

ServiceNow Reference Architecture

Capabilities and Use Cases

Created by: [Recorded Future Professional Services](#)

Published: August 2024

Updated: September 2024

Summary	2
Integration(s)	3
Security Incident Response / Threat Intelligence (SIR / TI).....	3
Key Feature(s).....	3
Required Module(s).....	3
Vulnerability Response (VR).....	3
Key Feature(s).....	3
Required Module(s).....	3
Vendor Risk Management (VRM).....	4
Key Feature(s).....	4
Required Module(s).....	4
IT Service Management (ITSM).....	4
Key Feature(s).....	4
Required Module(s).....	4
Use Cases	5
SIR/TI.....	6
Alert Triage.....	6
Observable Enrichment.....	8
Indicator Aggregation.....	10
VR.....	12
Vulnerability Calculator.....	12
CVE Enrichment.....	14
Attack Surface Dashboard.....	15
VRM.....	16
Vendor Assessment Dashboard.....	16
Company Enrichment.....	17
ITSM.....	18
ASI Alert Triage.....	18
Additional Reading	19
Professional Services Assistance	19

Summary

This reference architecture aims to give the reader an understanding of the capabilities achievable with the Recorded Future integrations into ServiceNow. This reference architecture is not a configuration guide. For configuration assistance or support, please contact professional services at Recorded Future.

Recorded Future maintains five ServiceNow integrations:

- ServiceNow Security Incident Response / Threat Intelligence (SIR/TI)
- ServiceNow Vulnerability Response (VR) via Recorded Future Vulnerability Module
- ServiceNow Vulnerability Response (VR) via Recorded Future Attack Surface Intelligence
- ServiceNow Vendor Risk Management (VRM)
- ServiceNow IT ServiceManagement (ITSM)

Each of these integrations depends but may not require a specific Recorded Future module. For example, SIR/TI can ingest Recorded Future TPI and Vulnerability alerts but does not require it. This document will outline which modules correspond to each integration and dive into the individual use cases. For installation documentation, contact your account manager or consultant.

Integration	SecOps Module	Threat Intelligence Module	Brand Module	Vulnerability Module	Third-Party Module	Attack Surface Module
SIR/TI	X	X	X	X	X	
VR				X		X
VRM					X	
ITSM						X

Integration(s)

This section gives the reader an understanding of the several Recorded Future-ServiceNow integrations. Recorded Future builds and maintains the following integrations into ServiceNow.

Security Incident Response / Threat Intelligence (SIR / TI)

ServiceNow Security Incident Response is an incident response management and ticketing system for security teams.

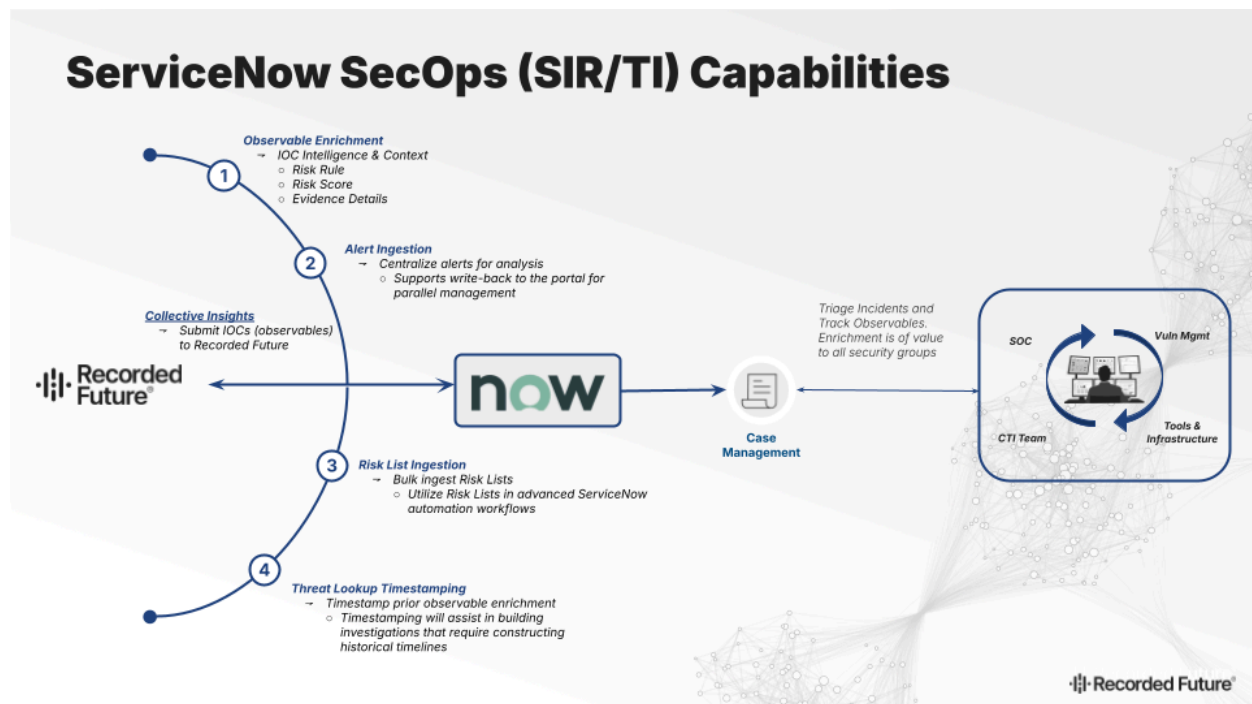
The Recorded Future for Security Incident Response / Threat Intelligence integration enables security operations teams to simplify their workflows, identify and contextualize incidents faster, and centralize their incident response within ServiceNow.

Key Feature(s)

- Ingestion of Recorded Future alerts and creation of SIR tickets with write-back support for alert status and alert notes.
- Enrich observables within SIR tickets.
- Bulk download Recorded Future risk lists.
- Aggregate Recorded Future IOC threat lookup results.
- Submit observables to Recorded Future Collective Insights.

Required Module(s)

- SecOps or Threat Intelligence (Risk Lists & Observable Enrichment)
- Brand Intelligence (Alerts)



ServiceNow SecOps Capabilities Overview

Vulnerability Response (VR)

Recorded Future for ServiceNow Vulnerability Response allows Vulnerability Management teams to incorporate Recorded Future vulnerability risk rules and risk scores into their patch management program.

