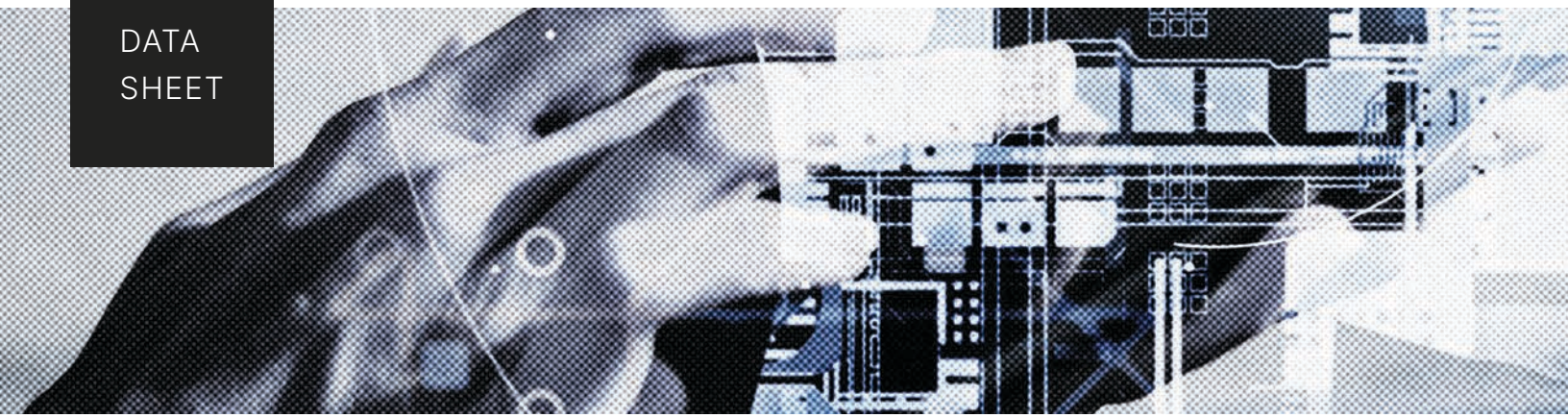
Recorded Future®

DATA SHEET



Attack Surface Intelligence for ServiceNOW IT Service Management

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 Service Management (ITSM) enables IT teams to actively monitor new risks associated with their external attack surface.

About This Integration

Analysts are inundated with alerts that lack context, leading to legitimate threats slipping through the cracks. Dynamic risk rule scoring and contextual evidence helps security and IT teams prioritize and remediate external-facing vulnerabilities and misconfigurations. Attack Surface Intelligence scores and ranks each risk, from assets linked to high risk vulnerabilities to hosts with basic authentication, and provides transparent context for each rule triggered to help organizations accelerate their remediation efforts.

Features

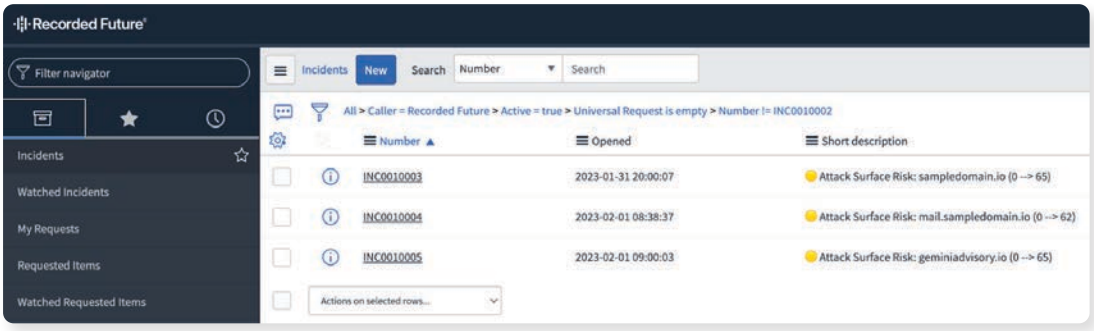
- Continuous internet scanning for a changing attack surface
- Transparent risk scoring, context and evidence
- Persistent and prioritized view of the external attack surface

Use Cases

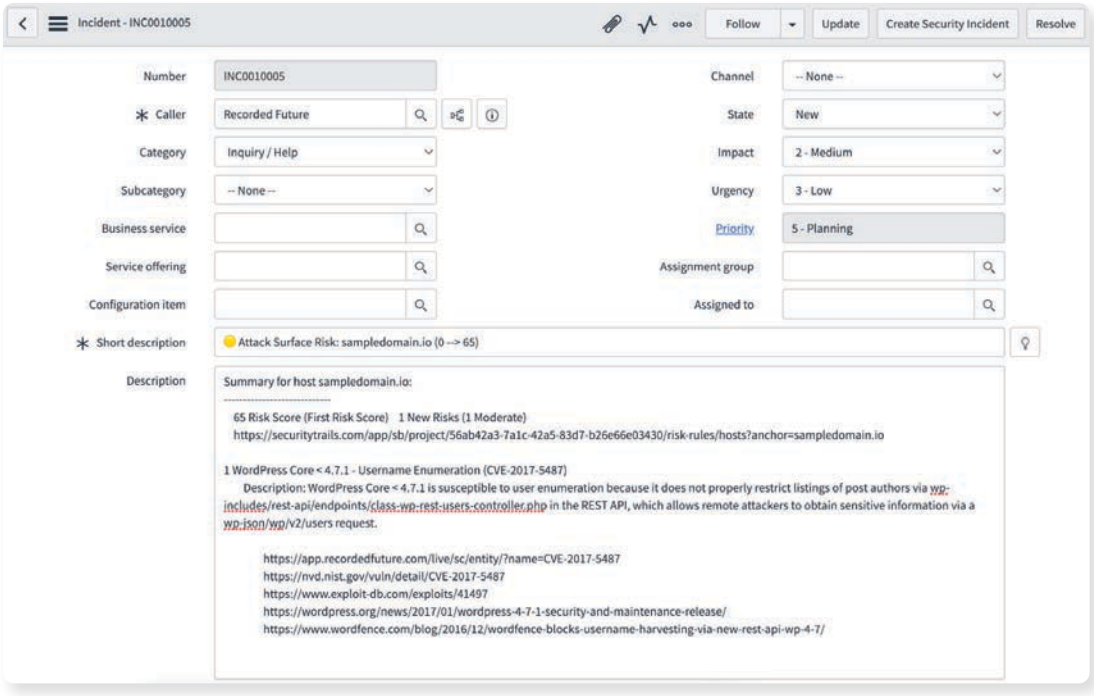
- Discover unknown and out of policy assets
- Accelerate vulnerability scanning and incident response
- Confidently prioritize assets vulnerable to threats or exploits
- Enforce security controls

In ServiceNOW ITSM the integration **creates a ticket for each host that has a new risk issue** within Recorded Future's Critical or Moderate severity bands. A short description field is populated with information about the asset in question as well:

- A colored indicator of whether the asset's Risk Score is considered Critical (**red**) or Moderate (**yellow**)
- The asset's descriptor (hostname, IP address, etc)
- The asset's previous and current Risk Score



Tickets are created within ServiceNOW ITSM when new Critical or Moderate risks are identified



A plaintext summary within the description field of the ticket contains additional context