Evolution of Incident Response

Shifting to Full Incident Management in Today's Threat Landscape

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper

August 2017

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Evolution of Incident Response: Shifting to Full Incident Management in Today's Threat Landscape

Table of Contents

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Evolution of Incident Response: Shifting to Full Incident Management in Today's Threat Landscape

The Evolution of Incident Response

A recent global survey revealed that data breach and data theft outranked natural and manmade disasters and IT system failures as the largest threat to an organization's reputation.[1]

It's not hard to understand why. The demands of digital business push organizations to increase the flow of data between suppliers, partners, and customers to create seamless experiences that enhance and accelerate the customer experience. But that very same connection increased the risk associated with now seemingly continuous data breaches and hacks. According to the 2016 Verizon Data Breach Investigation Report (DBIR),[2] a hacker can compromise an environment in minutes, wreaking havoc not only within the business's "four walls," but to every piece of its connected business including clients, partners, and suppliers.

The role of incident response (IR) can no longer be confined to a reactive process of opening a ticket, fixing a system, and closing the incident. Full incident response is proactive, and coordinates people and information to involve the right stakeholders and invoke quick decision-making and communication that protects brand value.

The role of incident response (IR) can no longer be confined to a reactive process of opening a ticket, fixing a system, and closing the incident.

Instead of treating the symptoms of an incident, as incident response was traditionally handled, the team now finds itself taking the lead role of not only addressing the outward technical issues, but also orchestrating people, processes, and technologies across the organization. This includes both technical and management stakeholders.

Operating in this new reality requires end-to-end visibility of complex landscapes and real-time access to data that will allow IR teams to trigger action quickly to speed cross-departmental collaboration and mitigate damage.

What's Holding Back More Effective Incident Response?

Most organizations invested heavily in automating protection and detection capabilities, but IR proved more challenging to automate because it has unique, human-centric requirements. However, even though there are common elements to incident response processes, there are also many variations to process, manage, and track different incidents in different organizations. This means, prior to the release of IR platforms as a technology solution, organizations had two choices.

First, and most commonly, teams were left to pull together information on alerts across complex, networked infrastructure from various systems manually, tracking it in paper binders, Word and PDF documents, and spreadsheets. They coordinated response through email.

Second, firms looking to augment incident response capabilities had to contract outside services to build a custom response platform for the task; a highly expensive and rigid solution.

The lack of a real-time, consumable, end-to-end view of data across security architectures creates indecision and increases risk. This slows response and complicates communication to customers, internal and external stakeholders, and support organizations such as legal staff and law enforcement.

[1] Forbes Insights
[2] 2016 Verizon DBIR

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

EMA Perspective: What Would Empower More Effective Incident Response?

The time is right for technology to further empower IR teams to create efficiencies and realize greater success internally. By creating orchestrated playbooks that leverage automation to support security analysts and can be executed within the system rather than by using isolated documents, the organization can standardize and expand its response strategy.[3] This will facilitate the flow of information among cross-organizational stakeholders and technical staff to expedite action and mitigate risk. An incident response platform helps teams orchestrate a robust response across people, processes, and technology by:

Serving as a hub for operational security data. Teams can easily consume real-time threat information from a myriad of security systems, placing the key information into a single repository. Analysts can then vet these leads for further investigation or identify them as dead ends.

Enhancing inter-organizational communications with a "360-degree view" of the threat. Information feeds, such as internal and external threat feeds, network intelligence, technical process requirements, and communications, need to create the ability to swiftly and accurately communicate relevant factors in a consistent manner to help put the threat into context to reduce risk. Integrating threat intelligence feeds directly into the incident response process enables immediate and actionable intelligence.

Giving a baseline for continuous improvement. With automated workflows and consistent, efficient response plans, organizations can deliver best practices to respond to evolving and ever-increasing threats.

IBM Resilient stands ahead in offering a platform for IR orchestration that enables organizations to manage the entire response process including all the technology, processes, and people needed for a full, effective, intelligent response. IBM Resilient's Incident Response Platform synthesizes and translates alerts to trigger step-by-step, role-based workflows. Based on industry best practices, the workflows are customizable according to the customer's own security framework. Visualization capabilities allow organizations to see an attack underway and how they are dealing with it. Dashboards and analytics enable security teams to fulfill regulatory compliance and provide insight to executives on incidents faced, response processes, and results.[4]

Resilient's Incident Response Platform synthesizes and translates alerts to trigger customizable, step-by-step, role-based workflows based on industry best practices.

Some market-leading capabilities of the platform include:

Dynamic Playbooks: Comprehensive IR playbooks that adapt in real time to the details of a cyber attack, providing dynamic action plans and best practices for responding to all incident types (from malware to DDoS to lost devices). Dynamic Playbooks are core to IR orchestration, enabling tools automation, enhancing collaboration between internal stakeholders, and driving down time to remediation.

Visual Workflows: Enables analysts to orchestrate incident response with visually-built, agile, and complex workflows. With Visual Workflows, security teams can coordinate the tasks that require action, enforce order and dependencies to perform correct tasks, and leverage technical integrations and automation.

[3] Bruce Schneier Blog-The Future of IR
[4] Resilient Datasheet

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Incident Visualization: Incident Visualization enables analysts to see connections between incidents and artifacts, helping them understand relationships between multiple IOCs and incidents in their environment, zero in on concerted attacks underway, and respond faster. Additionally, analysts can uncover broader campaigns, see how an attack unfolded over time, and take investigative or remedial actions directly from within the tool.

Action Module: The Action Module enables security teams to create a hub for incident response by integrating IT and security systems, and automating and orchestrating workflows. The Action Module allows for scripted actions, such as opening and updating IT tickets, gathering intelligence or forensics data, or quarantining or reimaging infected machines, which allows users to focus on more strategic tasks and resolve incidents faster and more effectively.

Privacy Module: With the EU's General Data Protection Regulation, or GDPR, going into effect in May 2018, organizations globally are working to prepare their notification and compliance processes today. The challenge is that privacy breach response is lengthy, tedious, and expensive. The Privacy Module transforms the process into one that is fast, efficient, and compliant. Built on a continuously updated database of global privacy regulations like GDPR, the Privacy Module provides data breach response plans that are pre-mapped to applicable regulations. These plans take the complexity out of tracking privacy breach legislation, industry regulations, company-specific obligations, third-party requirements, and industry best practices. Additionally, the Privacy Module provides a GDPR Preparatory Guide and Simulation to help organizations streamline IR and breach notification time, achieve compliance, and avoid penalties.

IBM Resilient's capabilities enable organizations to speed resolution, with one customer saying the platform enabled the team to manage incidents in one-tenth of the time it previously entailed. With a deeply experienced team behind it, including security thought leader Bruce Schneier as CTO, the platform is poised to continue delivering on its mission: to empower security teams to better prepare for and respond to the growing number of security incidents they face every day, and ensure all organizations can thrive in the face of rising cyber threats.

Customers using the IBM Resilient Platform are now able to speed incident resolution by as much as *ten times*.

About IBM Resilient

IBM Resilient's mission is to help organizations thrive in the face of any cyberattack or business crisis. The industry's leading 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. With Resilient, security teams can have best-in-class response capabilities. IBM Resilient has more than 200 global customers, including 50 of the Fortune 500, and hundreds of partners globally. Learn more at www.resilientsystems.com.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3588.082217