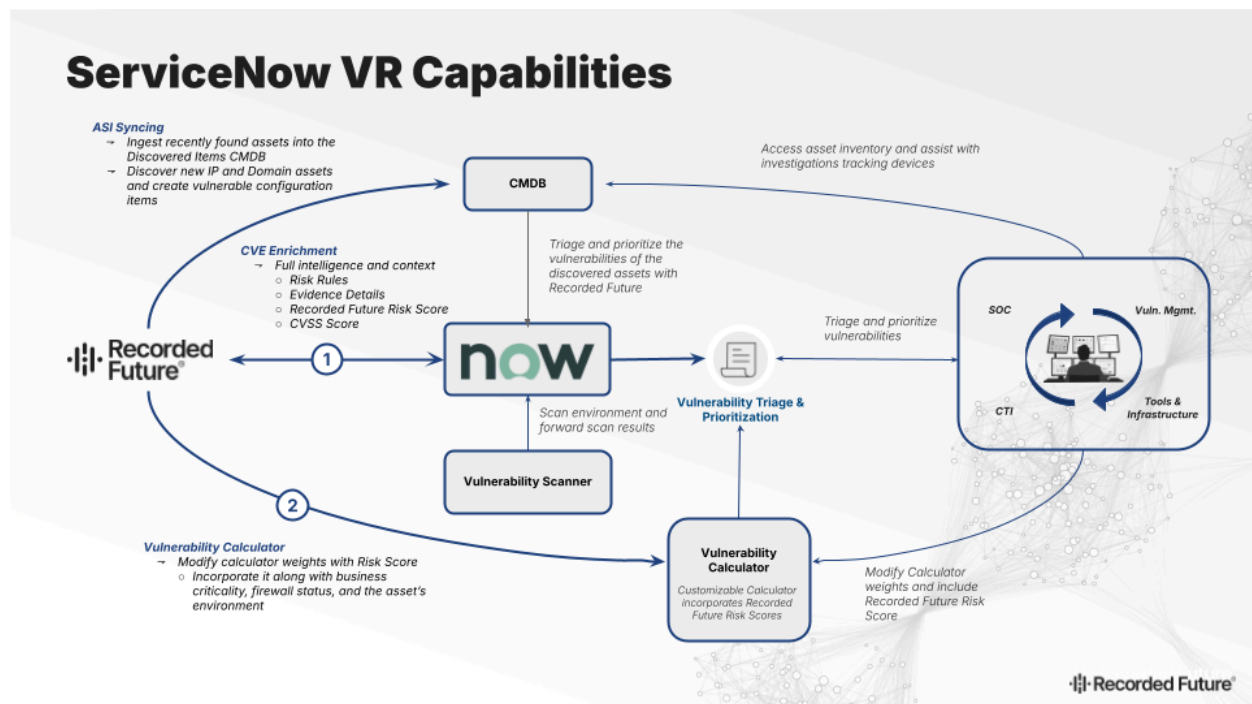
Additionally, Recorded Future ASI integrated into Vulnerability Response.

Key Feature(s)

- Threat-based risk scores for fast prioritization of vulnerabilities.
- Direct integration with the customizable ServiceNow vulnerability calculator.
- Customizable vulnerable items dashboard.

Required Module(s)

- Vulnerability Intelligence
- Attack Surface Intelligence (Not required. ASI complements ServiceNow Vulnerability Response)



ServiceNow VR Capabilities Overview

Vendor Risk Management (VRM)

Recorded Future for ServiceNow Vendor Risk Management allows third-party risk, governance risk and compliance, and vendor management teams to continuously monitor for risk intelligence on every organization in their Recorded Future third-party risk watchlist.

Key Feature(s)

- Dashboard of Recorded Future's third-party risk information
- Detailed evidence on risk rules
- Company enrichment

Required Module(s)

- Third-Party Intelligence

IT Service Management (ITSM)

Recorded Future for ServiceNow IT Service Management allows teams to continuously discover new assets and monitor exposure.

Key Feature(s)

- Ingest risk rule flagged ASI hosts as ITSM tickets.

Required Module(s)

- Attack Surface Intelligence

Use Cases

This section provides an overview of the use cases that Recorded Future builds, maintains and recommends for clients. Some use cases can be customized like dashboards or alert write-back.

For any custom use cases contact Professional Services at Recorded Future.

SIR/TI

This section provides an overview of use cases for Recorded Future within the ServiceNow Security Incident Response & Threat Intelligence integration.

Alert Triage

Timely alert triage is critical. The security gained by ingesting alerts like leaked credentials or domain abuse exposures as SIR tickets are dramatically higher when analysts are bound to SIR ticket SLAs.

Security Incidents Short description <input type="text" value="Search"/>					
All > Short description >= Recorded Future Cred					
<input type="checkbox"/> <input type="text" value="Search"/>	Number	Risk score	Priority	Assignment group	Short description ▲
	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>
	SIR0010011	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 1 reference
	SIR0010048	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 17 references
	SIR0010003	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 2 references
<input type="checkbox"/> ⓘ	SIR0010014	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 3 references
	SIR0010034	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 4 references
	SIR0010068	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 50 references
	SIR0010054	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 50 references
	SIR0010057	● 47	4 - Low	Security Incident Assignment	Recorded Future Credential Leak Alert: Leaked Credential Monitoring - 50 references

Recorded Future alerts ingested as Security Incidents

Security Incident SIR0010003		Discuss Follow Update Add Response Task Cancel Delete	
Incident Details Related Records MITRE ATT&CK Card Restriction			
Read access		Privileged access	
Watch list		Work notes list	
Description Leaked Credential Monitoring - 2 references Alert ID: ulaEi Triggered: 2024-01-13T13:04:44.687Z Targeted Credentials: Email: [REDACTED] Password: [REDACTED] Source: PasteBin Email: [REDACTED] Password: [REDACTED] Source: Nullified Forum Ingested observables: 3			

Recorded Future Leaked Credential Alert with compromised credentials

Recorded Future Alert Rules Create Security Inci Search						
All						
<input type="checkbox"/>	Active	Create Security Incident	Rule Name	Rule ID	Alert Category	Domain
<input checked="" type="checkbox"/>	true	true	Identify Typosquats	WhkPbn	Typosquat	global
<input checked="" type="checkbox"/>	true	true	Leaked Credential Monitoring	nBMJM_	Credential Leak	global
<input checked="" type="checkbox"/>	true	true	Domains on Code Repositories	nFFBJV	Default	global
<input checked="" type="checkbox"/>	true	true	Global Vulnerability Risk, New Critical ...	cJ8_9e	Default	global
<input checked="" type="checkbox"/>	true	false	Possible Fraud related to COVID-19	dQSUN	Default	global
<input checked="" type="checkbox"/>	true	false	Ransomware, Payment Sites and C&C Domains	fb3ICN	Default	global
<input checked="" type="checkbox"/>	true	false	TTP Monthly Metrics	jE-6Wt	Default	global
<input checked="" type="checkbox"/>	true	false	Global Vulnerability Risk, Vendors and P..	biQXYk	Default	global
<input checked="" type="checkbox"/>	true	false	Suppliers affected by COVID-19	dQJehr	Default	global

Note: Creating SIR tickets for alerting rules can be turned on or off

Alert write-back offers two flows: Transfer and Manage mode. Transfer mode is designed to migrate the management of a Recorded Future alert to ServiceNow. Manage mode is designed to parallel case management activity.

