Recorded Future®

ServiceNow Reference Architecture

Capabilities and Use Cases

Created by: Recorded Future Professional Services

Published: August 2024
Updated: September 2024

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.

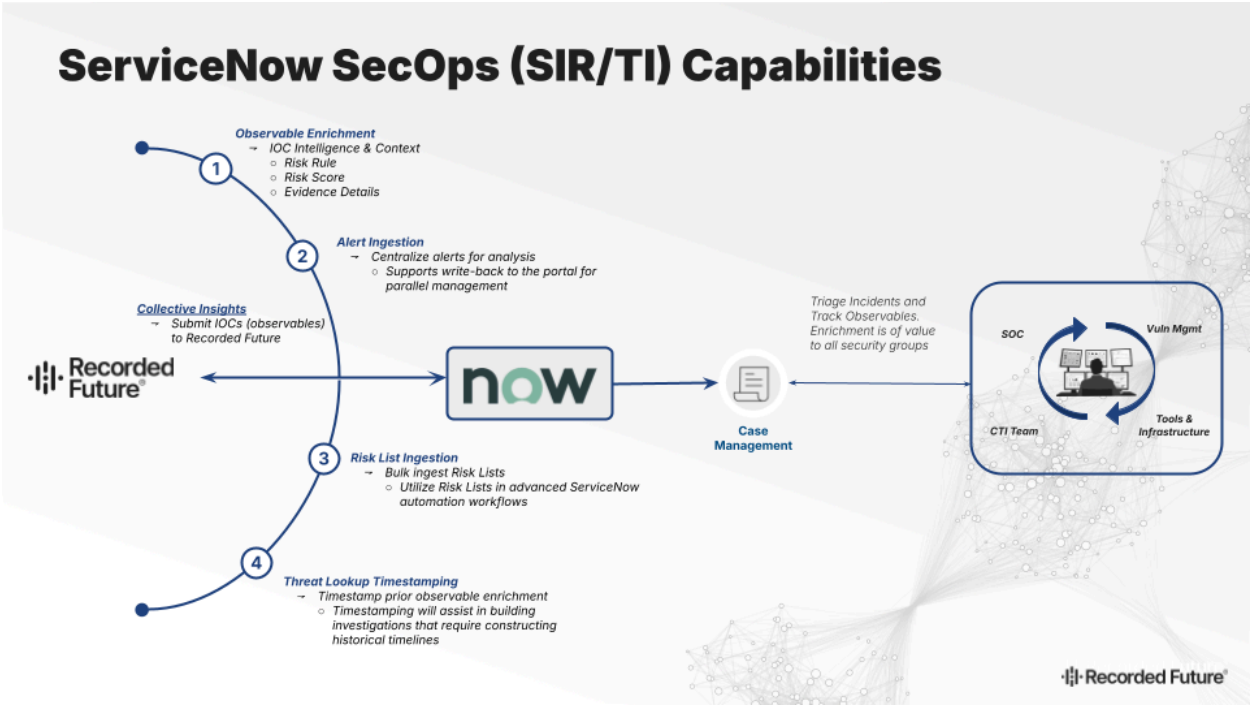
The Recorded Future for Security Incident Response / Threat Intelligence integration enables security operations teams to simplify their workflows, identify and contextualize incidents faster, and centralize their incident response within ServiceNow.

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.

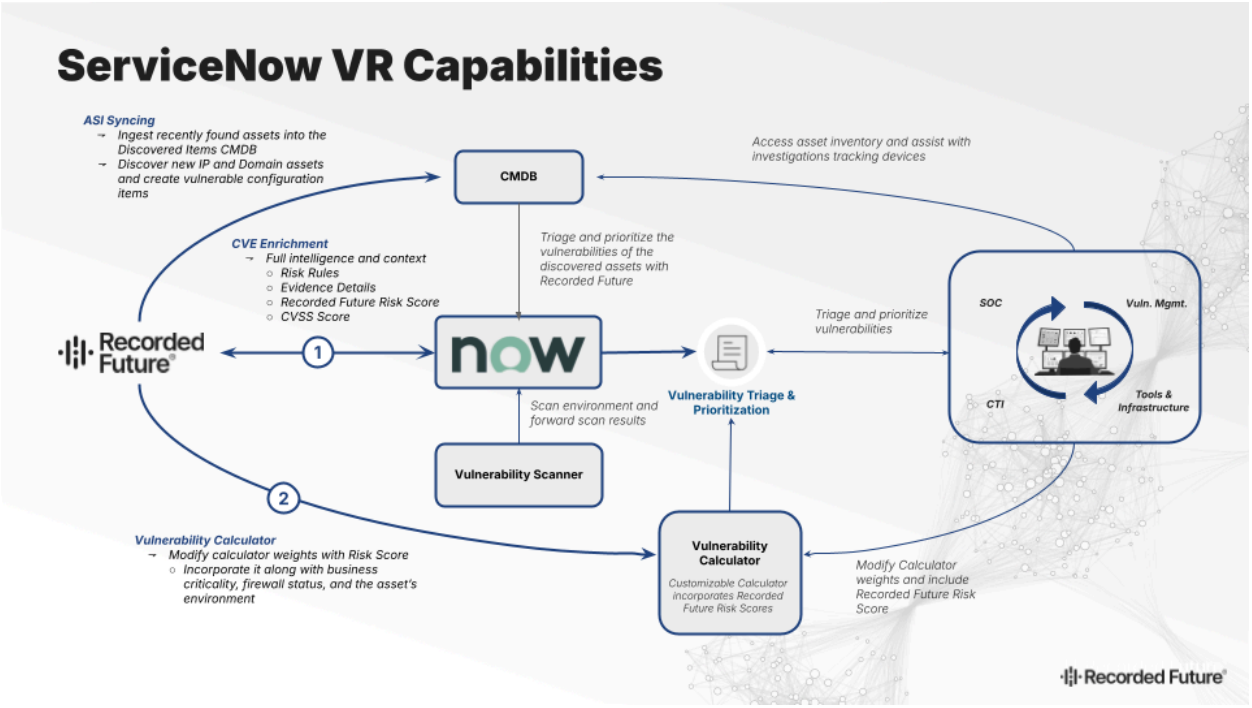
Additionally, Recorded Future ASI integrated into Vulnerability Response.

