TRACE3 + splunk>

Splunk Enterprise Security

Access data-driven insights, combat threats, protect your business, and mitigate risk at scale with analytics you can act on.

Splunk Enterprise Security (ES) is a data-centric, modern security information and event management (SIEM) solution that delivers data-driven insights for full breadth visibility into your security posture so you can protect your business and mitigate risk at scale. With unparalleled search and reporting, advanced analytics, integrated intelligence, and pre-packaged security content, Splunk ES accelerates threat detection and investigation so you can quickly act.

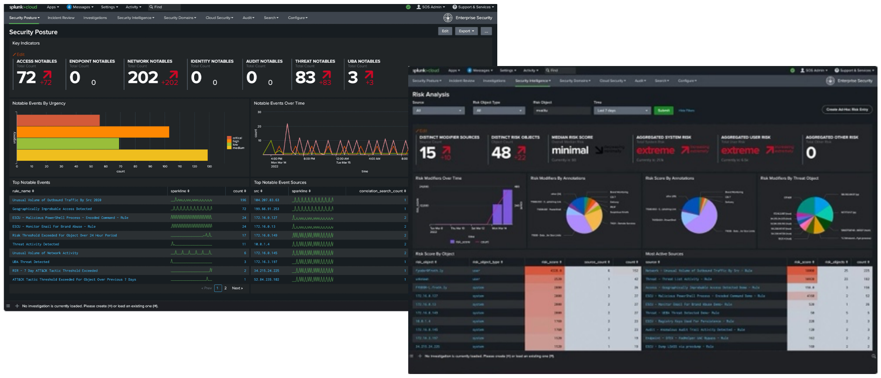
Trace3 + Splunk

Trace3's Security Observability services combines Splunk's Enterprise Security platform with expert thought leadership in solving business challenges through operational awareness and security visibility. Partnered with the Trace3 service delivery engineering team, we assess your current state, deploy, and implement the solution per your organization's unique environment and requirements, while utilizing Splunk and industry best practices to ensure delivered outcomes. Trace3 also has custom in-house developed applications available that can help you enrich your data and get even more out of your Splunk investment. The RAISE Situation and RAISE Framework apps provide data quality monitoring for your Splunk environment as well as identify security incidents that can be programmatically mapped to identities and hosts. As a Splunk Elite Sales & Services Partner, Trace3's expertise represents the highest standard for Splunk in advising, consulting, managing, and delivering.

Approach Methodology

With the combined power of Trace3 and Splunk, you can:

- Attribute risk to users and systems, map alerts to cybersecurity frameworks, then trigger alerts when risk exceeds thresholds to conquer alert fatigue
- Seamlessly align to CSF like MITRE ATT&CK, Kill Chain, CIS 18, and NIST
- Unlock the ability to ingest, normalize, & gain insights on any data and from any source
- Search & correlate across cloud, on-premises, or hybrid data sources
- 700 out-of-the-box customizable detections, over 100 being cloud-based



Security Posture

ACCESS NOTABLES	ENDPOINT NOTABLES	NETWORK NOTABLES	IDENTITY NOTABLES	AUDIT NOTABLES	THREAT NOTABLES	UBA NOTABLES
72 (+72)	0 (0)	202 (+202)	0 (0)	0 (0)	83 (+83)	3 (+3)

Top Notable Events

rule_name	count
Unusual Volume of Outbound Traffic By Src 2020	196
Geographically Improbable Access Detected	72
ESCU - Malicious PowerShell Process - Encoded Command - Rule	24
ESCU - Monitor Email For Brand Abuse - Rule	24
Risk Threshold Exceeded For Object Over 24 Hour Period	17
Threat Activity Detected	11
Unusual Volume of Network Activity	6
UBA Threat Detected	3
RIR - 7 Day ATT&CK Tactic Threshold Exceeded	2
ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days	1

Top Notable Event Sources

src	correlation_search_count
104.207.83.63	1
199.66.91.253	1
172.16.0.127	2
172.16.0.13	2
172.16.0.149	2
10.0.1.4	2
172.16.0.145	2
172.16.3.197	1
34.215.24.225	1
52.84.235.102	1

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Risk Analysis

DISTINCT MODIFIER SOURCES	DISTINCT RISK OBJECTS	MEDIAN RISK SCORE	AGGREGATED SYSTEM RISK	AGGREGATED USER RISK	AGGREGATED OTHER RISK
15	48	minimal	extreme	extreme	0

What You Can Expect

Defend against threats and provide high-fidelity alerts to shorten triage times and raise true positive rates.

Automatic security content updates delivered from the Splunk Threat Research Team help you stay on top of new & emerging threats.

Quickly pivot to the Investigation Workbench, which centralizes all threat intelligence, security context & relevant data, for fast & accurate assessments of incidents.

Easily monitor your environment through customizable dashboards such as: Executive Summary, Security Posture, SOC Operations, Incident Review, Risk Analysis, & Access Anomalies.

Adaptable Insights

Flexibility to customize correlation searches, risk-based alerts, reports, and dashboards to fit specific use cases.

Advanced Threat Detection

Improve detection of sophisticated threats like low-and-slow attacks that traditional SIEMs miss.

Adaptive Response Actions

Quickly launch an automated response to critical incidents and increase team productivity for repetitive tasks.

Prioritize Alerts

Accelerate investigations with built-in threat intelligence from Splunk Intelligence Management integration.