

Recorded Future and Securaa

 Recorded Future®



PRODUCT OVERVIEW

Securaa is a Unified SecOps platform used in Cybersecurity Operations. Securaa blends intelligence, risk-based asset management, vulnerability details, automation, and incident response into one single platform. Through this, security operation centers (SOCs) are able to reduce response time significantly and risk to the environment.

Securaa provides complete visibility of threats to organizations using business-driven KRIs and KPIs. Securaa is suited for organizations that are security-focused and want a single platform to collect, manage, and respond to threats detected by existing security technologies like SIEM, firewalls, threat intelligence, and endpoint protection platforms.

JOINT INTEGRATION DESCRIPTION

Securaa uses Recorded Future's intelligence data to enrich alerts, vulnerabilities, and indicators of compromise (IOCs). Securaa also provides playbooks and tasks as part of the automation library to query the Recorded Future platform in real-time to make actionable decisions driven by intelligence. This capability automates manual tasks run by analysts and reduces false positives. These tasks are focused on intelligence lookups and threat hunting. Securaa powered by Recorded Future's intelligence, ensures that analysts focus on threats that matter to their organization.

CHALLENGES OVERCOME THROUGH INTEGRATION

Securaa and Recorded Future empower next-gen SOC's to fuse high-quality intelligence with incoming security issues and automate response. The security issues can range from alerts related to malicious activity on IT infrastructure reported by SIEM & other security systems and software vulnerabilities coming from scanners. Securaa consumes alert and vulnerability scan data from various systems and fuses it with Recorded Future's threat and vulnerability intelligence. This allows SOC's to focus on alerts and vulnerabilities that have a higher impact on IT infrastructure and ignore the noise. The response can be manual or automated based on the organization's security teams.

USE CASES

The fusion of Recorded Future's intelligence data in Securaa targets the following use cases:

Alert Triage: Securaa's SOAR component enriches incoming alerts with intelligence from Recorded Future on indicators that are part of the alert to reduce time to verdict.

Threat Response: Playbooks can use Recorded Future related tasks to make real-time decisions on remediation.

Threat Hunting: SecuraaTIP module downloads Recorded Future's intelligence feeds, called risklists, at predefined intervals. Securaa provides threat hunting playbooks that alert when this indicator is detected in real-time or in historical alert data.

Vulnerability Management: SecuraaAVM component fuses the vulnerability scan and vulnerability intelligence data from Recorded Future to prioritize remediation of known vulnerabilities.

BENEFITS:

- Complete visibility of threats to organizations using business-driven KRIs and KPIs.
- Automated tasks and reduced false positives
- Focus on alerts and vulnerabilities that have a higher impact on IT infrastructure and ignore the noise

Enrichment

Input	Field Name	Field Value
	IP Address	101.108.180.193

Output

Basic Details

Score	Risk String	Criticality	Risk Summary	Criticality Label	First Seen	Last Seen
24	503	1	6 of 53 Risk Rules currently observed.	Unusual	2019-04-10T18:57:48.6Z	2020-09-20T20:51:19.9Z

Intelligence Card

Evidence Details

State	Criticality Label	Mitigation String	Timestamp	Criticality
(+)	Unusual		2020-09-19T17:05:00Z	1
(+)	Unusual		2020-04-03T06:45:16.775Z	1
(+)	Unusual		2020-09-19T02:41:36Z	1

Sightings

Published	Type	Source	Title
(-)	recentEvent	Log.guru Forum	Passive nymex floods 4 proxy
(+)	first	PasteBin	Unlabeled Photo from PasteBin
(-)	recentPaste	PasteBin	ssosha42

Enrichment

Recorded Future Intelligence

Unprocessed 20-10-2020 01:37:23 PM 20-10-2020 01:07:24 PM

Visit Domain Reputation

Input	Field Name	Field Value
	Domain Name	securam.cz

Output

Basic Details

Score	Risk String	Criticality	Risk Summary	Criticality Label	First Seen	Last Seen
20	447	1	4 of 47 Risk Rules currently observed.	Unusual	2012-12-18T13:10:13.36Z	2020-10-20T03:25:22.075Z

Intelligence Card

Sightings

Published	Type	Source	Title
(-)	recentInfoSec	GitHub	1192-2020102713000.xml
(+)	recentPaste	PasteBin	F&Bv Czech - SecuramCZ
(-)	recentDarkWeb	Shill Market	Other ChatP's



About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.



About Securaa

Securaa is founded by industry veterans with over 100+ years of industry experience advising CXO globally on technology and cybersecurity initiatives. Securaa has offices in the US and India.