In the case of *transfer mode*, the Recorded Future portal alert will close. In the case of *manage mode*, the Recorded Future portal alert remains open in tandem with the newly created ServiceNow incident. The table below breaks down each mode.

Trigger	Transfer Mode	Manage Mode
A New Recorded Future alert is found.	<p>State is set to dismissed</p> <p>Note is added "ServiceNow SIR/TI: transferred, tracked in ##" where ## is the ServiceNow incident ID.</p>	<p>State is set to assigned</p> <p>Note is added "ServiceNow SIR/TI: transferred, tracked in ##" where ## is the ServiceNow incident ID.</p>
A ServiceNow incident based on a Recorded Future alert is closed.	<p>Note is added "ServiceNow SIR/TI: closed"</p>	<p>State is set to dismissed</p> <p>Note is added "ServiceNow SIR/TI: closed"</p>

Observable Enrichment

One of the main use cases for any automation platform is to automate enriching indicators with threat intelligence. Automating this process is practicable and will reduce cycle time for analysts when assessing the severity of incidents.

With Recorded Future, you can directly enrich observables within SIR tickets by bringing in risk scores, evidence details, related entities, geolocation data and more. This combination of intelligence allows analysts to perform remediation actions such as blocking the indicator on the firewall or kick-starting threat hunts based on related entities and research links.

Related Indicators	Associated Tasks (1)	Child Observables	Matching Resources for IP	Observable Sources	Security Annotations	Threat Lookup Results (1)	Observable Enrichment Results	MITRE ATT&CK Techniques	Analyst Notes
Locations (IP Addr) (1)	Related Entities (24)	Risk Evidence (9)	Sightings (4)	Threat Lists (3)	RF Threat Lookup Result (1)	Recorded Future Research Links	Recorded Future Technical Links (3)		
<div> <div>Retrieval date</div> <div>Search</div> </div> <div>Observable = 180.184.69.31</div>									
Retrieval date	Risk score	Criticality	Rules triggered	Total rules	First sighting	Most recent sighting	Intelligence Card		
2024-01-30	99	Very Malicious	9	75	2021-11-16 00:00:00	2023-11-09 00:00:00	https://app.recordedfuture.com/live/sc/entity/ip:180.184.69.31		

Recorded Future Risk Score, Criticality, and Intelligence Card link

Related Indicators	Associated Tasks (1)	Child Observables	Matching Resources for IP	Observable Sources	Security Annotations	Threat Lookup Results (1)	Observable Enrichment Results	MITRE ATT&CK Techniques	Analyst Notes
Locations (IP Addr) (1)	Related Entities (24)	Risk Evidence (9)	Sightings (4)	Threat Lists (3)	RF Threat Lookup Result (1)	Recorded Future Research Links	Recorded Future Technical Links (3)		
<div> <div>Organization name</div> <div>Search</div> </div> <div>Observable = 180.184.69.31</div>									
Organization name	City	Country	Continent	ASN	CIDR name	CIDR ID	CIDR type	Retrieval date	
Beijing Volcano Engine Technology Co., Ltd.		China	Asia	AS137718	180.184.64.0/18	ip:180.184.64.0/18	IpAddress	2024-01-30	

Recorded Future Geolocation Data

Related Indicators	Associated Tasks (1)	Child Observables	Matching Resources for IP	Observable Sources	Security Annotations	Threat Lookup Results (1)	Observable Enrichment Results	MITRE ATT&CK Techniques	Analyst Notes
Locations (IP Addr) (1)	Related Entities (24)	Risk Evidence (9)	Sightings (4)	Threat Lists (3)	RF Threat Lookup Result (1)	Recorded Future Research Links	Recorded Future Technical Links (3)		
<div> <div>Entity</div> <div>Search</div> </div> <div>Observable = 180.184.69.31</div>									
Entity	Type	Count	Retrieval date						
ec2-18-222-189-135.us-east-2.compute.ama...	InternetDomainName	1	2024-01-30						
vodafone.it	InternetDomainName	1	2024-01-30						
109.248.6.210	IpAddress	1	2024-01-30						
154.215.16.174	IpAddress	1	2024-01-30						
154.215.20.180	IpAddress	1	2024-01-30						
ec2-65-0-27-196.ap-south-1.compute.amazo...	InternetDomainName	1	2024-01-30						
20.151.239.27	IpAddress	2	2024-01-30						
Cobalt Strike	Malware	5	2024-01-30						
amazon.com	InternetDomainName	2	2024-01-30						
121.4.64.103	IpAddress	1	2024-01-30						
152.67.26.76	IpAddress	1	2024-01-30						
mtc.com	InternetDomainName	2	2024-01-30						
165.232.186.168	IpAddress	1	2024-01-30						
Remote Access Trojan	MalwareCategory	1	2024-01-30						
googleusercontent.com	InternetDomainName	1	2024-01-30						
5.188.34.118	IpAddress	2	2024-01-30						
Cobalt Strike Beacon	Malware	2	2024-01-30						
Offensive Security Tools (OST)	MalwareCategory	5	2024-01-30						
101.42.169.90	IpAddress	1	2024-01-30						
Pupy RAT	Malware	1	2024-01-30						