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.

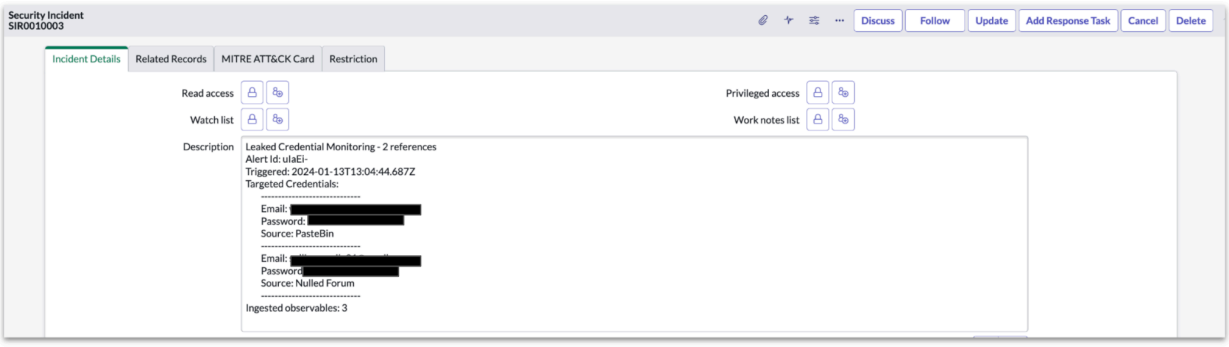
SIR/TI

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

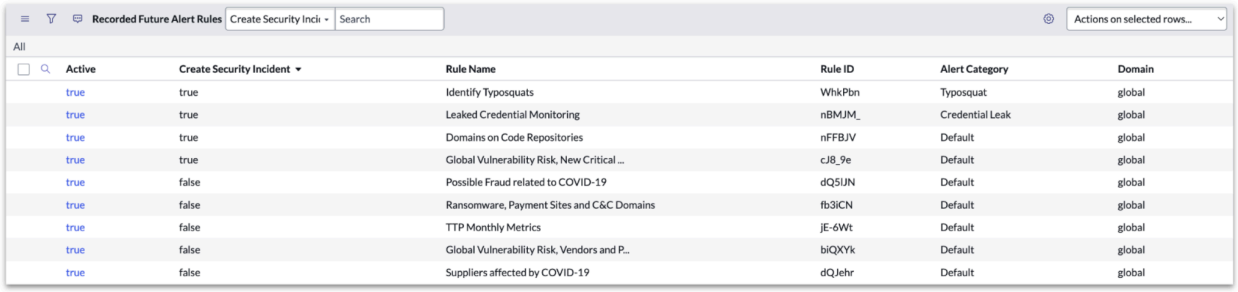
Alert Triage

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.

Recorded Future alerts ingested as Security Incidents



Recorded Future Leaked Credential Alert with compromised credentials



Active	Create Security Incident	Rule Name	Rule ID	Alert Category	Domain
true	true	Identify Typosquats	WhkPbn	Typosquat	global
true	true	Leaked Credential Monitoring	nBMJM_	Credential Leak	global
true	true	Domains on Code Repositories	nFFBJV	Default	global
true	true	Global Vulnerability Risk, New Critical ...	cJ8_9e	Default	global
true	false	Possible Fraud related to COVID-19	dQ5IJN	Default	global
true	false	Ransomware, Payment Sites and C&C Domains	fb3iCN	Default	global
true	false	TTP Monthly Metrics	jE-6Wt	Default	global
true	false	Global Vulnerability Risk, Vendors and P...	biQXYk	Default	global
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.

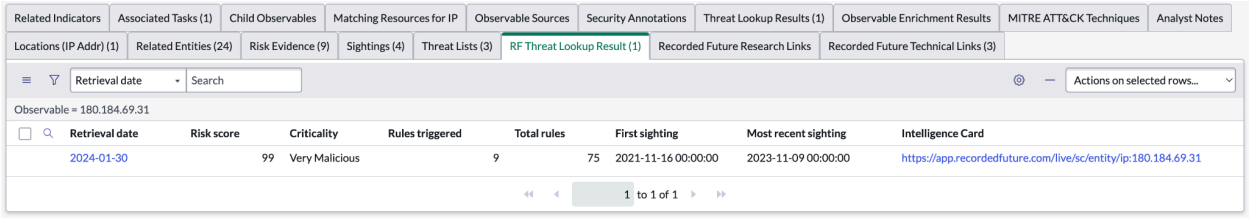
In the case of *transfer mode*, the Recorded Future portal alert will close. In the case of *manage mode*, the Recorded Future portal alert remains open in tandem with the newly created ServiceNow incident. The table below breaks down each mode.

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

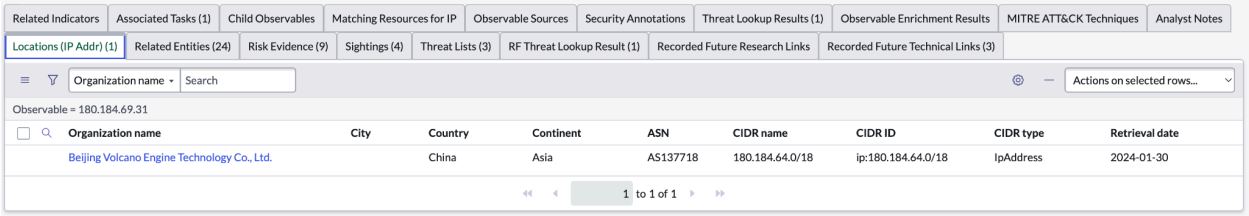
Observable Enrichment

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.

