

Minimize the enterprise attack surface with Armis and SentinelOne

The challenge

Enterprise attack surfaces are growing exponentially as connected assets proliferate across networks. And while visibility has always been essential for managing security and IT operations, as environments become more complex, real-time visibility of every device on the network—including servers, workstations, IoT, OT, IoMT, mobile and cloud assets—has become paramount for maintaining a robust security posture.

The problem is that many types of IP-enabled assets, such as IoT and OT devices, can't be supported with EDR, patching, or vulnerability management initiatives due to operating system and other design constraints. Moreover, even IT assets may be missing or have misconfigured agents. And assets with internet-facing vulnerabilities are ripe for compromise by attackers looking for an easy door into a corporate network.

To eliminate cumbersome manual data-gathering and correlation efforts on overstretched security teams and better control the attack surface, CISOs are increasingly turning to extended detection and response (XDR) solutions. XDR is a comprehensive approach to security that combines multiple data types and sources to give analysts a complete picture of what is happening across an organization's attack surface. They combine the features of solutions for protecting endpoints, networks, the cloud, and other attack vectors into a comprehensive approach. And the most robust XDR approaches rely on unified visibility, deep asset intelligence, and real-time behavioral context to maximize protections.

Integration snapshot

The Armis integration for SentinelOne Singularity XDR integration provides:

- ▶ Real-time visibility of every IT, OT, IoT, IoMT, mobile and cloud asset in the enterprise
- ▶ Orchestrations that help accelerate threat response times
- ▶ Automations that reduce burdens on the security team

Key Benefits

- ▶ Gain unified visibility of assets and asset risk with consolidated visibility of managed and unmanaged assets that includes deep asset intelligence
- ▶ Accelerate triage by automatically enriching SentinelOne with Armis device and threat context to inform and accelerate investigation processes
- ▶ Reduce the attack surface by enriching Ranger asset fingerprinting with Armis context to understand and isolate unmanaged and potentially risky devices

The solution

Armis integration for SentinelOne Singularity XDR.

Armis and SentinelOne have partnered to deliver unified asset intelligence, threat enrichment, and attack surface reduction for enterprise security teams.

SentinelOne Singularity XDR unifies and extends protection, detection, investigation, and response capabilities across the entire enterprise, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automatable response across the technology stack. The Armis platform is the industry's most comprehensive asset intelligence platform, providing unified asset intelligence and superior security for organizations that need to protect against unseen operational and cyber risks, increase efficiencies, optimize use of resources, and safely innovate with new technologies to grow the business. Together, Armis and SentinelOne provide unparalleled XDR capabilities.

Armis learns and tags the specific use of every asset, including like devices used for different purposes. It also continuously maps connections and communications between assets and services, learning the relationships and dependencies between, and the importance of, assets across your environment. Through the Armis Collective Asset Intelligence Engine, the industry's first collective engine that tracks and analyzes attributes of over 2 billion assets worldwide, Armis even detects behavioral anomalies.

SentinelOne's patented Storyline observes all concurrent processes within all major operating systems and cloud workloads to connect dots between related events and activities to build further context. Distributed intelligence watches each Storyline to drive instantaneous protection against advanced attacks.

Overall, the integration enables unified, real-time visibility of every IT, OT, IoT, IoMT, mobile and cloud asset in the environment along with orchestrations that help accelerate threat response times and automations that reduce burdens on the security team so they can focus on complex security issues and proactive maintenance.

Gain unified visibility of assets and asset risk

SentinelOne enriches Armis with device metadata and application inventory for deep visibility into SentinelOne-managed endpoints. SentinelOne endpoints appear within the Armis console with real-time endpoint health, device characteristics, and application inventory. Broad coverage of device types between SentinelOne and Armis provides a real-time source of asset inventory and risk. Application inventory from SentinelOne feeds into the contextual risk scores in Armis (for example, notifying Armis of an endpoint with a vulnerable version of Adobe Flash). And context from SentinelOne Storyline complements Armis risk models to help you better understand, prioritize, and act on the most critical vulnerabilities in the environment.

The screenshot displays the Armis console interface. On the left, a sidebar contains navigation icons for Dashboard, Inventory, Alerts, Activity Log, Policies, Reports, and Settings. The main content area is titled 'LAB-5 Workstation 2' and shows a 'Medium' risk level with '0 Alerts'. Below this, it lists 'Personal Computers, Computers' as the Type/Category, 'Windows 10' as the OS, and 'Data sources' as a tag. The IP address is '10.65.52.174' and the MAC address is 'fe80:c0a3:5c6:8889:b89a'. The device is associated with the 'Corporate' boundary. The 'Last Seen' timestamp is 'Jul 28, 2022 12:27 PM'. The right pane shows a detailed view of the device with sections for Identifiers, Profile, Status, and OS / Firmware. The Identifiers section lists Name, Serial Number, Network Interfaces, Public IP, SentinelOne UUID, and SentinelOne Last Logged In User. The Profile section lists Type, Category, Model, Brand, and Purdue Level. The Status section lists Inventory Status, SentinelOne Health Status, SentinelOne Last Active, and SentinelOne Subscribed On. The OS / Firmware section lists Windows 10. The Other section is currently empty.