Recorded Future Related Entities

Related Indicators	Associated Tasks (1)	Child Observables	Matching Resources for IP	Observable Sources	Security Annotations	Threat Lookup Results (1)	Observable Enrichment Results	MITRE ATT&CK Techniques	Analyst Notes
Locations (IP Addr) (1)	Related Entities (24)	Risk Evidence (9)	Sightings (4)	Threat Lists (3)	RF Threat Lookup Result (1)	Recorded Future Research Links	Recorded Future Technical Links (3)		
<div> <div>Rule name</div> <div>Search</div> <div>⊗</div> <div>Actions on selected rows...</div> </div>									
Observable = 180.184.69.31									
<input type="checkbox"/>	Rule name	Description	Criticality	Timestamp	Mitigation	Retrieval date			
<input type="checkbox"/>	Historically Reported by DHS AIS	15 sightings on 1 source: DHS Automated ...	Unusual	2023-09-27 00:00:00		2024-01-30			
<input type="checkbox"/>	Historically Reported in Threat List	Previous sightings on 2 sources: Recent...	Unusual	2024-01-30 00:00:00		2024-01-30			
<input type="checkbox"/>	Historically Linked to Intrusion Method	6 sightings on 2 sources: Twitter, Recor...	Unusual	2023-11-09 00:00:00		2024-01-30			
<input type="checkbox"/>	Recently Communicating Validated C&C Server	1 sighting on 1 source: Recorded Future ...	Suspicious	2024-01-25 00:00:00		2024-01-30			
<input type="checkbox"/>	Validated C&C Server	4 sightings on 1 source: Recorded Future...	Very Malicious	2024-01-30 00:00:00		2024-01-30			
<input type="checkbox"/>	Historically Reported as a Defanged IP	3 sightings on 2 sources: redpacketsecur...	Unusual	2023-05-05 00:00:00		2024-01-30			
<input type="checkbox"/>	Historically Reported C&C Server	65 sightings on 2 sources: Recorded Futu...	Suspicious	2023-05-19 00:00:00		2024-01-30			
<input type="checkbox"/>	Previously Validated C&C Server	529 sightings on 1 source: Recorded Futu...	Suspicious	2024-01-28 00:00:00		2024-01-30			
<input type="checkbox"/>	Historical Suspected C&C Server	52 sightings on 3 sources: ThreatFox Inf...	Unusual	2023-11-09 00:00:00		2024-01-30			
<div> <div><<</div> <div><</div> <div>1 to 9 of 9</div> <div>></div> <div>>></div> </div>									

Recorded Future Risk Evidence (Risk Rules) Details

Related Indicators	Associated Tasks (1)	Child Observables	Matching Resources for IP	Observable Sources	Security Annotations	Threat Lookup Results (1)	Observable Enrichment Results	MITRE ATT&CK Techniques	Analyst Notes
Locations (IP Addr) (1)	Related Entities (24)	Risk Evidence (9)	Sightings (4)	Threat Lists (3)	RF Threat Lookup Result (1)	Recorded Future Research Links	Recorded Future Technical Links (3)		
<div> <div>Name</div> <div>Search</div> <div>⊗</div> <div>Actions on selected rows...</div> </div>									
Observable = 180.184.69.31									
<input type="checkbox"/>	Name	Category	Type	Start date	Stop date	Score			
<input type="checkbox"/>	146.70.111.92	Victims & Exploit Targets	IpAddress	2024-01-24	2024-01-30	28			
<input type="checkbox"/>	Cobalt Strike	Actors, Tools & TTPs	Malware	2024-01-24	2024-01-30				
<input type="checkbox"/>	Cobalt Strike Beacon	Actors, Tools & TTPs	Malware	2024-01-24	2024-01-30				
<div> <div><<</div> <div><</div> <div>1 to 3 of 3</div> <div>></div> <div>>></div> </div>									

Recorded Future Technical Links

Additionally, Collective Insights can be enabled when setting up the SIR/TI integration which will submit every enriched indicator within incidents to be sent back to Recorded Future. These collective insights submissions empower the SecOps dashboard and the Malware Threat Map in the Threat Intelligence Module.

SIR - Observable Enrichment

SIR - Alerts

SIR - Risk Lists

VR - Risk Lists

VR - Calculator

VRM - API settings

Auto-update observable ☐

API re-query hours

Collective Insights ☒

Recorded Future Collective Insights

Indicator Aggregation

Besides managing incidents and their nested observables, the ServiceNow SIR/TI integration can also aggregate and store IOCs from prior Recorded Future enrichment calls (threat lookups).

Timestamping when an observable threat lookup happens allows analysts to search for historically seen observables, including first and most recent time stamps. Allowing analysts to observe an IOC at a set time will assist in building investigations that require constructing historical timelines.

Prior enrichment lookups are stored in the threat lookup results.

Recorded Future Threat Lookup Results View: RF Observable Data type Search Actions on selected rows									
All	Data type	Observable	Risk score	Criticality	Rules triggered	Total rules	First sighting	Most recent sighting	Intelligence Card
	Threat Lookup Result	slice.vanilla.futurecdn.net	0	0	0	53	2020-09-03 00:00:00	2024-01-13 00:00:00	https://app.recordedfuture.com/live/sc/entity/idslice.vanilla.futurecdn.net
	Threat Lookup Result	order.seller.id	0	0	0	53	2018-06-13 00:00:00	2024-01-25 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsorder.seller.id
	Threat Lookup Result	252fd1e0ek4ebabms.cloudfront.net	0	0	0	53	2022-09-29 00:00:00	2024-01-14 00:00:00	https://app.recordedfuture.com/live/sc/entity/ids252fd1e0ek4ebabms.cloudfront.net
	Threat Lookup Result	safebrowsing.google.com	5	Unusual	1	53	2013-09-23 00:00:00	2024-01-12 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsafebrowsing.google.com
	Threat Lookup Result	https://www.recordedfuture.com/	0	0	0	35	2023-12-22 00:00:00	2023-12-22 00:00:00	
	Threat Lookup Result	app.recordedfuture.com	5	Unusual	1	53	2016-05-11 00:00:00	2024-01-22 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsapp.recordedfuture.com
	Threat Lookup Result	sendgrid.net	24	Unusual	5	53	2013-09-24 00:00:00	2024-01-12 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsendgrid.net
	Threat Lookup Result	seelp.org	0	0	0	53	2018-08-18 00:00:00	2024-01-12 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsseelp.org
	Threat Lookup Result	img.promio-connect.com	0	0	0	53	2019-12-12 00:00:00	2024-01-30 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsimg.promio-connect.com
	Threat Lookup Result	180.184.69.31	99	Very Malicious	9	75	2021-11-16 00:00:00	2023-11-09 00:00:00	https://app.recordedfuture.com/live/sc/entity/ips180.184.69.31
	Threat Lookup Result	recordedfuture.com	5	Unusual	1	53	2011-12-29 00:00:00	2024-01-22 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsrecordedfuture.com
	Threat Lookup Result	api.recarga.com	0	0	0	53	2017-12-14 00:00:00	2024-01-16 00:00:00	https://app.recordedfuture.com/live/sc/entity/idsapi.recarga.com

Threat Lookup Results

Additionally, the SIR/TI integration enables analysts to bulk upload Recorded Future risk lists, allowing analysts to freely browse and lookup any ingested indicator within the Observables table.