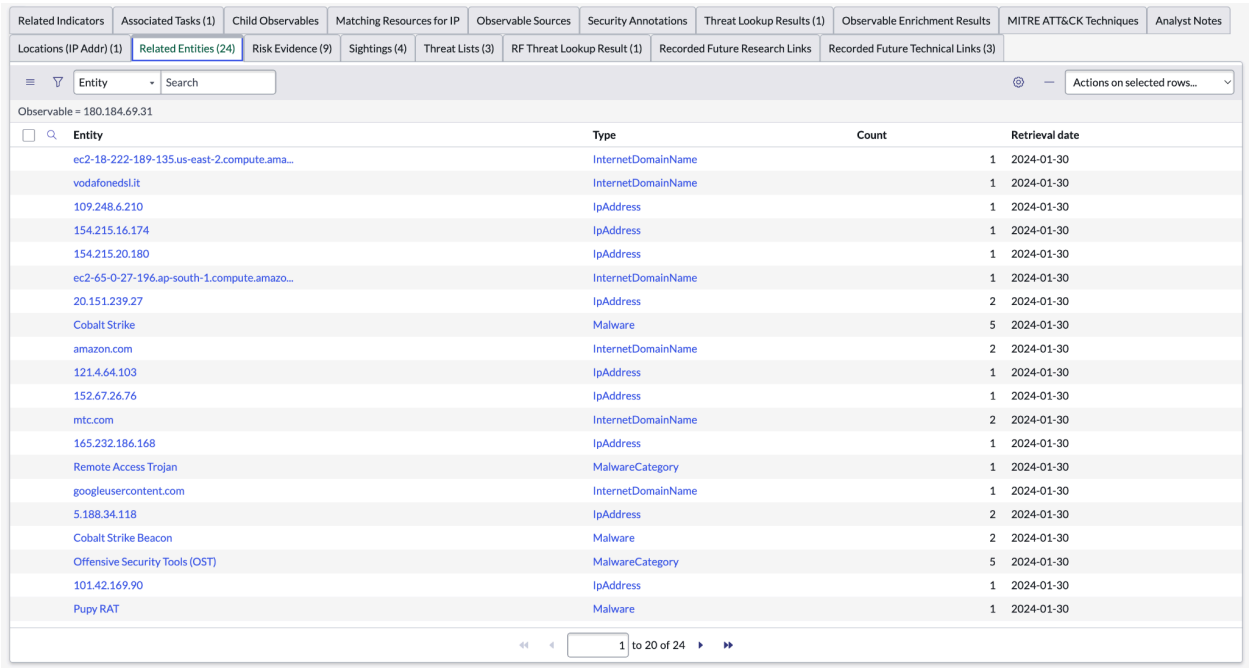
With Recorded Future, you can directly enrich observables within SIR tickets by bringing in risk scores, evidence details, related entities, geolocation data and more. This combination of intelligence allows analysts to perform remediation actions such as blocking the indicator on the firewall or kick-starting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



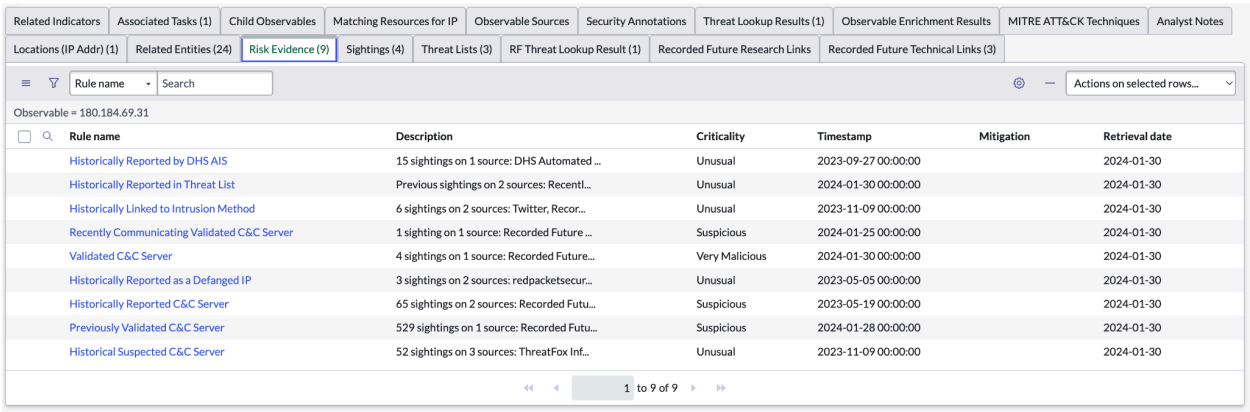
Recorded Future Risk Score, Criticality, and Intelligence Card link



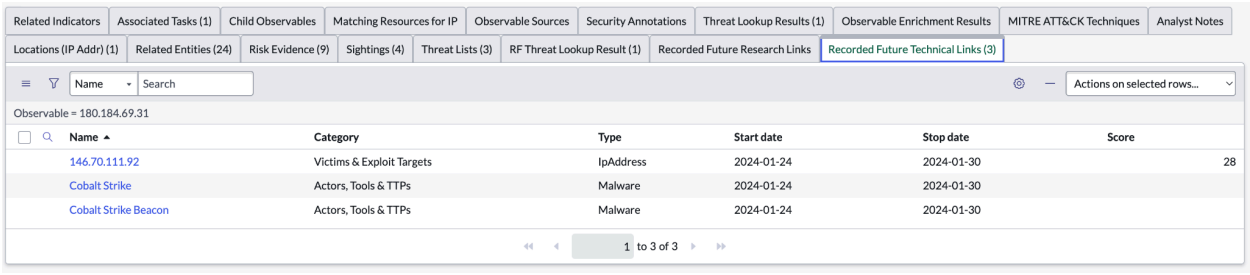
Recorded Future Geolocation Data



Recorded Future Related Entities

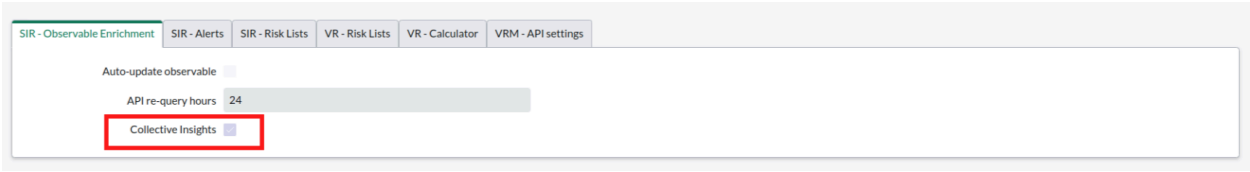


Recorded Future Risk Evidence (Risk Rules) Details



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.



