

Attack Surface Intelligence for Splunk

Discover and Defend Your Changing External Attack Surface



Challenge

As the scope of an organization's digital footprint expands, security teams must navigate a vast array of exposure points. By integrating Attack Surface Intelligence with existing security products, organizations can enhance their overall defense strategy with a dedicated focus on external vulnerabilities and assets. With comprehensive visibility, every asset and vulnerability is identified, providing the clarity needed to drive targeted remediation efforts. Seamless automation and integration reduce response times and enhance risk prioritization across the board. Ultimately, Attack Surface Intelligence transforms raw data into strategic actions, enabling your security team to stay ahead of emerging challenges.

Recorded Future Attack Surface Intelligence® offers continuous visibility into an organization's digital infrastructure, enabling proactive management of risks and vulnerabilities. The Splunk integration supports key use cases including Asset Discovery and Inventory, Risk Prioritization, and Continuous Monitoring, seamlessly enhancing analysts' workflows. It provides a detailed external asset inventory, visibility into exposure metrics, and real-time updates on new assets and risks, empowering security teams to prioritize mitigation efforts effectively. Comprehensive dashboards offer insights into top vulnerabilities, asset distributions, and exposure trends, ensuring informed risk management and swift incident response.

Benefits



Achieve proactive risk management by seamlessly integrating external asset inventory and exposure metrics into Splunk.



Prioritize and remediate vulnerabilities swiftly with real-time insights on asset discovery and exposure trends.



Enhance overall security posture through comprehensive dashboards that provide actionable intelligence on digital infrastructure.

Key Features:



Asset Discovery and Inventory Management



Risk Prioritization and Exposure Analysis

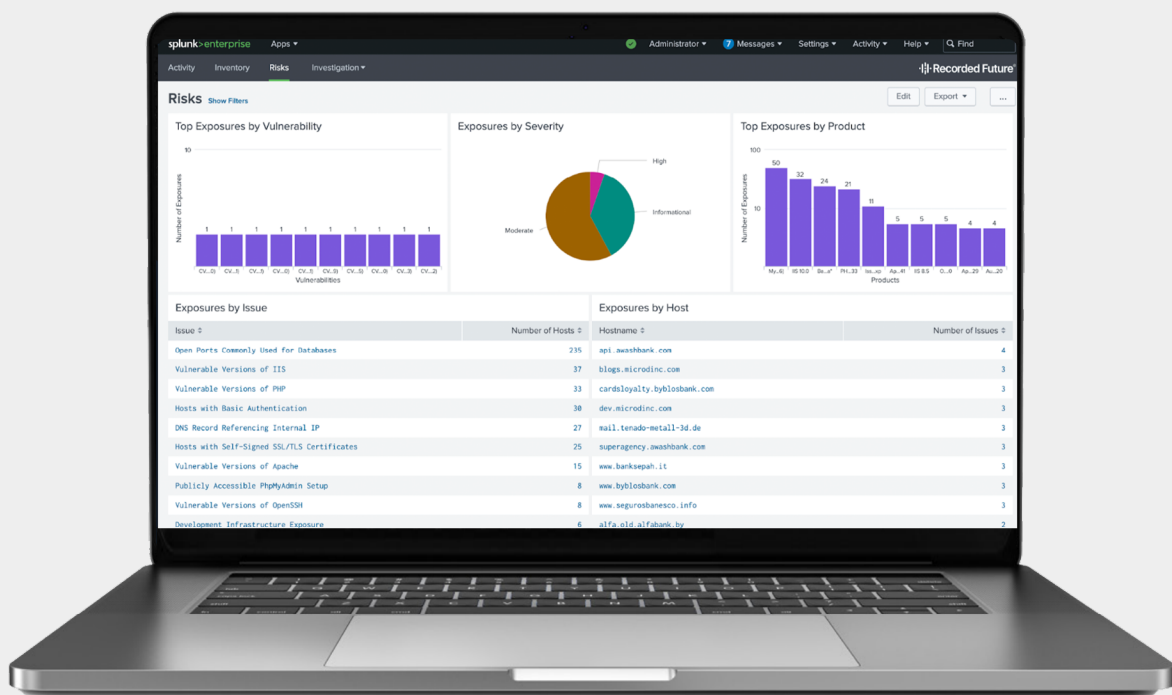


Continuous Monitoring and Activity Updates

Solution

The Recorded Future Attack Surface Intelligence (ASI) Add-on for Splunk empowers security teams with a persistent view of their organization's digital infrastructure, enabling proactive risk management and threat mitigation. By seamlessly integrating ASI data into the Splunk platform, security analysts can effectively discover assets, continuously monitor exposures, and prioritize risk mitigation efforts. This comprehensive visibility allows organizations to stay ahead of changes, abnormalities, and exploitable vulnerabilities, ensuring a robust security posture.

- 1. Asset Discovery and Inventory Management:** The ASI Add-on provides a detailed inventory of external-facing assets, enabling security teams to identify gaps in IT Asset Management and Vulnerability Management programs. This comprehensive view categorizes assets by hosting provider, IP address, open ports, country, hosting server, and certificate issuer.
- 2. Risk Prioritization and Exposure Analysis:** The integration empowers analysts to prioritize risk mitigation efforts by providing exposure information, including top exposed vulnerabilities, vulnerable IP addresses, and affected products.
- 3. Continuous Monitoring and Activity Updates:** Analysts receive updates on newly discovered assets and newly identified or cleared exposures.



Results



Increase visibility into your attack surface

Comprehensive asset inventory and exposure metrics provide full infrastructure visibility.



Accelerate exposure detection and response

Real-time updates enable swift incident response and proactive risk management.



Improve risk prioritization and decision-making

Detailed exposure insights help prioritize high-risk vulnerabilities efficiently.

ABOUT RECORDED FUTURE Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,900 businesses and government organizations across more than 80 countries to provide real-time, unbiased and actionable intelligence. Learn more at recordedfuture.com.