SIR - Observable Enrichment
SIR - Alerts
SIR - Risk Lists
VR - Risk Lists
VR - Calculator
VRM - API settings

Recorded Future Risk List Configs

Risk List	Active	Frequency (Hours)	Last load time
+			

Update
Delete

Configure and Ingest Risk Lists

Recorded Future SIR Risk List dropdowns

Name

Search

All

Name

- Credentials/Bruteforce attacks;Indicators Found in Honeypots
- Credentials/Bruteforce attacks;Traffic From Connections (IPs) Linked to Malware
- Default domain risklist
- Default domain risklist (Qradar)
- Default domain risklist hourly
- Default hash risklist
- Default hash risklist (Qradar)
- Default hash risklist hourly
- Default IP risklist
- Default IP risklist hourly
- Default url risklist
- Default url risklist (Qradar)
- Default url risklist hourly
- Default vulnerability risklist
- Default vulnerability risklist hourly
- General;Indicators Frequently Linked to Malware
- Insider Threat;Network Devices Using TOR to Anonymize Traffic
- Large domain risklist
- Large hash risklist
- Large IP risklist

1 to 20 of 85

Library of Recorded Future Risk Lists

VR

This section provides an overview of use cases for Recorded Future within the ServiceNow Vulnerability Response integration.

Vulnerability Calculator

The Vulnerability calculator is a ServiceNow function that calculates a vulnerable item's ServiceNow risk score. This risk score is part of the Vulnerable Items table and is distinct from the Recorded Future risk score, although it will incorporate it along with business criticality, firewall status, and the asset's environment.

The risk score for vulnerable items is recalculated regularly by a scheduled job, and it is possible to trigger a recalculation of all items of a single vulnerable item on demand.

Without threat intelligence and relying only on business criticality or other environment variables, teams cannot truthfully assess the severity of vulnerable assets. Therefore, the ServiceNow VR risk calculator incorporates Recorded Future intelligence to represent the risk severity accurately.

These weights can be modified to weigh clients' most prioritized attributes. However, the weights must always sum to 100.

Risk Calculator Criteria

Set the weight for each parameter according to its importance in the overall risk score calculation. Add any other fields using 'Add Criteria' button and set the field level weightage to calculate the risk for Vulnerability items.

Risk rule fields				⊙	⏪	⏩	1 to 8 of 8	⏴	⏵	—
Field name	Table	Weight	Weight breakdown/Condition							
✕ Vulnerability Exploit skill level	Vulnerable Item [sn_vul_vulnerable_item]	0	Default : 50 , Novice : 100 , Intermediate : 50 , Expert : 0							
✕ Service Business criticality	Related Services [sn_vul_m2m_ci_services]	10	Default : 0 , Empty String : 0 , 1 - most critical : 100 , 2 - somewhat critical : 75 , 3 - less critical : 50 , 4 - not critical : 25							
✕ Vulnerability Exploit attack vector	Vulnerable Item [sn_vul_vulnerable_item]	0	Default : 50 , Remote : 100 , Local : 0							
✕ Firewall status	Server [cmdb_ci_server]	15	Default : 50 , Empty String : 50 , Internet : 100							
✕ Recorded Future Risk Score	National Vulnerability Database Entry [sn_vul_nvd_entry]	55	Default : 0 , Empty String : 0 , 0 : 0 , 1-10 : 10 , 11-20 : 20 , 21-30 : 30 , 31-40 : 40 , 41-50 : 50 , 51-60 : 60 , 61-70 : 70 , 71-80 : 80 , 81-90 : 90 , 91-99 : 100							
✕ Vulnerability Severity	Vulnerable Item [sn_vul_vulnerable_item]	0	Default : 50 , 1 - Critical : 100 , 2 - High : 75 , 3 - Medium : 50 , 4 - Low : 25 , 5 - None : 0							
✕ Vulnerability Exploit exists	Vulnerable Item [sn_vul_vulnerable_item]	0	Default : 50 , Yes : 100 , No : 0							
✕ Environment	Server [cmdb_ci_server]	20	Default : 50 , Empty String : 50 , Production : 100							

VR Calculator Weights

The table below explains the calculator weights:

Attribute	Attribute Entry	Risk Calculation	Weight
Recorded Future Risk Score	0-99	0 - 100	55%
Business Criticality	1 - Most critical	100	10%
	2 - Somewhat critical	75	
	3 - Less critical	50	
	4 - Not critical	25	
	No criticality set	0	
Firewall Status	Internet Facing = TRUE	100	15%
	Internet Facing = FALSE	25	
Environment	Production	100	20%
	Test, Development, Other (including empty or null)	50	

The below weights are the default values but are easily customizable.

- **Recorded Future Score: Weighted 55**

The Recorded Future Score considers the threat of exploitation and is weighted the highest because it accounts for how weaponized a CVE has become. If multiple Risk Scores are associated with the VIT (because there are several CVEs associated with the VIT), then the highest Risk Score is used for this field. Recorded Future provides Risk Scores between 0 and 99, but within ServiceNow VR, the calculator rounds up to the nearest multiple of 10. So a Risk Score of 51 rounds up to 60, and a Risk Score of 99 rounds up to 100.

- **Business Criticality: Weighted 10**

Business Criticality is subjective to the business and is weighted lower since the asset could be more critical to one group vs. another. However, it still provides valuable context to the asset.

- **Firewall Status: Weighted 15**

Whether the Firewall status of the asset is public or private will impact how easy it is for an attacker to access the asset in question.

- **Environment: Weighted 20**

The environment in which the vulnerability exists is critical to understanding the potential impact. If in production, it can affect your company and your customers; if it's in development, this is less harmful to customers but could impact business operations.

Recorded Future cannot provide internal risk calculation. Therefore, Business Criticality, Firewall Status, and Environment augment the risk score based on environmental factors.

CVE Enrichment

Once the vulnerability calculator is configured to incorporate Recorded Future risk scores, teams can take the next step by incorporating Recorded Future's evidence details into the triage process.

In larger environments, when inundated with vulnerable assets, patching often requires justification beyond a numerical risk score. Recorded Future provides this information within ServiceNow VR by including additional evidence details within the Vulnerable Item (VIT).

Remediation Tasks (1)

Affecting Tasks

Impacted Services (2)

State Change Approvals

Recorded Future VR Risk Evidence (8)

Recorded Future VR Risk Score (1)

Recorded Future CVEs (1)

Criticality

Search

—

Actions on selected rows...