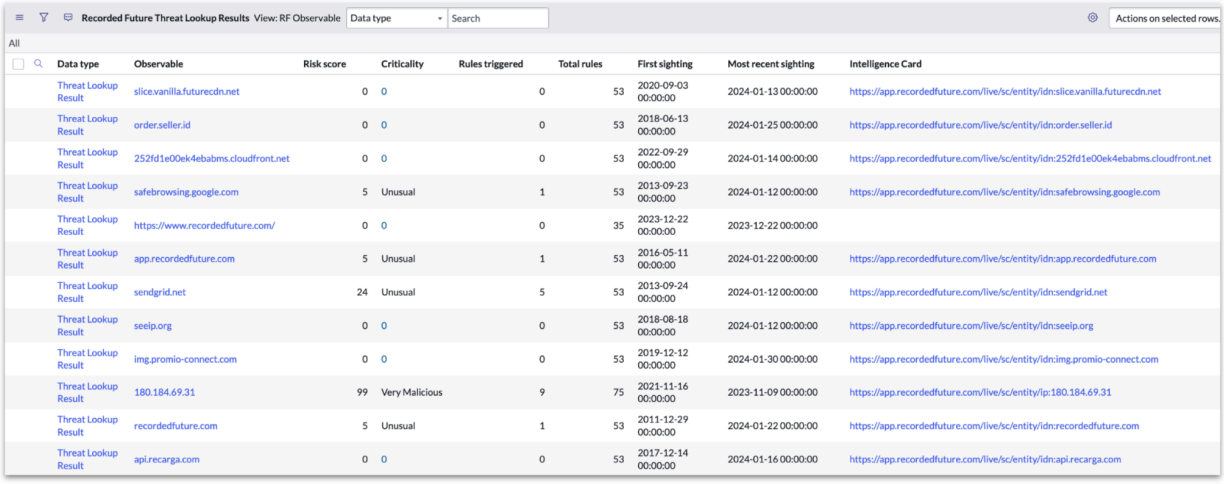
Recorded Future Collective Insights

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.

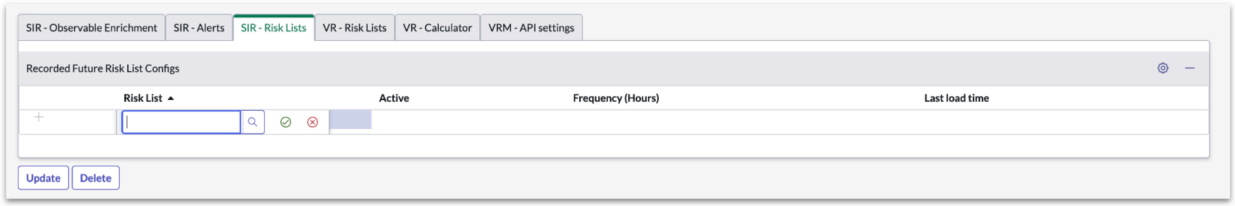
Prior enrichment lookups are stored in the threat lookup results.



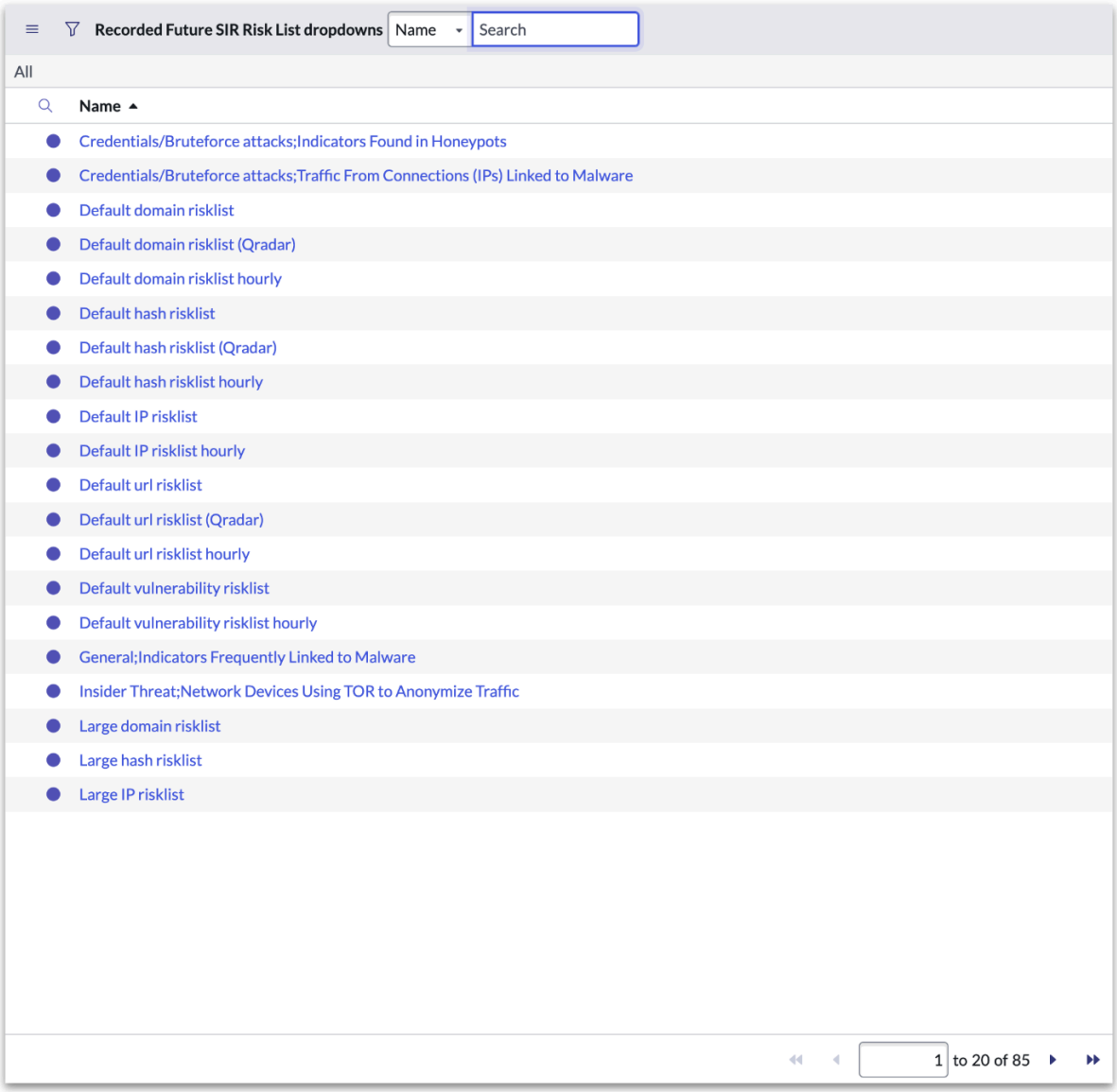
Data type	Observable	Risk score	Criticality	Rules triggered	Total rules	First sighting	Most recent sighting	Intelligence Card
Threat Lookup Result	slice.vanilla.futurecdn.net	0	0	0	53	2020-09-03 00:00:00	2024-01-13 00:00:00	https://app.recordedfuture.com/live/sc/entity/idn:slice.vanilla.futurecdn.net
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/idn:order.seller.id
Threat Lookup Result	252fd1e00ek4ebabms.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/idn:252fd1e00ek4ebabms.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/idn:safebrowsing.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/idn:app.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/idn:sendgrid.net
Threat Lookup Result	seeip.org	0	0	0	53	2018-08-18 00:00:00	2024-01-12 00:00:00	https://app.recordedfuture.com/live/sc/entity/idn:seeip.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/idn:img.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/ip:180.184.69.31
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/idn:recordedfuture.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/idn:api.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.



