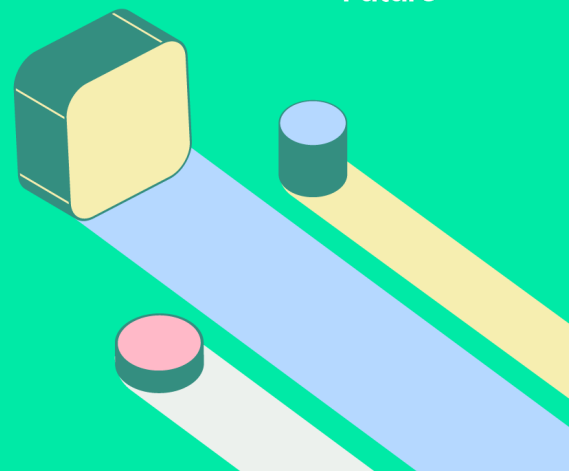


### *Solution brief*

# Vulcan Cyber and Recorded Future



## **The challenge**

Overwhelmed by a flood of vulnerabilities and the escalating sophistication of threats, security teams face an urgent need to prioritize risk measures based on contextual relevance and actionable intelligence, aligned with their business objectives and operational environment. Empowering proactive decision-making rooted in pertinent findings is imperative to navigate the evolving attack surface and reduce risk across it effectively.

## **Vulcan Cyber and Recorded Future - better together**

The Vulcan Cyber and Recorded Future integration delivers tailored threat intelligence aligned with specific business needs, ensuring relevance and actionability. It provides trustworthy data reflecting the organization's true risk, facilitating informed decision-making and resource allocation. Leveraging the Recorded Future comprehensive database of vulnerabilities and exploits, together with the Vulcan Cyber exposure operating system (ExposureOS), strengthens vulnerability risk management practices, enabling proactive identification and contextualized prioritization. With up-to-date insights on emerging threats, organizations can effectively minimize the risk of exploitation and potential threats.

## **Joint solution key features**

- **Threat risk score for each vulnerability:** Get a comprehensive threat risk score for every vulnerability, offering insights into the severity and potential impact of each security issue.
- **Filter and prioritize vulnerabilities efficiently:** Leverage Recorded Future's 'risk rules' prioritization method to filter and prioritize vulnerabilities based on their potential impact and likelihood of exploitation.

- **Risk-based patching prioritization:** Utilize a risk-based approach to prioritize patches and remediation actions.
- **Comprehensive threat intel coverage:** Access threat intelligence from diverse sources including the open web, dark web, expert research, and more.

## Use cases

- **Foster alignment between vulnerability management and incident response teams:** Enhance collaboration by ensuring both teams utilize consistent language and risk terminology in threat intelligence analysis and response efforts.
- **Access real-time and actionable intelligence:** Empower proactive exposure management and remediation with timely insights that enable swift and effective response to emerging threats.
- **Implement risk-based prioritization:** Extend beyond CVSS scoring by incorporating factors such as the likelihood of exploitation and relevant context for each vulnerability.

The screenshot displays the Vulcan interface for a specific vulnerability. The main content area shows an intelligence card for CVE-2017-7826, detailing its description, last seen date, risk score, and associated risk rules. A table lists these risk rules with their names, criticalities, and descriptions. The interface also includes a sidebar with navigation options and a right-hand panel for running campaigns.

**Intelligence Card: CVE-2017-7826**

- Description:** Memory safety bugs were reported in Firefox 56 and Firefox ESR 52.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox + 57, Firefox ESR + 52.5, and Thunderbird + 52.5.
- Last seen:** 2023-10-23T18:05:06.079Z
- Risk score:** 71
- Risk summary:** 4 of 23 Risk Rules currently observed.

Rule name	Criticality	Description
Linked to Historical Cyber Exploit	Low	1 sighting on 1 source: Lco. Most r...
Historically Linked to Penetration ...	Low	7 sightings on 4 sources: Sesin at, ...
Historically Referenced by Insiak Gr...	Low	1 sighting on 1 source: Insiak Grou...
NIST Severity: High	High	1 sighting on 1 source: Recorded F...

