

# Recorded Future and Nevelex Labs

## PRODUCT OVERVIEW

Security Flow is a new automation and orchestration tool for corporate security and IT. Security Flow helps companies integrate their diverse security tools, enabling them to harness the full value of each product with ease, saving significant time and money. Security Flow has three primary differentiators:

1. Licensing model price accommodates unlimited actions and unlimited seats without increasing costs.
2. Batch of Professional Service hours to launch Security Flow are included with licensing.
3. Broadcast event mechanism to help decouple flows (playbooks) from plugins (integrations).

## JOINT INTEGRATION DESCRIPTION

- Reduces the mean time of a response to a Phishing incident by automated gathering of threat intelligence.
- **Proactive Information Sharing to Help Prevent Malware and Ransomware Attacks:** Improves existing security infrastructure by integrating information exchange between Recorded Future and disparate security products.

## CHALLENGES OVERCOME THROUGH INTEGRATION

- Automated gathering of threat intel on IoCs within security incidents
- Reducing security analyst's work by automating incident threat analysis and response. Analysts can then focus on the high value work, resulting in stronger, more securely defended corporate networks.
- Simplified flow (playbook) construction by supporting broadcast events.

## USE CASES

- Automation of analysis of IoCs within phishing or malicious emails. All IoCs within a reported email are sent through this plugin to determine their risk score. If the risk score analysis determines the email contains a risky IoC, the email is automatically purged from all the end user's mailboxes.
- Set up a regular flow (playback) to migrate cached risk list hash information into a web gateway to automatically block future attempts to download those malicious files.
- Monitor alerts from Recorded Future to trigger a blocking of lookalike domains and perform other user configured actions.

Recorded Future®



## BENEFITS:

- Reduces the mean time of a response to a Phishing incident by automated gathering of threat intelligence.
- **Proactive Information Sharing to Help Prevent Malware and Ransomware Attacks:** Improves existing security infrastructure by integrating information exchange between Recorded Future and disparate security products.

**Incident Timeline**

Incident Name: NI-Associate-IOCs | Category: None | Message: 56721378.F13ad6 | Message Events | Assignee: | Incident Status: Open

Message - Plugin Success Response: NI-Associate-IOCs | Created incident with status: Open

Message - Plugin Success Response: NI-Recorded-Future | Recorded Future Report Response

Recorded Future - File Hash Report

Risk Score	Criticality	Risk Summary
71	Malicious	2 of 12 Risk Rules currently observed.

Hash: 5673e32d7d8201169bc04264 | Hash Algorithm: MD5 | Source: Connect API Query

Intel Card: https://app.recordedfuture.com/web/console/entry/5673e32d7d8201169bc04264

Risk Rules Triggered: Positive Malware Verdict - Malicious

Message - Plugin Success Response: NI-Recorded-Future | Recorded Future Report Response

Recorded Future - IP Address Report

Risk Score	Criticality	Risk Summary
64	Suspicious	14 of 53 Risk Rules currently observed.

IP Address: 195.22.26.248 | Source: Connect API Query

Intel Card: https://app.recordedfuture.com/web/console/entry/195.22.26.248

Risk Rules Triggered: Recent Multicategory Backlist - Suspicious

Associated Indicators of Compromise

IOC	Trust Level
5673e32d7d8201169bc04264	(H)
195.22.26.248	(H)

**Configure New Instance**

Recorded Future | Recorded Future | Recorded Future plugin. Adds the ability to gather threat intelligence on URLs, domains, IP addresses, and file hashes. v0.9.5

Fabric Instance Settings | Value

Associated Fabric Instance | Default DXL (Data Exchange Layer) Broker

Instance Name | Value

Instance Name | Recorded Future

Instance Settings | Value

Unique ID | Unique ID: rfi

API Key | API Key: [Redacted]

Fallback to Connect API if not found in Risk List | When risk list caching is enabled, there is no guarantee that the cache will contain the IOC being enriched. This mode enables a fallback to querying the Recorded Future Connect API for information. The Connect API is always the source for up-to-date information.  No

Enable Domain Risk List Caching | Enables caching of a domain risk list from Recorded Future.  No

Domain Risk List | Pulls and caches a domain risk list from Recorded Future. Each request uses five (5) API credits. Domain Risk List: Select...

Enable Hash Risk List Caching | Enables caching of a hash-risk list from Recorded Future.  Yes

Hash Risk List | Pulls and caches a hash-risk list from Recorded Future. Each request uses five (5) API credits. Hash Risk List: Default (Recommended)

Cancel Save



## 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 Nevelex Labs

With an enterprise consultancy driven background stemming from 18 years of experience, Nevelex Labs harnessed those skills to create a powerful, yet easy to utilize, orchestration, automation and response platform.