Configure and Ingest Risk Lists



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.

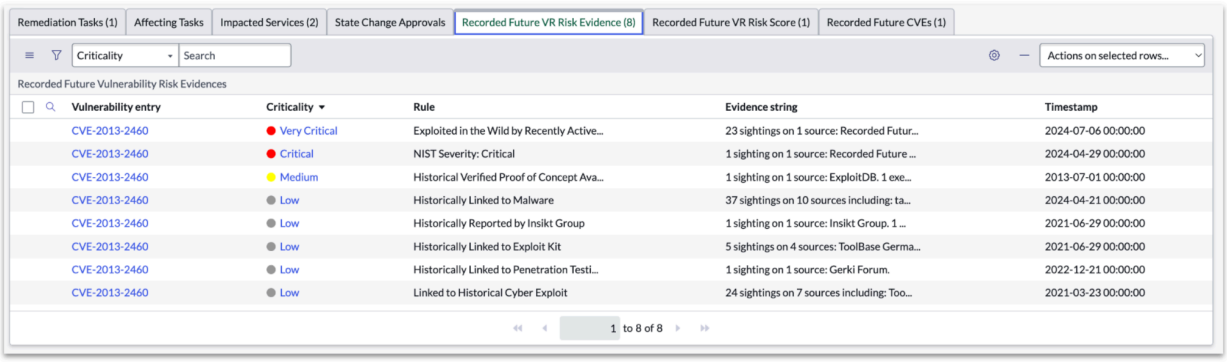
- **Environment:** Weighted 20
  The environment in which the vulnerability exists is critical to understanding the potential impact. If in production, it can affect your company and your customers; if it's in development, this is less harmful to customers but could impact business operations.

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

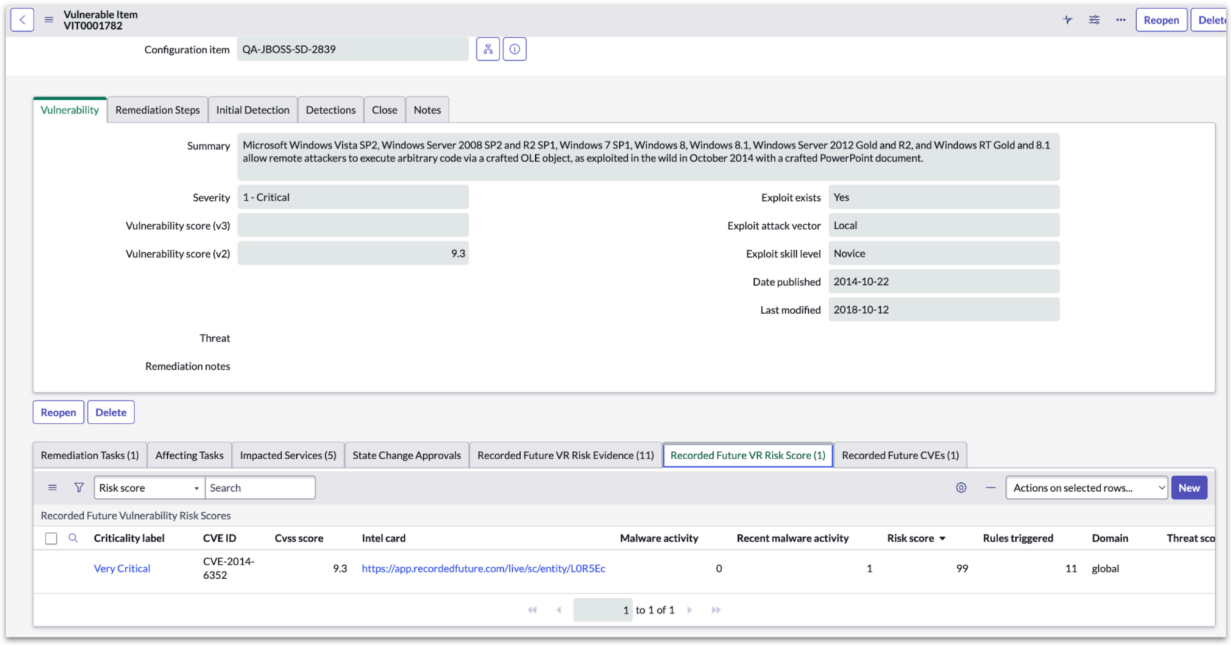
CVE Enrichment

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).



