IBM Security
Whitepaper

Why an Incident Response Platform (IRP) is a better choice than ticketing

Most organizations have a ticketing system to deal with routine help desk requests, such as a forgotten password or broken laptop. Why not use it for incident response? Three reasons: Time, complexity, and intelligence.

Security incidents require rapid, dynamic, and decisive responses, and help desk requests aren't typically built for that. As incidents unfold, new information warrants changes in response — often in rapid succession. That means your incident response process requires a level of agility that ticketing systems aren't generally designed to deliver.

In reality, ticketing systems are meant to proceduralize routine tasks, not empower teams and other technologies to manage complex incidents. An effective response to security incidents requires a system that embraces complexity, and delivers the tools to help your team react faster, coordinate better, and respond smarter — without complicated programming or dedicated resources.

	Ticketing systems	IBM Resilient® Incident Response Platform
Confidentiality and user security; roles and responsibilities	• Response relies on individual discretion of those handling tickets • All-or-none permissions to an issue • Does not conform to regulations	• Information directed specifically to IT security teams or those who are involved with incident • Granular containment of information on a need-to-know basis
Effectiveness	• Limited tools to ensure follow-through, limited ability to take action on related security systems, limited data entry methods	• Your response team gets information it needs, when needed, including detailed instructions for assigned tasks. • Efficient data gathering
Customization	• Aimed at broad user set with nothing specific to incident response	• Made specifically to support incident response management
Maintenance and ease of use	• High level of technical skills required to implement, maintain and use • UI aimed at IT people, not typical users • Operational overhead of server and software maintenance and patching	• No additional maintenance or implementation resources required • Simple, easy to use UI, so training is not necessary • Maintenance tasks available via a simple Web UI, not an API or specialized programming language

Why an Incident Response Platform (IRP) is a better choice than ticketing

Consistency and repeatability	• Response relies on individual discretion of those handling tickets • Does not conform to regulations	• Incidents follow pre-defined, best-of-breed processes every time, independent of staffing • Supports simulations, playbooks, task tracking, and post-mortem • Allows tabletop incident training for consistent response
Compliance	• No knowledge base of regulatory requirements; you must create this on your own and track against it	• Response procedures include industry best practices and appropriate compliance requirements • Backed by audit-worthy reporting, PCI-compliant
Purpose	• General purpose IT solution	• Purpose-built for incident response management
Threat intelligence	• Has no built-in intelligence	• Includes an extensive knowledge base • Growing array of threat intelligence providers with automated artifact correlation across multiple systems
Reporting and analytics	• General reporting	• Custom executive reporting, specific to incident response. • Incident burn-down charts to ease status reports • Widgetized dashboards to streamline reporting and make it self-service

Scalability, customization, and updating	• Not incident-specific	• Updates continually, with no maintenance required from you • Automatic regulatory requirements updates • Regular best practice updates from expert partners • Easy to customize via the web UI, not an API or via specialized programming expertise
Incident response expertise	• None	• Considerable vendor and industry best practice expertise to inform your incident
Integration	• Not integrated into your security infrastructure	• Easily integrated into your security infrastructure, including existing ticketing systems, SIEMs and escalations from other systems
Time savings	• Incident response process has to be built from scratch	• Includes more than a dozen, best practices-based runbooks. • Incident response time decreases — getting you back to business faster • No training required • Turns response into resilience
Support	• No incident response-specific support	• Considerable support resources • Community driven best practices from expert partners

For more information

To learn more about this offering, contact your IBM sales representative or visit **ibm.com/**us-en/marketplace/resilient-incident-response-platform.

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

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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.