security use cases."

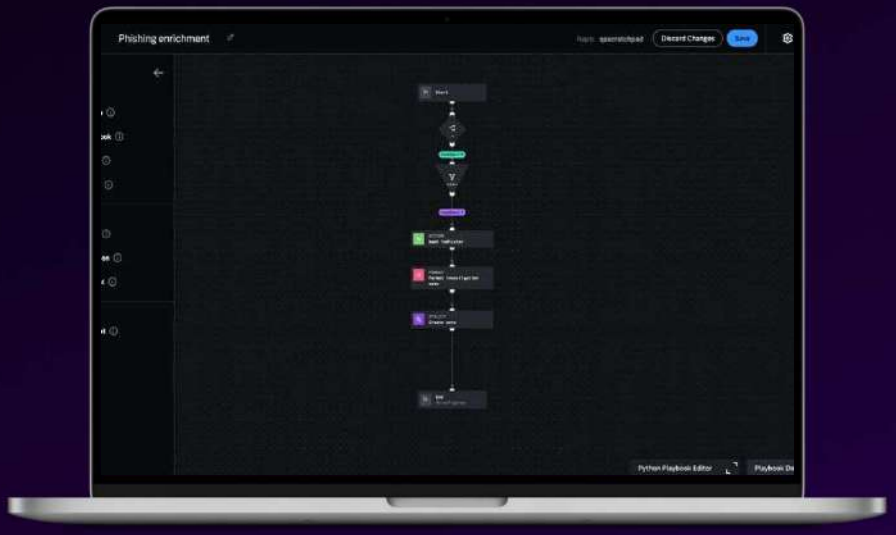
– Senior Vice President, Chief Global Security Officer, Aflac

Product Web Page - Product First Call Deck - Product Brief - Product Tour - Demo Video

Splunk SOAR

Work smarter by automating repetitive tasks, respond to security incidents in seconds, and increase analyst productivity.

- **Enhance team productivity** with automation for speed and efficiency.
- **Take prioritized actions** to act on the most pressing threats.
- **Respond with threat context** for common threats automatically.
- **Automate with ease** using pre-built playbooks, integrations, or build customized playbooks.
- **Get more out of your security stack** by orchestrating workflows across teams and tools.
- **Foster collaborative investigations** for a cohesive investigative process.
- **Actionize your data** by integrating SOAR with Splunk ES and Splunk Attack Analyzer.



"It's easy to send alerts directly from Splunk Enterprise Security to Splunk SOAR. Instead of spending hours looking into an incident, it can often be handled in just minutes."

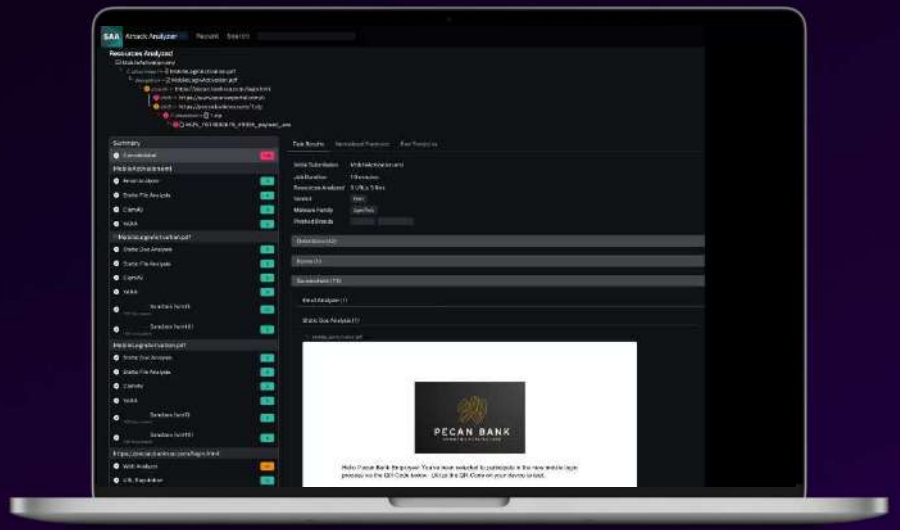
– Threat Detection Engineer, Tide

Product Web Page - Product First Call Deck - Product Brief - Product Tour - Demo Video

Splunk Attack Analyzer

Automatic analysis of active threats for contextual insights to accelerate investigations & resolution

- **Take the manual work out** of threat analysis and integrate into SOC workflows seamlessly.
- **Ensure a baseline standard** of investigation with consistent, comprehensive, and high-quality threat analysis.
- **Interact seamlessly** with malicious content in a dedicated, unattributable environment.
- **Achieve intelligent automation** for end-to-end threat analysis and response with easy integration with Splunk SOAR.
- **Enhance the analyst experience** by reducing the toil of threat analysis and free up valuable time.