Recorded Future Risk Evidence Details

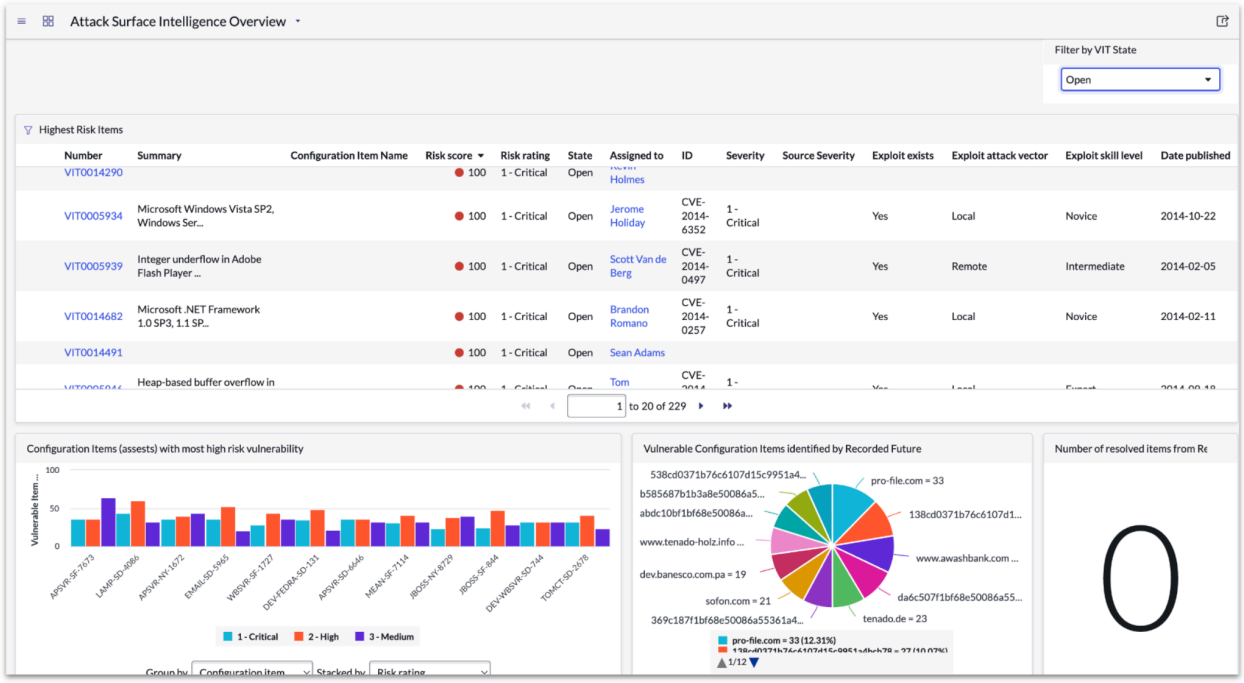


Recorded Future Risk Score

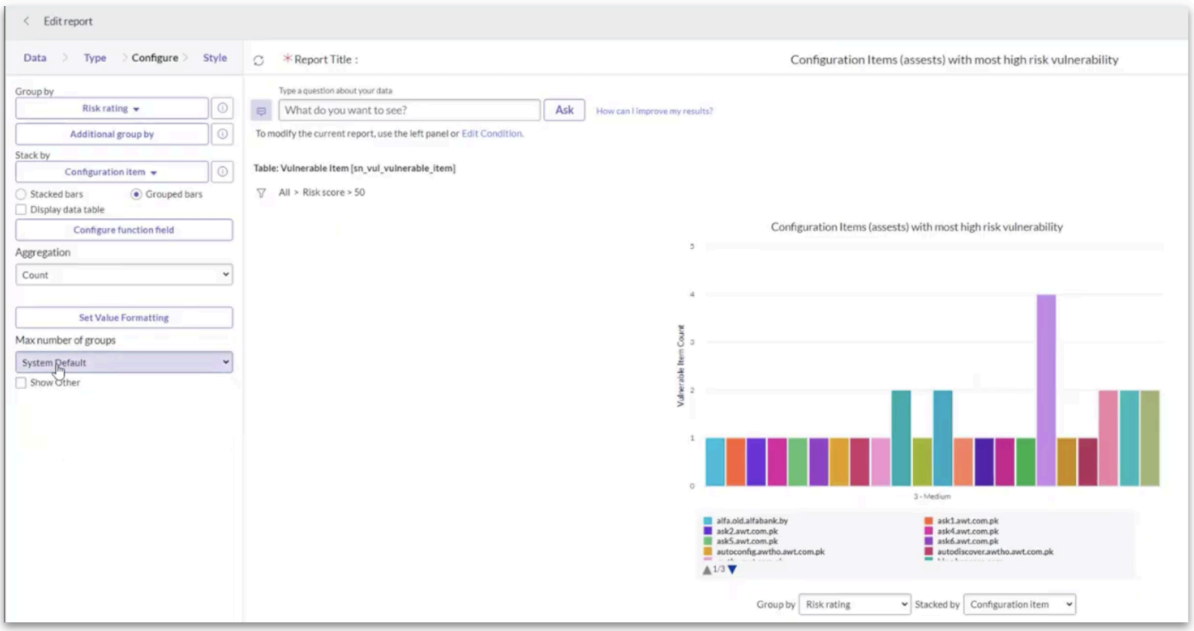
Attack Surface Dashboard

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.

