Recorded Future®

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

DATA SHEET

Recorded Future for Cortex XSOAR

Elite Intelligence to Accelerate Investigation and Response

Today's ever-changing security landscape makes it nearly impossible for time-strapped security operations and incident response teams to mitigate every potential threat to their organization. Overwhelmed by manual processes and high alert volume, they're unable to take advantage of the breadth of intelligence available, instead they focus only on internal logs and data. Security teams need a platform that centralizes intelligence in real time and harnesses that information to drive action across security infrastructures.

To meet these challenges, Recorded Future empowers security teams with improved threat visibility and accelerated incident response. Integrating comprehensive, real-time intelligence into the security orchestration and automation features of Cortex XSOAR solves for the following use cases:

Threat Detection: The explosive growth of indicators makes detecting real threats extremely resource-intensive for already overwhelmed security teams. Recorded Future connects the dots between the broadest range of sources across every language. This intelligence and critical context enables Cortex XSOAR to automatically analyze and identify IOCs related to phishing attacks, malware, and command-and-control servers, empowering security teams to automate responses and reduce risk for the organization.

Alert Triage: With the Recorded Future and Cortex XSOAR integration, analysts see which alerts should be prioritized based on a real-time risk score that is backed by transparent evidence. An enrichment playbook automatically prioritizes alerts, quickly discounts false positives, identifies the most significant threats, and takes immediate action.

Threat Prevention: Armed with proprietary, evidence-based findings, organizations are able to automatically identify and block high-risk utilize IPs, URLs, hashes, and domains at the perimeter, minimize false positive blocking, automate incident response, and improve overall security posture.

Vulnerability Prioritization: Recorded Future provides necessary, real-time context around disclosed vulnerabilities based on the organization's technologies, industry, company, and more. By positioning direct access to evidence on the new and exploited vulnerabilities impacting their assets within Cortex XSOAR, organizations are enabled to produce deeper analysis and prioritize CVEs faster.

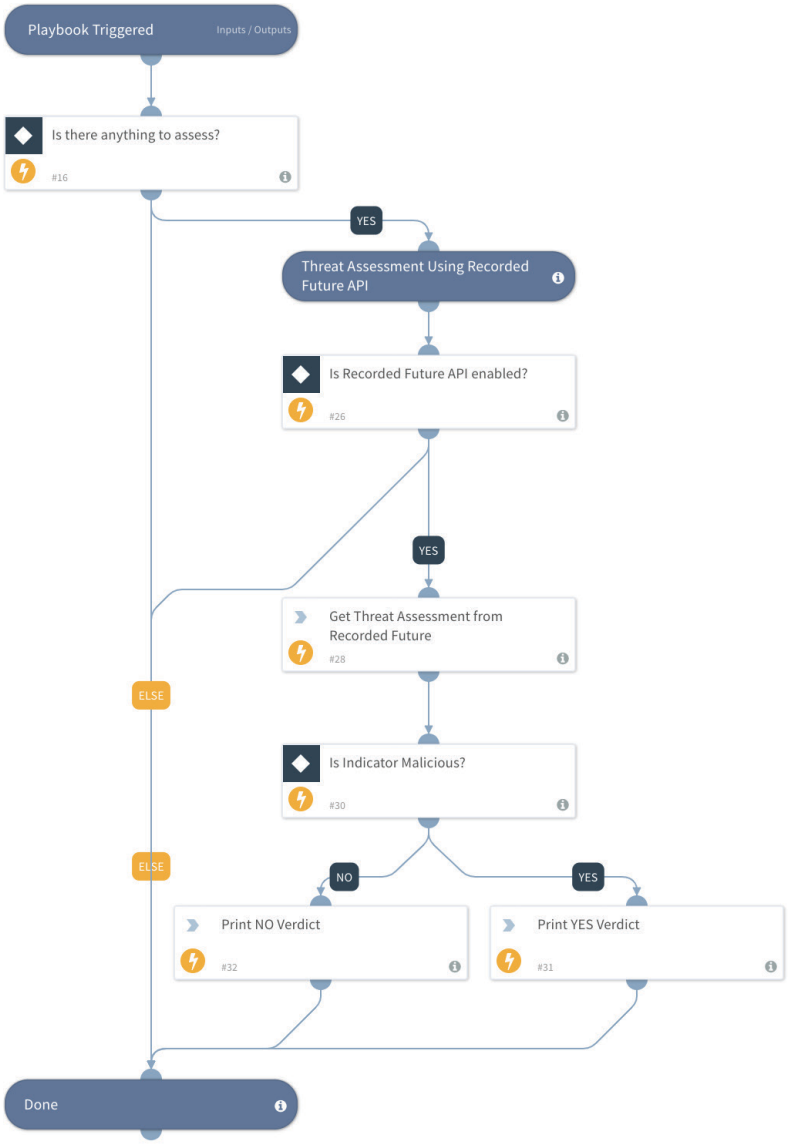
BENEFITS:

- Proactively block threats before they impact your business
- Automatically detect risky IOCs in your environment
- Triage alerts faster with elite, real-time intelligence
- Respond quickly with transparency and context around internal telemetry data
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation
- Shorten your decision-making cycle by automating key tasks with analyst reviews
- Maximize your security investment in Cortex XSOAR

COMPATIBILITY:
Cortex XSOAR, Recorded Future

Key Features

- Automate Recorded Future enrichment of IPs, URLs, domains, and file hashes as playbook-driven tasks within Cortex XSOAR
- Access related entities for an indicator in Recorded Future from Cortex XSOAR in real time
- Leverage hundreds of Cortex XSOAR product integrations to further enrich Recorded Future alerts and coordinate response across security functions
- Run thousands of commands — including commands for Recorded Future — interactively via a ChatOps interface, while collaborating with other analysts and Cortex XSOAR's chatbot



Recorded Future's threat assessment command identifies command-and-control incidents found in XSOAR.

Recorded Future®

About Recorded Future

Recorded Future delivers the world's most advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations. With proactive and predictive intelligence, Recorded Future's platform provides elite, context-rich, actionable intelligence in real time that's ready for integration across the security ecosystem.

Learn more at recordedfuture.com.

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

About Cortex XSOAR

Cortex XSOAR, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response time and analyst productivity.

For more information, visit paloaltonetworks.com/cortex/xsoar