HP ArcSight and IBM Resilient Incident Response Platform

Fast and easy integration between IBM Resilient incident response platform (IRP) and your HP ArcSight SIEM

Overview

By integrating your ArcSight SIEM data into the IBM Resilient® Incident Response Platform (IRP), you can automatically escalate ArcSight case and events into Resilient incidents and enrich them with artifacts.

IBM Resilient IRP forms your IR hub and connects your ArcSight data to the rest of your security stack.

Benefits

By integrating your ArcSight SIEM and the Resilient IRP, you empower your security team to:

- **Automatically escalate critical ArcSight data into Resilient incidents, enabling the SOC to focus on key incidents**
  The ArcSight integration can automatically escalate cases, correlated events, and base events into Resilient incidents triggered by ArcSight rules. This ensures that you have the full scope of an incident inside your Resilient IR hub, and that the data will map onto the right playbooks and actions automatically.

- **Manually escalate ArcSight events and enrich Resilient incidents**
  Using the ArcSight UI, you can map the fields, artifacts, and IOCs you want into Resilient templates. You can easily create a custom mapping for your ArcSight alerts so that your Resilient incidents have the right data every time. If the incident already exists, the integration will enrich it with the new data from ArcSight.

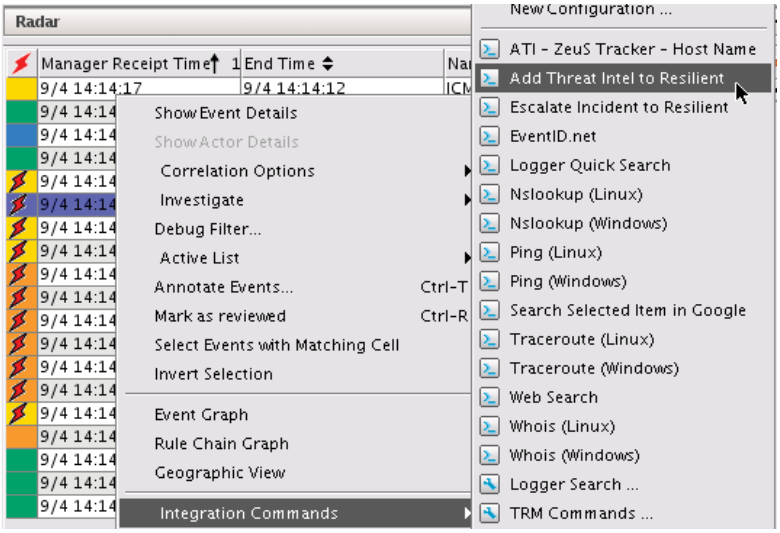

Figure 1: Manually or automatically escalate ArcSight events into the Resilient Platform

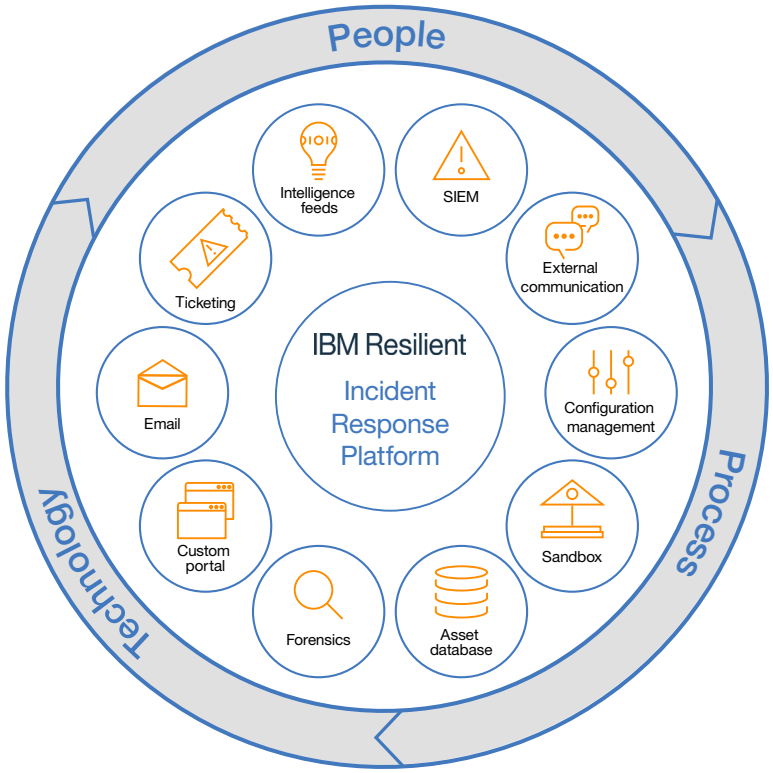

Figure 2: How the Resilient IRP acts as a central hub for IR orchestration

IBM Resilient Incident Response Platform (IRP) is your hub for incident response

When you integrate IBM Resilient IRP with ArcSight, you arm your IR teams with the technology and intelligence they need to take action quickly and effectively. Resilient IRP helps define, orchestrate, automate, and streamline response processes with built-in dynamic playbooks based on industry best practices (including NIST and SANS), regulatory guidelines, and customization determined by organizational needs.

Resilient IRP becomes a hub for your entire security ecosystem — an integrated security solution with the correct process, enriched intelligence, deep-data analytics, and simulation capabilities you need to respond to threats effectively and correctly every time.

IBM Resilient provides you with the ability to integrate, orchestrate, and automate all aspects of your security stack, not just IBM software. By combining the power of ArcSight and the Resilient IRP, you can seamlessly take information from ArcSight, and leverage it for a faster, more effective, and more intelligent response to security incidents.

Every organization needs the full suite of prevention, detection, and response. Resilient IRP acts as a central hub for managing all three. With the addition of the Resilient platform, you can increase the ROI of your ArcSight deployment, bridge the gap between the SOC and your board room, and create faster time to value. It also provides seamless integration and easy vendor management.

Empower your security team to build consistent, repeatable, and effective processes for managing and resolving security incidents — and ensure no security alerts are forgotten.

Free your teams to spend more time focusing on triaging and remediating incidents, and less time manually searching for information from different systems. Your IBM representative is committed to your success. They will work with you to ensure that all your use cases and processes are covered, and that Resilient IRP meets your needs as an IR hub.

IBM Resilient IRP empowers organizations to respond to cyberattacks and business crises. It enables faster and more effective response through the orchestration and automation of IR processes. The platform works seamlessly with the prevention and detection systems that you already use so you can create a central hub for IR management.

For more information about the IBM Resilient IRP, schedule a demonstration today at http://info.resilientsystems.com/incident-response-platform-schedule-a-demo

About IBM Resilient

The mission of IBM Security is to help organizations thrive in the face of any cyberattack or business crisis. The Resilient Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. Many Fortune 500 companies, and hundreds of partners globally depend upon IBM for Resilient best-in-class security solutions.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2018

87014287USEN-00