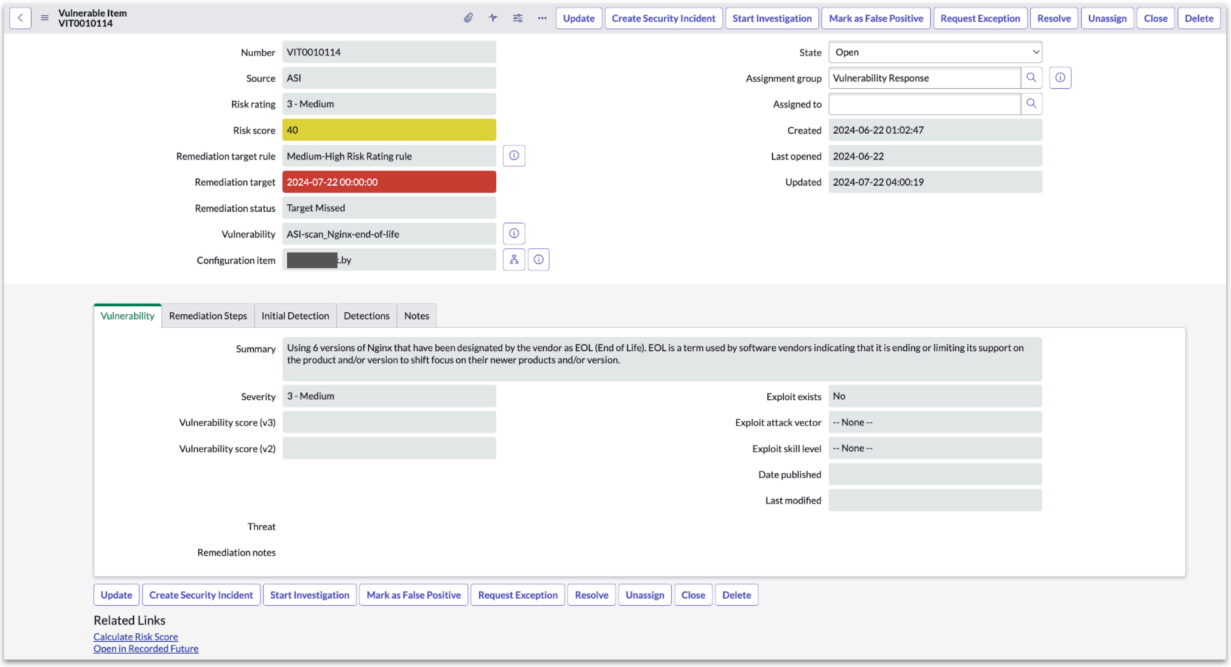
Because assessment is based on the Recorded Future Total Internet Inventory, companies gain insight into previously unknown assets. Clients find ASI and standard vulnerability management tools and workflows to be complementary. ASI discovers assets and vulnerability management tools scan them.

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.



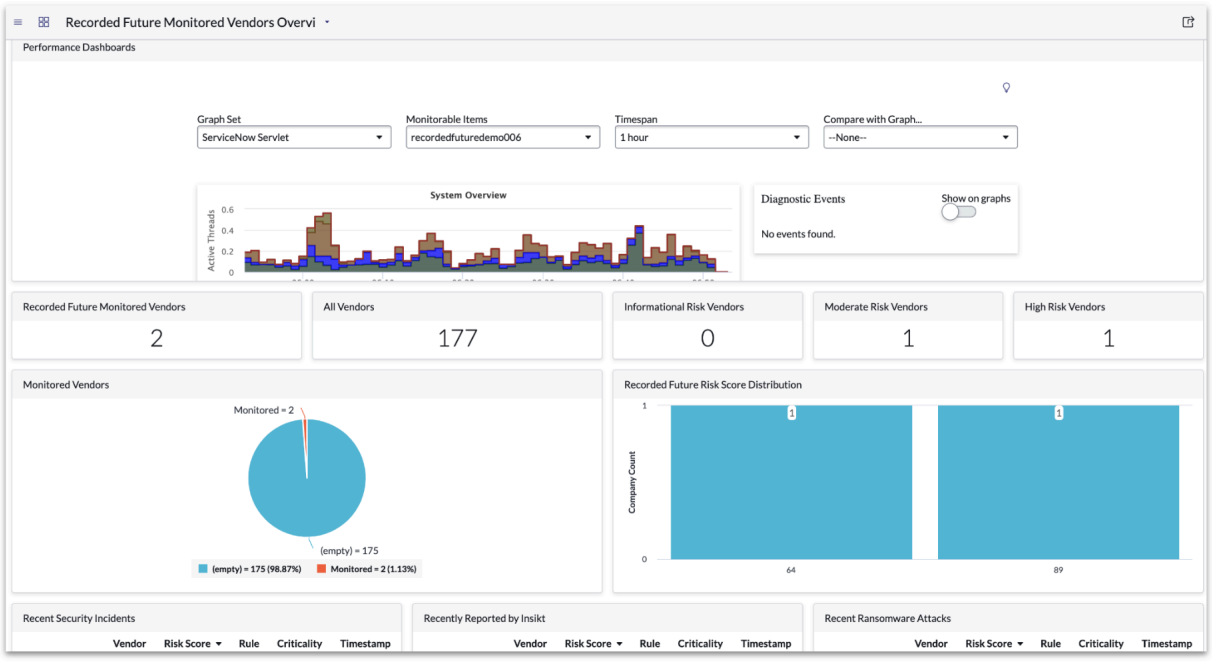
ASI Sourced Vulnerable Item

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.