Recorded Future Vulnerability Risk Evidences

<div><input type="checkbox"/></div> <div><div></div></div> <div>Vulnerability entry</div>	Criticality	Rule	Evidence string	Timestamp
<div>CVE-2013-2460</div>	<div><div></div><div>Very Critical</div></div>	Exploited in the Wild by Recently Active...	23 sightings on 1 source: Recorded Futur...	2024-07-06 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Critical</div></div>	NIST Severity: Critical	1 sighting on 1 source: Recorded Future ...	2024-04-29 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Medium</div></div>	Historical Verified Proof of Concept Ava...	1 sighting on 1 source: ExploitDB. 1 exe...	2013-07-01 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Low</div></div>	Historically Linked to Malware	37 sightings on 10 sources including: ta...	2024-04-21 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Low</div></div>	Historically Reported by Insikt Group	1 sighting on 1 source: Insikt Group. 1 ...	2021-06-29 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Low</div></div>	Historically Linked to Exploit Kit	5 sightings on 4 sources: ToolBase Germa...	2021-06-29 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Low</div></div>	Historically Linked to Penetration Testi...	1 sighting on 1 source: Gerki Forum.	2022-12-21 00:00:00
<div>CVE-2013-2460</div>	<div><div></div><div>Low</div></div>	Linked to Historical Cyber Exploit	24 sightings on 7 sources including: Too...	2021-03-23 00:00:00

1 to 8 of 8

Recorded Future Risk Evidence Details

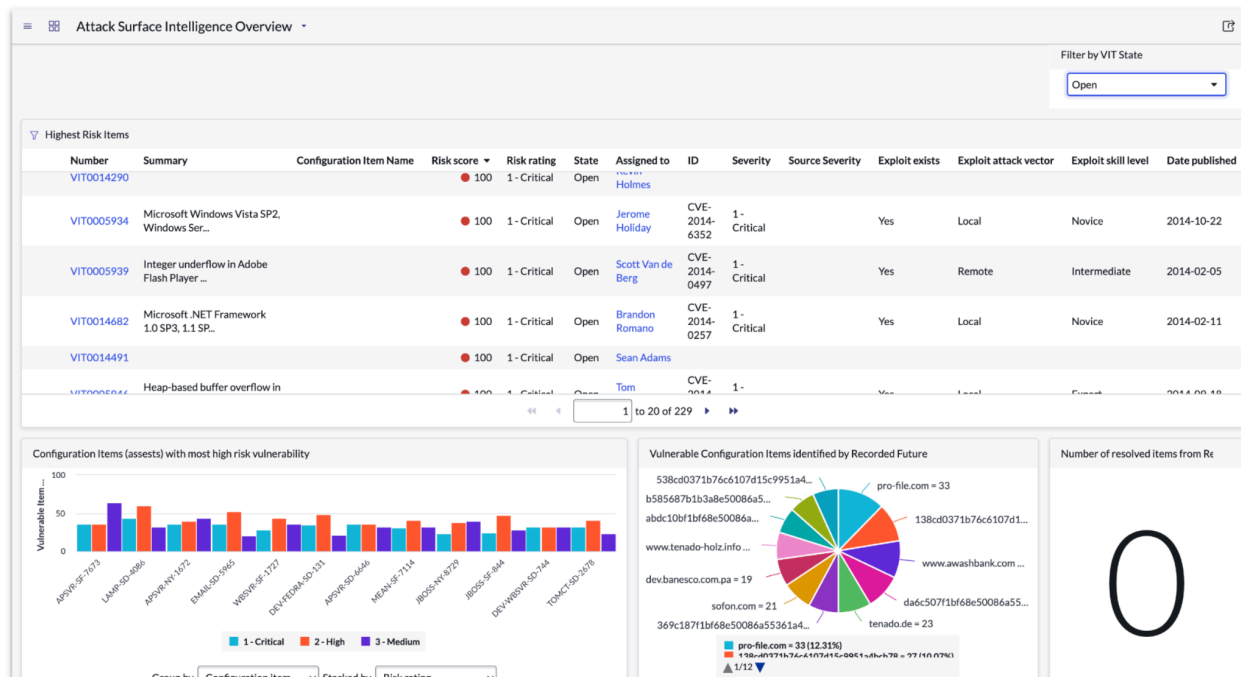
<div> Vulnerable Item VIT0001782 </div> <div> Configuration item QA-JBOSS-SD-2839 </div> <div> Reopen Delete </div>																																
<div> Vulnerability Remediation Steps Initial Detection Detections Close Notes </div> <div> <div> Summary Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object, as exploited in the wild in October 2014 with a crafted PowerPoint document. </div> <div> <div> Severity 1 - Critical </div> <div> Vulnerability score (v3) </div> <div> Vulnerability score (v2) 9.3 </div> </div> <div> <div> Threat </div> <div> Remediation notes </div> </div> <div> Reopen Delete </div> </div>																																
<div> Remediation Tasks (1) Affecting Tasks Impacted Services (5) State Change Approvals Recorded Future VR Risk Evidence (11) Recorded Future VR Risk Score (1) Recorded Future CVEs (1) </div> <div> <div> Risk score Search </div> <div> Recorded Future Vulnerability Risk Scores </div> <table> <thead> <tr> <th><input type="checkbox"/></th><th>Criticality label</th><th>CVE ID</th><th>Cvss score</th><th>Intel card</th><th>Malware activity</th><th>Recent malware activity</th><th>Risk score</th><th>Rules triggered</th><th>Domain</th><th>Threat sco</th></tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td><td>Very Critical</td><td>CVE-2014-6352</td><td>9.3</td><td>https://app.recordedfuture.com/live/sc/entity/LOR5EC</td><td>0</td><td>1</td><td>99</td><td>11</td><td>global</td><td></td></tr> </tbody> </table> <div>1 to 1 of 1</div> </div>											<input type="checkbox"/>	Criticality label	CVE ID	Cvss score	Intel card	Malware activity	Recent malware activity	Risk score	Rules triggered	Domain	Threat sco	<input type="checkbox"/>	Very Critical	CVE-2014-6352	9.3	https://app.recordedfuture.com/live/sc/entity/LOR5EC	0	1	99	11	global	
<input type="checkbox"/>	Criticality label	CVE ID	Cvss score	Intel card	Malware activity	Recent malware activity	Risk score	Rules triggered	Domain	Threat sco																						
<input type="checkbox"/>	Very Critical	CVE-2014-6352	9.3	https://app.recordedfuture.com/live/sc/entity/LOR5EC	0	1	99	11	global																							

