·l·l· **Recorded Future** ®

Attack Surface Intelligence for ServiceNow Vulnerability Response

Digital transformation initiatives have led to an explosion of assets on the public internet. Driving forces such as an uptick in remote workforce, cloud sprawl, M&A events, increased use of third party software, and more are making it increasingly difficult for organizations to maintain a persistent view of their internet-facing assets.

Assets move, change, and appear constantly, and this dynamic nature means traditional manual asset inventory processes simply cannot keep up. In addition, attackers can use large scale automation to identify exploitable assets in minutes and hours, while it can take days to weeks for an organization to even know where to start looking.

Recorded Future Attack Surface Intelligence provides a persistent view of an organization's digital infrastructure and associated risks to stay ahead of changes, abnormalities, and exploitable vulnerabilities. Integration into ServiceNow IT Vulnerability Response enables IT teams to actively monitor new risks associated with their external attack surface.

About This Integration

The integration between Recorded Future and ServiceNow Vulnerability Response revolutionizes threat detection and remediation processes for security and IT teams. It introduces a suite of essential use-cases, enhancing operational efficiency and risk mitigation.

When Attack Surface Intelligence (ASI) identifies a new asset, the integration seamlessly integrates it into the Configuration Management Database (CMDB) if not already known, ensuring a comprehensive asset inventory. Similarly, the detection of new exposures triggers the creation of vulnerable items, addressing the exposure + configuration item combination. To streamline response efforts, the integration automatically closes vulnerable items after 14 days if the exposure is resolved on the asset, with configurable options available.

Features

- Access to the largest archive of past and present DNS history
- Continuous internet scanning for a changing attack surface
- Transparent risk scoring, context and evidence
- Persistent and prioritized view of the external attack surface
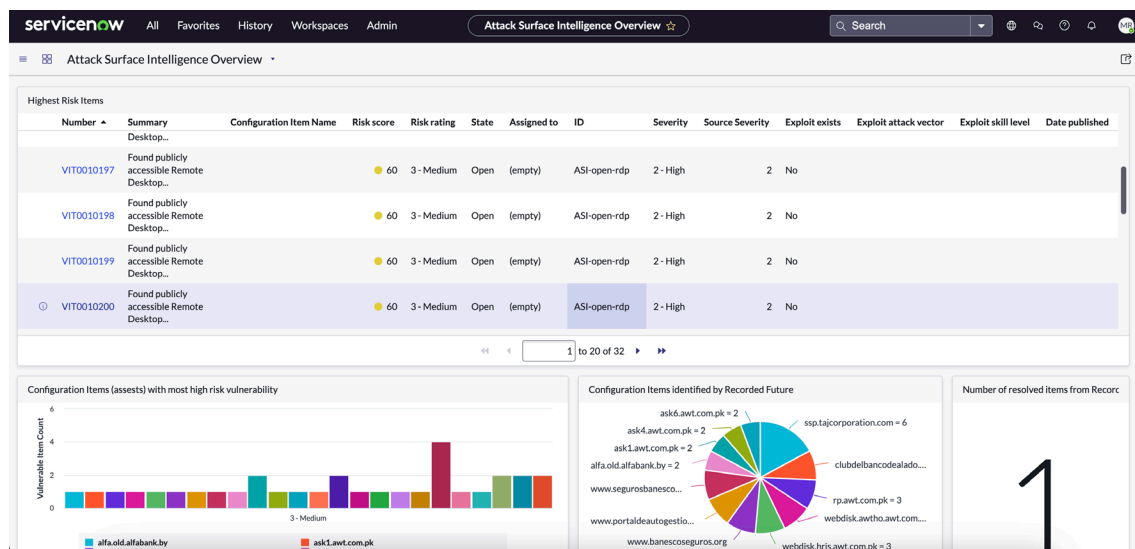
Use Cases

- Discover shadow IT and out of policy assets
- Accelerate vulnerability scanning and incident response
- Confidently prioritize assets vulnerable to threats or exploits
- Enforce security controls

The exposures uncovered by Recorded Future are supported by top-tier intelligence, extending beyond vulnerabilities to encompass critical aspects such as misconfigurations and End-of-Life (EOL) software. Moreover, this data seamlessly integrates with other asset and vulnerability datasets within ServiceNow, enabling a comprehensive approach to threat management and remediation.

Dashboards offer real-time insights, displaying integration run health, assets and vulnerable items created by Recorded Future in CMDB, configuration items with the most exposures, and exposures with the most associated configuration items. This comprehensive visibility empowers teams to make informed decisions and prioritize remediation efforts effectively. The integration facilitates a seamless pivot back to Recorded Future, allowing for detailed investigations into assets.

The exclusion of muted exposure results from the Recorded Future portal prevents false positives or low-priority rule management, ensuring a focused response and preventing information overload for analysts. This integration represents a pivotal advancement in proactively managing external-facing vulnerabilities and misconfigurations.

www.recordedfuture.com   @RecordedFuture