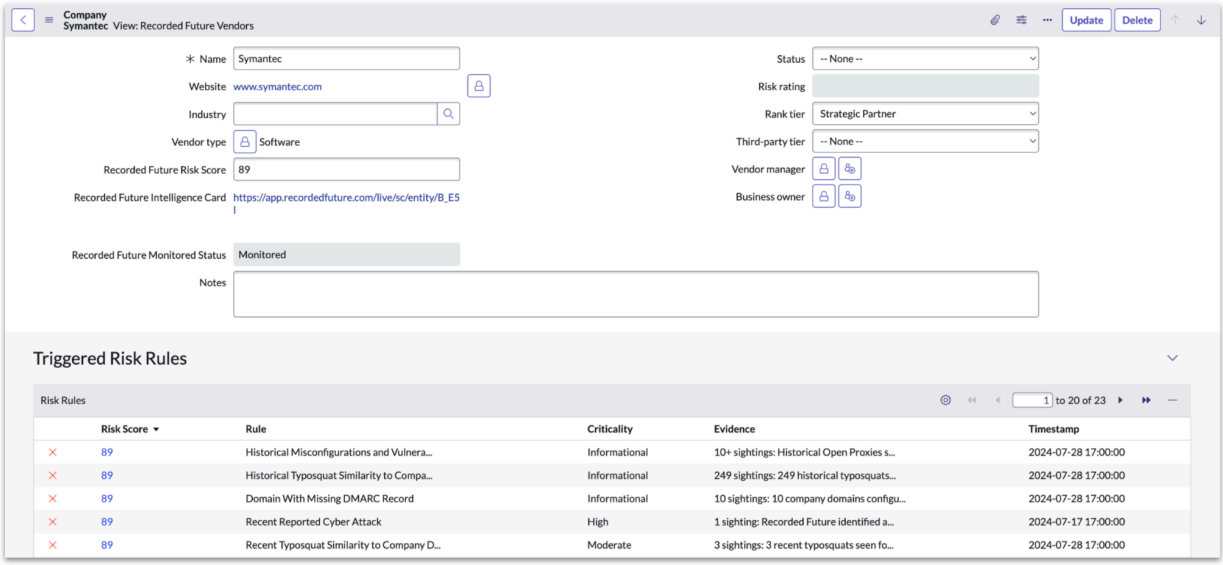


Threat Lookup Results

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.



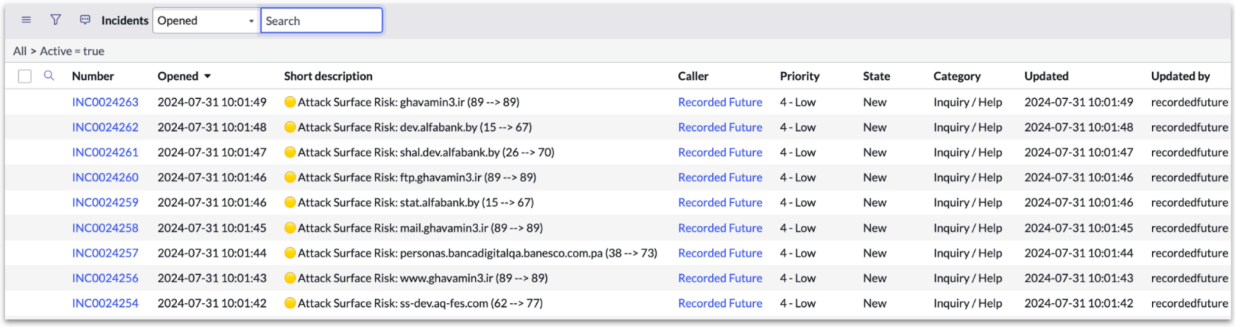
Company Enrichment

ITSM

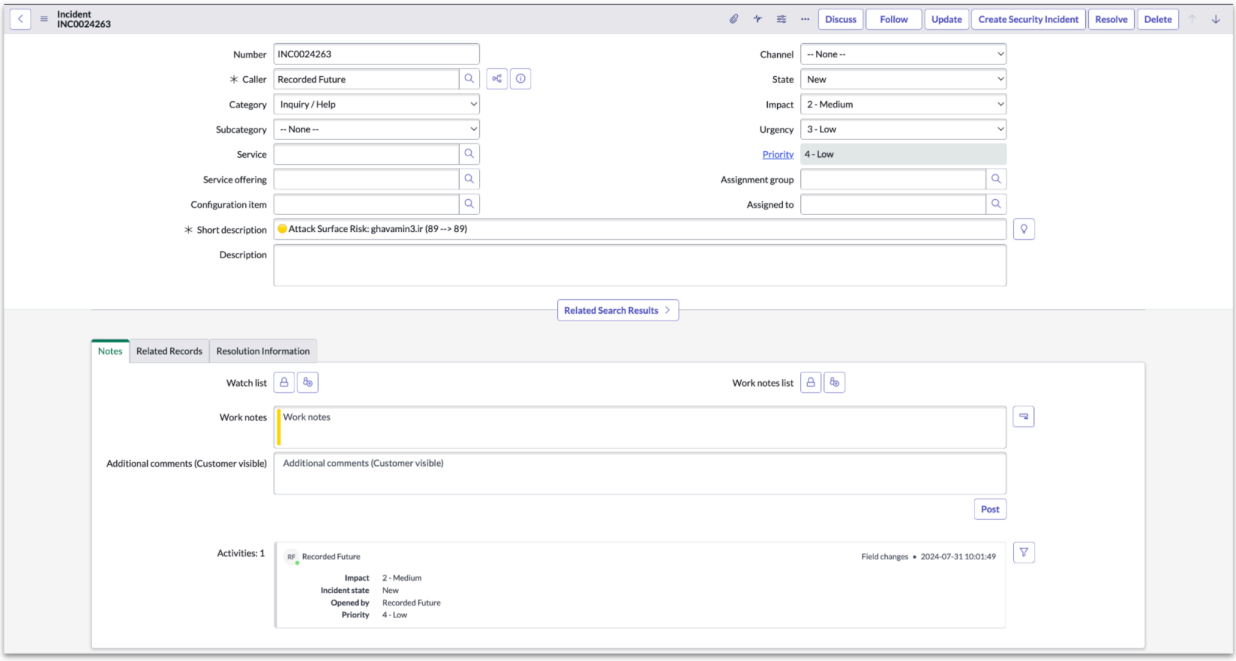
This section provides an overview of use cases for Recorded Future within the ServiceNow ITSM integration.

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.



ASI Alert Overview



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.