Advanced Security Orchestration, Automation, and Response

Accelerate incident response with advanced security orchestration and automation.

Highlights

- Enables fast decisions and quick actions by the incident response team
- Integrates with 100+ security tools
- Automates repetitive, menial tasks
- Utilizes OODA Loops methodology
- Responds quickly to complex attacks

Overview

Organizations today battle complex cyberattacks that change as they unfold and more intel is gathered. Responding effectively has become more complicated than ever with complicated technology environments and a growing skills gap.

To combat this, security teams are leveraging security orchestration, automation, and response (SOAR) platforms to face these growing threats because it empowers analysts to make intelligent decisions and act quickly. Advanced incident response orchestration coordinates people, process, and technology both within the Security Operations Center (SOC) and across the organization.

The battle-tested IBM Resilient® SOAR Platform is programmed to help improve response times from hours to minutes by streamlining the response process.

Empower your response team

IBM Resilient SOAR Platform provides an advanced orchestration platform that fuels dynamic and accelerated response.

By automating repetitive and menial tasks and delivering the right information to the right analyst at the right time, orchestration with Resilient drives down mean-time-to-response and makes analysts more effective, efficient, and strategic.

A large pharmaceutical customer reduced the time it takes to obtain a forensics image from 84 minutes down to less than two by orchestrating and automating a key process with their response to threats.

"With Resilient, our time to respond to an emerging threat went from 84 minutes to under two minutes."

— Director of Cyber Security,
Global Pharmaceutical Company

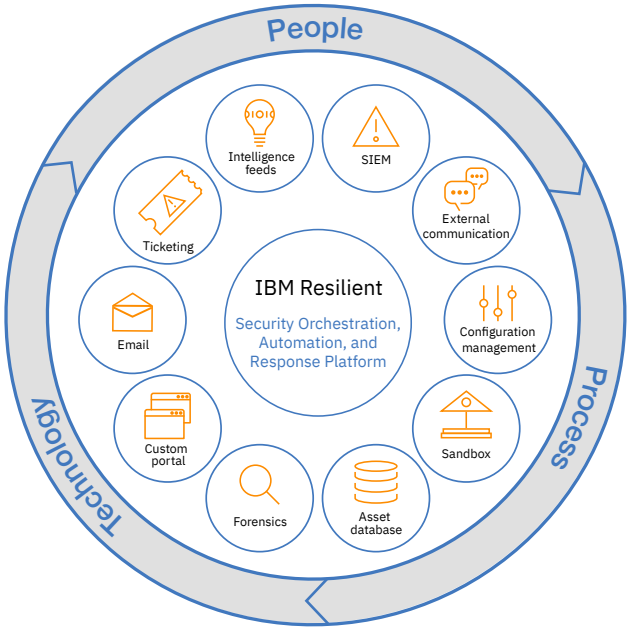

Figure 1: How the IBM Resilient SOAR Platform acts as a central hub for incident response orchestration.

Orchestration platform features

With the latest innovations to the IBM Resilient SOAR Platform, organizations have the tools they need to build an orchestrated, dynamic, and accelerated response program. Inspired by the OODA Loops (observe, orient, decide, and act) methodology from the U.S. Military, the Resilient SOAR Platform enables analysts to cycle through the OODA Loop process faster and more accurately.

And with the ability to integrate with more than 100 security tools, Resilient connects every aspect of your existing security environment with your IR process, forming a central hub for incident response orchestration.

The latest orchestration innovations to the Resilient SOAR Platform include:

- **Dynamic playbooks:** Provide the agility and sophistication needed to contend with complex attacks. Dynamic playbooks automatically adapt to real-time incident conditions and ensure repetitive, initial triage steps are complete before an analyst even opens the incident.
- **Visual workflows:** Enable analysts to orchestrate incident response with visually built, complex workflows based on tasks and technical integrations.
- **Incident visualization:** Graphically displays the relationships between incident artifacts or indicators of compromise (IOCs) and incidents in an organization's environment.
- **Timers:** Enable time-based rules in workflows that help teams ensure timely response, identify bottlenecks, and comply with organizational SLAs.
- **Artifact workflows:** Enable tools-to-tools automation workflows, while also allowing for people-centric tasks and approvals.
- **Tasks and scripts:** Add in-platform scripting functionality to workflows, enabling in-platform automation.

Benefits

With Resilient SOAR Platform, CISOs and their security teams can:

Accelerate response to complex attacks
Empowers security organizations to respond to complex attacks, demonstrate business value of the security spend, and increase ROI on entire security stack by integrating with more than 100 different technologies.

Improve and measure SOC productivity
Enables SOC Managers to increase and measure SOC productivity by integrating with existing security tools, and automatically adapting the response process to meet the attack. Enforces SLAs and ensures that the right analyst is working on the right tasks with the right tools.

Alleviate the skills gap
Acts as a force multiplier by enabling junior analysts to manage sophisticated threats and focus energy on investigation and response — rather than pivoting between tools — by automating triage and enrichment tasks.

Improve the data breach notification processes
Streamlines privacy response management by providing a knowledgebase of global regulations and response plans that instantly map to the latest regulations, taking the complexity out of fulfilling privacy breach regulations and obligations.

Orchestrate your response and empower your security team to act faster and more intelligently.

For more information

Schedule your demonstration of the Resilient Incident Response Platform today at: **ibm.com**/us-en/marketplace/resilient-incident-response-platform

© Copyright IBM Corporation 2019

IBM Corporation Security Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2019

IBM, the IBM logo, ibm.com, Resilient, and Resilient Systems, are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle

BUD03063-USEN-00