Security Incidents: Who is coordinating a response?

With the number of cyber threats on the rise – not only in terms of the number of attacks but in terms of the impact and resulting disruption as well, even enterprises known for their information security standards have come under scrutiny.

National Institute of Standards and Technology (NIST), a part of the U.S. Department of Commerce, is responsible for developing information security standards and guidelines. In August 2012, it released a special publication, SP 800-61 Revision 2, "Computer Security Incident Handling Guide" that is widely accepted as an authority document on incident handling, incident analysis, and incident response.

NIST 800-61 Revision 2, in its abstract, states, "Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources."

With the number of cyber threats on the rise – not only in terms of the number of attacks but in terms of the impact and resulting disruption as well – even enterprises well-known for their information security standards have come under scrutiny. In recent years, data breaches have been reported at an increasingly worrying array of companies – Tesco Bank, Yahoo, Target, Anthem, Ashley Madison, eBay, JP Morgan Chase, Home Depot, Sony Pictures Entertainment, Global Payments Inc., Tricare, Citibank, Heartland Payment Systems, etc.

What's happened to these organizations can happen to anyone. Truly determined cyber attackers can find a way through any number of intrusion detection and prevention applications that might be in place. According to Ponemon Institute's "2016 Cost Of Data Breach Study: Global Analysis", there is a 26% likelihood of a company having one or more data breach occurrences in the next 24 months, with the potential material data breach involving 10,000 lost or stolen records. The same study found that the cost of a data breach is significantly higher if the breach takes longer than 30 days to contain.

Most organizations invest heavily in defense, which is appropriate. For obvious reasons, proactively preventing problems through effectively securing applications, firewalls, networks, systems etc. is likely to be more cost effective than reacting to problems after they occur.

However, most security incidents do not follow a blueprint. These incidents can vary widely in nature and impact. The Incidents can be generated by malicious third parties, but can just as likely occur due to system failures or human errors; rendering it impossible to have a 100% assurance that your prevention methods are successful.

What is a security incident?

While organizations can develop their own definitions of security events and incidents, there are some generally accepted definitions.

A security event is an occurrence or an observation the represents an anomaly. This can be anything that represents an abnormal activity – including system glitches, or a firewall blocking a connection attempt. Events with negative impact – like a malware attack – are considered adverse events. Security Incidents are either an imminent threat or a current violation of information security policies, standards or acceptable use.

In the 2016 Incident Response Survey by Custom research, **93% of the responders** said that their ability to respond to a security incident was either significantly or somewhat limited by the burden of manual processes.

NIST lists a set of attack vectors, including the following:

1. External / Removable media
2. Attrition (According to NIST, attrition is "An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.")
3. Web
4. Email
5. Improper Usage
6. Loss or theft of equipment
7. Others

Clearly, each of these different types of incidents requires a different approach for identification, analysis and response.

Since incidents tend to impact or compromise sensitive data, including Personally Identifiable Information (PII), cardholder data and sensitive authentication information (PCI), Patient Health Information (PHI), etc., it is critical to respond quickly and effectively when security breaches occur.

The Challenge With Responding To Incidents

Your organization most likely employs a number of detection systems like Security Information & Event Management (SIEM) systems, Firewalls, Security Endpoints, Identity & Access management tools, Threat Intelligence and Vulnerability detection tools, and other network security systems. Using all of these typically results in a lot of "noise" – generating thousands of events per day and terabytes of data per month. Sifting through these events and separating the wheat from the chaff requires significant effort and manpower - generally Security & IT teams cannot scale to manage.

Acting on this noise requires organizations to be in a position to not only consolidate all this information, but also have the capacity to understand the business impact and prioritize the incidents by their risk profile and the organization's security posture.

Mapping the security incident to the business services and the configuration items it is most likely to impact (or is already impacting), establishing and executing a workflow to arrest and remediate the breach, and enabling cross-department coordination ends up being the most time-consuming aspect of the response coordination.

Security responders are typically overwhelmed by the size and disruption; or, even more worryingly; may not have a true understanding of the business impact or prioritization for the incidents. This generally happens because responses are coordinated and managed manually, through the use of excel spreadsheets, emails, chat sessions etc. There is no prior knowledge base with historical information that captures what activities or tasks were performed the last time a similar incident occurred. Enterprise Strategy Group (ESG) Custom research conducted a survey, "Incident Response Survey," in 2016, in which 93% of the responders said that their ability to respond to a security incident was either significantly or somewhat limited by the burden of manual processes.

ServiceNow Security Operations leverages the platform's native ITIL capabilities and NIST 800-61 guidelines to provide organizations with the ability to respond to security incidents more efficiently and effectively.

ServiceNow Security Operations

ServiceNow Security Operations leverages the platform's native ITIL capabilities and NIST 800-61 guidelines to provide organizations with the ability to respond to security incidents more efficiently and effectively.

It integrates with 3rd party detection systems to consolidate threat information, prioritize incidents and provides request automation between IT, Information Security and Business teams.

ServiceNow Security Incident responder automatically creates a security incident and uses data already available in ServiceNow's Configuration Management Database (CMDB) to list the critical business services impacted by the compromised assets. In addition, ServiceNow integrates with the National Vulnerability Database to gather intelligence related to known vulnerabilities, allowing the responder to "enrich" the security incident data.

This enables responders to quickly determine the response, remediate threats fast by launching the appropriate emergency patches to these assets, set SLAs for activities to be performed by other teams, and to automate communications and notifications.

Conclusion

With a stack of several applications already within your Security Operations portfolio, you might be wondering whether you need to add one more.

The reality is that the systems you already have in your technology stack are most likely geared towards identification and prevention; but not towards coordinating and automating security incident responses, or towards generating alerts, notifications or communications. It's also likely that your security operations systems are not integrated with your CMDB and /or service management platforms, and thereby you are missing the opportunity to automatically catalog and prioritize incidents, based on vulnerability risk and business service impacts.

ServiceNow Security Operations solves that gap in your current capability maturity.

Integrhythm works extensively with organizations looking to implement ServiceNow GRC and Security Operations applications to

a) Improve cross-department collaboration during the Security Incident Response process
b) Streamline remediation by using predefined workflows and automating routing tasks
c) Configuring security dashboards that enable you to measure and report on your overall security metrics

For further information regarding our approach, or to know more about ServiceNow's Security Operations capabilities, please contact us at ***info@integrhythm.com***. We're here to help.

Integrhythm Inc.

www.integrhythm.com
lnked.in/integrhythm
info@integrhythm.com