Recorded Future Risk Score

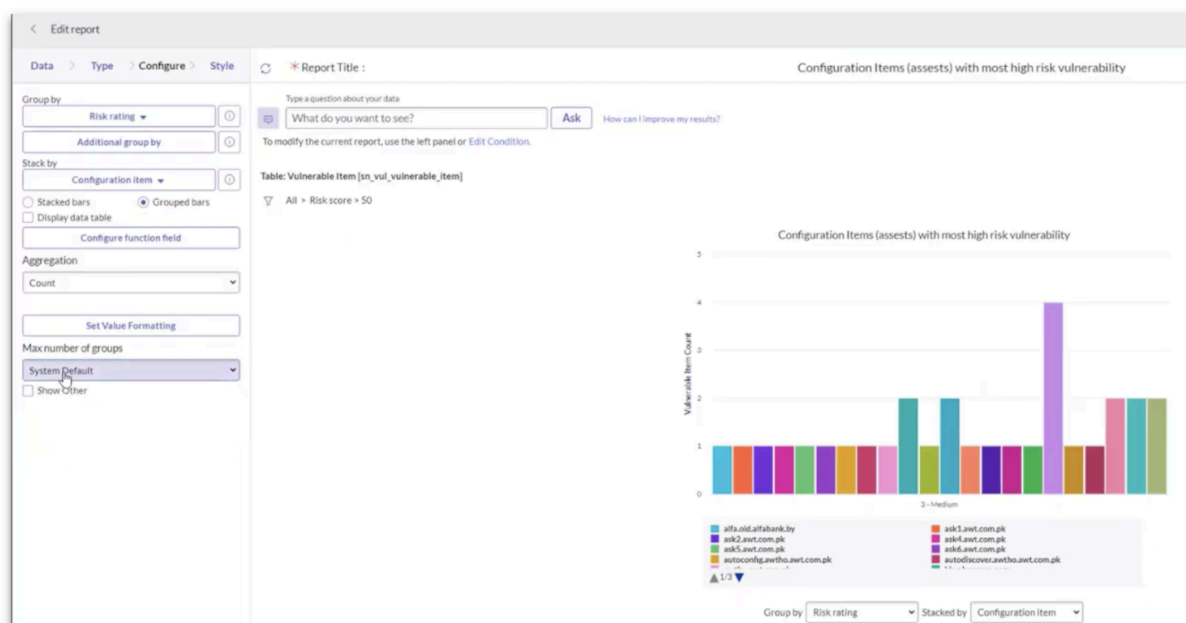
Attack Surface Dashboard

Recorded Future provides a dashboard within the ServiceNow that incorporates your ingested assets with Recorded Future's ASI intelligence. You can easily identify your highest risk vulnerabilities with the provided summary, risk score and attack vector / exploit information.

You can also group your configuration items by risk rating, risk score, vulnerability severity or by configuration item. These dashboards / reports can be further customized to suit your specific criteria.



Recorded Future ASI Dashboard



Recorded Future ASI Dashboard Customization

Syncing ASI Scans with CMDB

ServiceNow CMDB tables are an organization's source of truth for asset inventory management. They are incorporated into many workflows including patch management and incident response. During investigations and incident response, maintaining and having access to a mature asset inventory is pivotal to preventing threats.

The Recorded Future ASI integration into ServiceNow provides comprehensive coverage, automatically pulling all newly discovered assets via ASI into ServiceNow's CMDB tables. This includes all domains and IP addresses belonging to those assets. The integration ensures that no duplicate entry is created, even if an asset already exists in the CMDB.

Because assessment is based on the Recorded Future Total Internet Inventory, companies gain insight into previously unknown assets. Clients find ASI and standard vulnerability management tools and workflows to be complementary. ASI discovers assets and vulnerability management tools scan them.

Having your CMDB tables updated with your entire surface area provided by ASI will allow your company insights into devices previously unknown the existence of.

Importing ASI Exposures

ASI exposures represent any misconfiguration or vulnerability that may present an opportunity for an adversary within your attack surface.

These exposures create ServiceNow Vulnerable Items, containing a summary of the exposure, the severity and the associated configuration item. The Vulnerable Item will also contain a direct link to the configuration item within the Recorded Future portal for quick access.

Vulnerable Item

VIT0010114

Update

Create Security Incident

Start Investigation

Mark as False Positive

Request Exception

Resolve

Unassign

Close

Delete

Number

VIT0010114

State

Open

Source

ASI

Assignment group

Vulnerability Response

Risk rating

3 - Medium

Assigned to

Risk score

40

Created

2024-06-22 01:02:47

Remediation target rule

Medium-High Risk Rating rule

Last opened

2024-06-22

Remediation target

2024-07-22 00:00:00

Updated

2024-07-22 04:00:19

Remediation status

Target Missed

Vulnerability

ASI-scan_Nginx-end-of-life

Configuration item

.by

Vulnerability

Remediation Steps

Initial Detection

Detections

Notes

Summary

Using 6 versions of Nginx that have been designated by the vendor as EOL (End of Life). EOL is a term used by software vendors indicating that it is ending or limiting its support on the product and/or version to shift focus on their newer products and/or version.

Severity

3 - Medium

Exploit exists

No

Vulnerability score (v3)

Exploit attack vector

-- None --

Vulnerability score (v2)

Exploit skill level

-- None --

Threat

Date published

Remediation notes

Last modified

Update

Create Security Incident

Start Investigation

Mark as False Positive

Request Exception

Resolve

Unassign

Close

Delete

Related Links

[Calculate Risk Score](#)
[Open in Recorded Future](#)

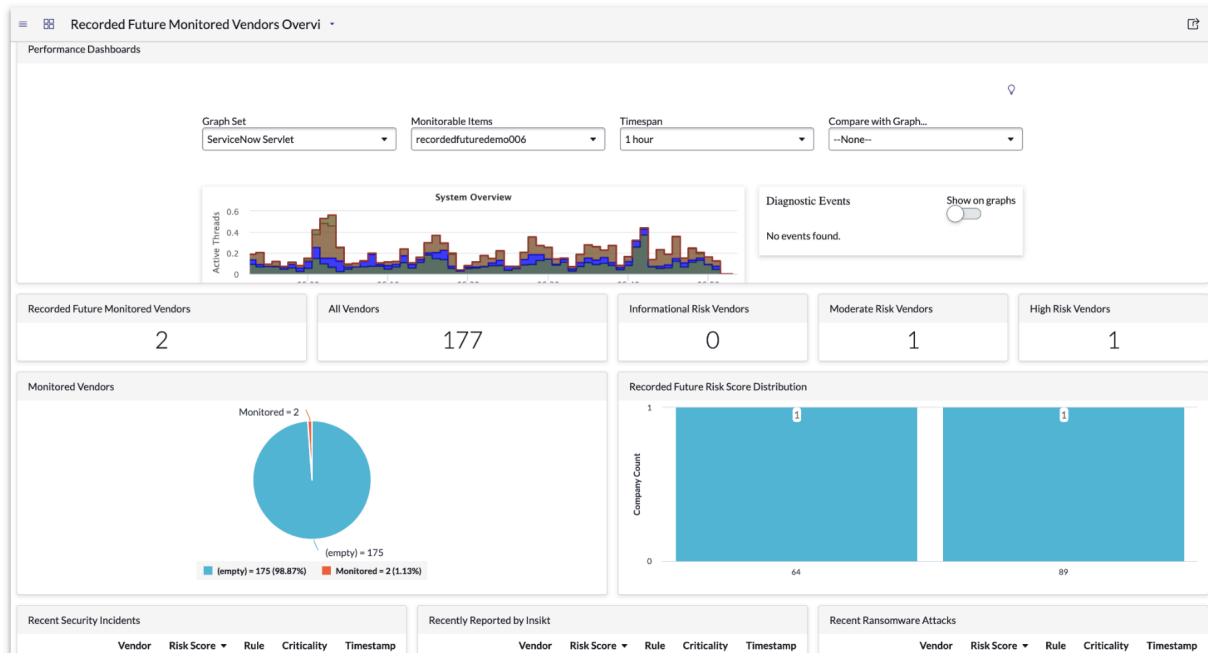
ASI Sourced Vulnerable Item

VRM

This section provides an overview of use cases for Recorded Future within the ServiceNow Vendor Risk Management integration.