Identifiers	
Name	LAB-5 Workstation 2
Serial Number	—
Network Interfaces	(1 Interfaces)
Public IP	10.65.52.174
SentinelOne UUID	a4db08b7-5729-4ba9-8c08-f2df493465a1
SentinelOne Last Logged In User	Administrator

Profile	
Type	Personal Computers
Category	Computers
Model	ProDesk 600 G1 TWR
Brand	Hewlett Packard
Purdue Level	4.0

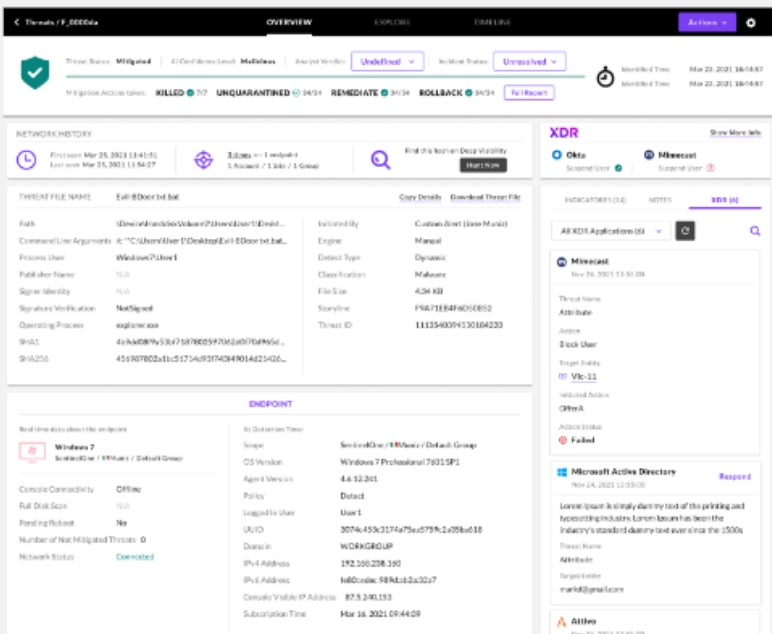
Status	
Inventory Status	Managed
SentinelOne Health Status	Healthy
SentinelOne Last Active	Oct 24, 2020 7:07 PM
SentinelOne Subscribed On	May 26, 2020 2:33 AM

OS / Firmware	
Windows 10	

Other	
-------	--

Accelerate threat response with XDR context enrichment

Automatically enrich SentinelOne-identified threat information with additional asset intelligence and context from Armis. The additional context consolidates the triage workflow, eliminating the need for security analysts to search across multiple consoles. Instead of wasting precious minutes, hours, or even days hunting down information security analysts can focus on rapid responses to attacks and minimizing damages.



Threat Status: Mitigated

Threat File Name: EulerDocBot.exe

Copy Details:


Field	Value
Path	\\Device\\Harddisk0\\Volume2\\Users\\User1\\Desktop\\EulerDocBot.exe
Process User	Windows7\\User1
File Size	434 KB
Signature Verification	Not Signed
Operating Process	explorer.exe
SHA1	45a4a0b9a53a7587605970a3a076a9a5d...
SHA256	45a307602a1a5173a937a0347014a23426...

Endpoint:

Field	Value
OS Version	Windows 7 Professional 7601 SP1
Agent Version	4.4.32.201
Policy	Default
Logged In User	User1
UUID	3074c453c217475a257932a258a018
Domain	WORKGROUP
IPv4 Address	192.168.238.190
IPv6 Address	fe80::c0a6:88d1:2a32:7
Console Validity IP Address	87.5.240.153
Subscription Time	Mar 16, 2021 09:44:09

Associated Devices:

Device Name	IP Address
Windows 7	192.168.238.190



May 5, 2022 4:01PM

Enrichment type
Correlated Armis alert

Matched on
IP 123.123.123.123
S1 Event ID 1234567, A123B56

Severity
High

Armis alert title
Krack attack detected

Type
Anomaly detection

Status
Unhandled

Time of alert
05, 30, 2021 17:03

Associated devices
11151, 13

[More](#)

Increase network visibility and control

SentinelOne Singularity Ranger provides visibility into unmanaged and potentially malicious devices (for example, user endpoints, servers, and IoT assets) on the network. Armis collects additional information on connected assets that can enrich and tag assets in Ranger with additional metadata. Context from Armis helps close visibility gaps and improve the quality of data within SentinelOne. With Ranger, admins can build policies to isolate or quarantine unmanaged devices from communicating with SentinelOne-managed endpoints. For example, admins can use tags applied by Armis to create policies in SentinelOne. If Armis tags an asset as an industrial control system (ICS), SentinelOne admins can isolate managed assets from directly communicating with the ICS asset to minimize the risk of lateral movement or malicious insider activity.

Take XDR to the next level with Armis and SentinelOne

With the Armis integration for SentinelOne Singularity XDR enterprises can leverage best-in-breed XDR and asset management solutions to power unified security workflows. Shared intelligence and context helps security teams reduce the attack surface while accelerating incident investigation and triage.

About Armis

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in San Francisco, California.

1.888.452.4011 | armis.com

20220425-1