**Analyst Notes:**

- CVE-2017-7826 allows Memory Corruption affecting Mozilla Firefox

**VULCAN.** Unique Vulnerabilities Software Clusters CVE Clusters

Vulnerable (7,905) Fixed (1,639) Acknowledged (501) All

All Business Groups 99% 98% Filter Search By Name Export Take Action (0) ▼

Showing 1,526

Name	Where	Threats Tag	is	Recorded Future risk: CRITICAL	Recorded Future risk: HIGH	Recorded Future risk: MEDIUM	Remote	Security Feature Bypass	Security Misconfiguration	SLA Status	Business Groups
Path traversal in Mlflow				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Exceeding	
CVE-2023-29199				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2 Exceeding	
MFS42017-19 Firefox Security vulnerabilities fixed in Firefox 55 (CVE-2017-7779)				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Exceeding	Specific Asset L... Specific Assets...
CentOS Linux: CVE-2016-4658: Moderate: libxmi2 security update (CESA-201613816)				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Exceeding	Specific Asset L... Specific Assets...
MFS42017-24 Firefox Security vulnerabilities fixed in Firefox 57 (CVE-2017-7827)				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2 Exceeding	Specific Asset L... Specific Assets...

**VULCAN.** Hosts (83,557) Code Projects (1,047) Websites (50) Images (249) Cloud Resources (41,492)

35.5K 35.5K 10.9K 323 47 109

83.6K Hosts from 12 connectors

Scan Coverage 11.2K Unscanned hosts Found by: Microsoft TVM, AWS, ServiceNow, GCP

Vulnerability Breakdown 71.2K Vulnerable hosts 71.2K 6 5

Hosts per OS 71.6K 4.2K 2.5K 1.2K 660 541 480 34

All Business Groups Filter Search By Name Export Add Tag Tags

Showing 68

Name	Where	Threats Tag	is	Recorded Future risk: CRITICAL	Recorded Future risk: HIGH	Recorded Future risk: MEDIUM	Remote	Security Feature Bypass	Security Misconfiguration	Tags
ec2-3-128-131-227.us-east-2.comp.ite.amazonaws.com				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	groupy (more than 1200) Site Importance: (+1)
test-debian-11				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	asset_statestop... (public_facing)
ivanti-clent1	14.103.150.20			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cloud Agent (External Facing) groupy (more than 1200) (+3)
semexp_machine	172.31.30.215			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Name: semexp_machine asset_statestop...
test-machine	10.1.0.4			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	asset_statestop... (pa)
ivanti-Client2	52.246.252.53			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	groupy (more than 1200) Site Importance: (+1)
ec2-3-136-103-168.us-east-2.comp.ite.amazonaws.com	3.136.103.168			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	groupy (more than 1200) Site Importance: (+1)
Opus-kali-c2c	172.31.0.247			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Name: Opus-kali-c2c test: David.josh@vulca... asset_statestop... (+2) Asset Critical... Asset Location...

**VULCAN.** Connectors

<p><b>Detectify</b></p> <p>Last data ingestion: Fri, Jan 5, 2024, 11:02 PM Error Connecting</p>	<p><b>Rapid7</b></p> <p>Last data ingestion: Tue, Sep 5, 2023, 12:01 AM</p>	<p><b>Recorded Future</b></p> <p>Last data ingestion: Mon, Feb 19, 2024, 11:05 PM</p>
<p><b>Tenable.io</b></p> <p>Last data ingestion: Mon, Feb 19, 2024, 11:05 PM</p>	<p><b>Tenable.sc</b></p>	<p><b>Veracode</b></p> <p>Last data ingestion: Tue, Jan 23, 2024, 11:04 PM Error Connecting</p>
<p><b>WS DATA - GithubDependabot DON...</b></p> <p>Last data ingestion: Wed, Jan 10, 2024, 11:03 PM</p>	<p><b>2nd Test Proctor &amp; Gamble Vulc...</b></p> <p>Last data ingestion: Tue, Aug 22, 2023, 8:34 PM</p>	<p><b>AKAMI - Vulcan Report</b></p> <p>Last data ingestion: Sun, Jun 25, 2023, 11:19 AM</p>

## **About Recorded Future**

The Recorded Future Intelligence Platform delivers an end-to-end view of threats across the enterprise. At the core is the Intelligence Graph, with the world's most comprehensive reference data set, collected and curated over 10+ years, and continually enhanced.

## **About Vulcan Cyber**

Vulcan Cyber has developed the market-leading Exposure operating system (ExposureOS) to provide information security teams with one platform to prioritize, orchestrate, and mitigate exposure risk at scale throughout the entire attack surface.