Vendor Assessment Dashboard

Recorded Future provides a dashboard within the ServiceNow that incorporates your vendors and their risk scores. Serving as a homepage for GRC, Supply Chain Management, or Other Third-Party Risk Management teams, the Vendor Assessment Dashboard makes it easy to pivot to what matters most.



Threat Lookup Results

Company Enrichment

GRC and Supply Chain Management team's require assessing the risk and reputation of vendor's their company works with. Within VRM, ServiceNow provides risk scores, triggered risk rules, and evidence details within ServiceNow company records, including timestamps.

Providing this information with ServiceNow can expedite the research and handling of information between departments who have access to ServiceNow and makes the information easy and quick to understand for whomever is responsible in handling third-party risk.

Company
Symantec View: Recorded Future Vendors

NameSymantec

Websitewww.symantec.com

Industry

Vendor typeSoftware

Recorded Future Risk Score89

Recorded Future Intelligence Cardhttps://app.recordedfuture.com/live/sc/entity/B_E5

Recorded Future Monitored StatusMonitored

Notes

Status-- None --

Risk rating

Rank tierStrategic Partner

Third-party tier-- None --

Vendor manager

Business owner

Update

Delete

Triggered Risk Rules

Risk Rules

1 to 20 of 23

	Risk Score	Rule	Criticality	Evidence	Timestamp
✖	89	Historical Misconfigurations and Vulnera...	Informational	10+ sightings: Historical Open Proxies s...	2024-07-28 17:00:00
✖	89	Historical Typosquat Similarity to Compa...	Informational	249 sightings: 249 historical typosquats...	2024-07-28 17:00:00
✖	89	Domain With Missing DMARC Record	Informational	10 sightings: 10 company domains configu...	2024-07-28 17:00:00
✖	89	Recent Reported Cyber Attack	High	1 sighting: Recorded Future identified a...	2024-07-17 17:00:00
✖	89	Recent Typosquat Similarity to Company D...	Moderate	3 sightings: 3 recent typosquats seen fo...	2024-07-28 17:00:00

Company Enrichment

ITSM

This section provides an overview of use cases for Recorded Future within the ServiceNow ITSM integration.

ASI Alert Triage

Timely alert triage is critical. ASI Alerts related to the increase in the risk rating of a configuration item are brought in as incidents (INC). If your organization owns SIR, these alerts can be promoted to SIR incidents.

Incidents

Opened

Search

All > Active = true

<input type="checkbox"/>	Number	Opened	Short description	Caller	Priority	State	Category	Updated	Updated by
<input type="checkbox"/>	INC0024263	2024-07-31 10:01:49	🟡 Attack Surface Risk: ghavamin3.ir (89 --> 89)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:49	recordedfuture
<input type="checkbox"/>	INC0024262	2024-07-31 10:01:48	🟡 Attack Surface Risk: dev.alfabank.by (15 --> 67)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:48	recordedfuture
<input type="checkbox"/>	INC0024261	2024-07-31 10:01:47	🟡 Attack Surface Risk: shal.dev.alfabank.by (26 --> 70)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:47	recordedfuture
<input type="checkbox"/>	INC0024260	2024-07-31 10:01:46	🟡 Attack Surface Risk: ftp.ghavamin3.ir (89 --> 89)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:46	recordedfuture
<input type="checkbox"/>	INC0024259	2024-07-31 10:01:46	🟡 Attack Surface Risk: stat.alfabank.by (15 --> 67)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:46	recordedfuture
<input type="checkbox"/>	INC0024258	2024-07-31 10:01:45	🟡 Attack Surface Risk: mail.ghavamin3.ir (89 --> 89)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:45	recordedfuture
<input type="checkbox"/>	INC0024257	2024-07-31 10:01:44	🟡 Attack Surface Risk: personas.bancadigitalqa.banesco.com.pa (38 --> 73)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:44	recordedfuture
<input type="checkbox"/>	INC0024256	2024-07-31 10:01:43	🟡 Attack Surface Risk: www.ghavamin3.ir (89 --> 89)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:43	recordedfuture
<input type="checkbox"/>	INC0024254	2024-07-31 10:01:42	🟡 Attack Surface Risk: ss-dev.aq-fes.com (62 --> 77)	Recorded Future	4 - Low	New	Inquiry / Help	2024-07-31 10:01:42	recordedfuture

ASI Alert Overview

Incident
INC0024263

[Discuss](#)
[Follow](#)
[Update](#)
[Create Security Incident](#)
[Resolve](#)
[Delete](#)

Number: INC0024263

Channel: -- None --

Caller: Recorded Future

State: New

Category: Inquiry / Help

Impact: 2 - Medium

Subcategory: -- None --

Urgency: 3 - Low

Service:

Priority: 4 - Low

Service offering:

Assignment group:

Configuration item:

Assigned to:

Short description: Attack Surface Risk: ghavamin3.ir (89 --> 89)

Description:

Related Search Results >

Notes
Related Records
Resolution Information

Watch list

Work notes list

Work notes

Additional comments (Customer visible)

Activities: 1

Field changes: 2024-07-31 10:01:49

ASI Incident

Additional Reading

Find below additional information of the various Recorded Future products mentioned throughout this document.

[Recorded Future Collective Insights](#)

[Recorded Future ServiceNow ASI Integration](#)

[Recorded Future ServiceNow VR Integration](#)

[Recorded Future Research Links](#)

[Recorded Future Third-Party Risk Scoring](#)

Professional Services Assistance

Recorded Future provides a custom service for use case development to identify and implement the capabilities outlined in this document and also develop new capabilities based on discovery workshops with customers.

For more information on use case development or assistance with creating custom use cases and implementation, please get in touch with your Sales or Intelligence Services representative and arrange a conversation with Professional Services at Recorded Future to see how we can help.