"Splunk SOAR is able to take the outputs from Splunk Attack Analyzer and update the case management ticket with the results to provide the results of the analysis. This gets the information right where it needs to go – into the analyst's hands within minutes."

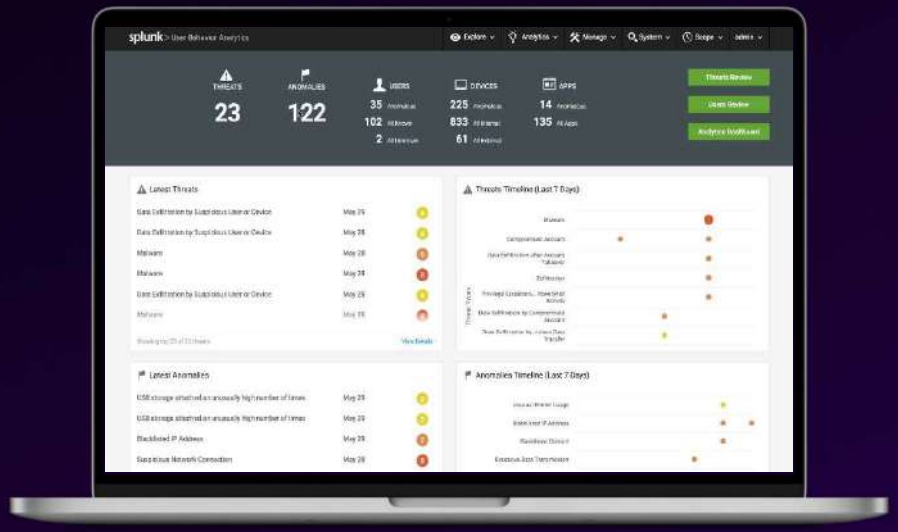
– Sr. Director, Global Security Operations, Splunk

Product Web Page - Product First Call Deck - Product Brief - Product Tour

Splunk User Behavior Analytics (UBA)

Detect unknown threats and anomalous behavior using machine learning

- **Detect and eliminate the most advanced threats** with multi-entity profiling and unsupervised ML
- **Enhance security visibility with rich contextual insights** so you can act decisively.
- **Visualize threats across multiple attack phases** to understand root cause, severity, and timelines.
- **Over 20 different dashboards** offer hundreds of permutations to view threat information and quickly form opinions on threat events.
- **Simplify incident investigations to increase SOC efficiency** and reduce MTTD and MTTR
- **Splunk UBA integrates workflows with Splunk Enterprise Security (SIEM)** for a wide-reaching defense against the most sophisticated threats



"Splunk UBA is giving us deep insight into our insider threat and what our trusted users are doing at any given instant."

– Associate Vice President, NASDAQ

Product Web Page - Product First Call Deck - Product Brief - Product Tour - Demo Video

Splunk Asset and Risk Intelligence (ARI)

Continuous asset and identity intelligence

- **Gain comprehensive asset visibility** to reduce risk exposure.
- **Accelerate security investigation** with accurate asset context.
- **Identify compliance gaps** in security controls.
- **Seamless integration and deployment** with Splunk Enterprise Security.
- **Get more out of your security stack** by orchestrating workflows across teams and tools.
- **Bridge the IT and Security gap** with seamless ServiceNow CMDB integration.

Product Web Page - Product First Call Deck - Product Brief

Security Expertise

Security content and threat research to help you stay ahead of threats.

- **Rapid response to empower blue teams** with the latest insights for high-profile security incidents.
- **Security research** with actionable guidance and recommendations.
- **Verified research and content** in the form of detection searches, use cases, and playbooks.
- **Powerful threat research tools** to test your detection searches against cyber attacks.