FORTINET

WHITE PAPER

Prepare for the Unpredictable: Why Specialized Skills and Tools are Needed for Effective Incident Response

Executive Summary

The digital attack surface is expanding at an astronomic pace. There are "edges" everywhere, giving cyber criminals nearly endless entry options to enterprise networks. Further, the threat landscape continues to evolve with ever-more sophisticated attacks and evasive techniques. The reality today is that it is not possible for organizations to stop every threat before it enters the network.

When an organization discovers an incident, it needs to respond immediately to minimize the damage. Understanding the nature, scope, and risks posed by the incident in order to correctly respond requires specialized tools, skills, and repeatable processes. Organizations need specialized personnel to enable effective threat mitigation.

Nearly 80% of organizations are introducing innovations faster than their ability to secure them against cyberattacks.[1]

"Time is money and being slow to detect and contain a breach can be costly … It now takes a combined 279 days to identify and contain a breach, up from 266. Speedy responses could be a massive cost saver. Companies able to detect and contain a breach in under 200 days spent on average $1.2 million less."[3]

Breaches Are Inevitable and Immediate Response Is Critical

The corporate network, branch offices, remote users and devices, and cloud assets are all vectors that threat actors are finding new ways to attack. "With the boundaries between what's inside the firewall and what's outside becoming less and less discernible, an organization's attack surface—everything it needs to worry about defending—now begins inside the corporate network and extends all the way to the outer reaches of the internet, even into the homes of employees."[2]

The sudden and widespread switch to remote work has increased the enterprise attack surface very quickly. It's a daunting task to protect every device that finds its way onto a network. Many of these devices may not even be known to IT, but are still a potential entry point for attackers.

In addition, attacks continue to accelerate in speed and sophistication. For example, malware automation and evasion techniques make it not only difficult to stop but also help it spread very quickly. There have also been more targeted attacks specifically featuring ransomware. Adversaries are taking a bit more time doing some reconnaissance to target a specific victim. They are in the environment for weeks at a time, mapping it out, circumventing security controls. The longer they lurk, the more damage they will do. This time gives them the opportunity to not only drop the ransomware payload but also to figure out ways to exfiltrate your data and then hold that information hostage as well.

Even in cases that don't involve ransomware, the longer an attacker spends in your network, the more access they can get to devices, data, and accounts. This increases the impact of the breach and also drives up the amount of time needed to remove them and their access, also driving up the cost to remediate.

Organizations are realizing that they can't escape breaches, but they can mitigate them. Putting an incident response (IR) plan in place **before** there is an incident is key to any cybersecurity strategy.

What Is Incident Response?

IR is the process of detecting, investigating, and managing the fallout from a security incident or breach. The goal is to limit the amount of damage (cost and reputation) caused by the attack and reduce recovery time.

But this process requires specialized teams, the right tools, and repeatable processes.

Incident Response Skills

Most medium-sized organizations and enterprises have staff that are responsible for at least the daily operation of security tools. However, these tools are typically focused on threat prevention, and teams are tasked with deployment, configuration, and ongoing management of the toolset. Further, these security administration tasks are often just one of many responsibility areas shared by the team. As such, day-to-day security operators typically need a wide range of IT and security product knowledge, but have limited time or experience with IR.

By contrast, when an organization is in the midst of a breach situation, a completely different set of emergency skills and cybersecurity knowledge are required. These include expertise in:

- Authentication and access controls
- Security vulnerabilities
- Protocol design
- Malicious code analysis
- TTP of the adversaries
- Implementation flaws
- Configuration weaknesses
- Log analysis including OS (Windows and Linux, Apple), network (firewalls, proxies, SIEM, PCAP)
- Digital forensics

In short, they need to understand the tools and trade of the cyberattacker, rather than the technologies and operation of cyber defense. And, given the rapidly evolving cyber threat landscape, to do so they also need to be passionate about their responsibilities and keep current with the latest tactics, techniques, and procedures used by threat actors.

Incident Response Tools

Similarly, these teams require a different toolset. While the prevention-oriented security controls operated on a day-to-day basis may raise warning signs that an incident is in progress, if they were able to identify them definitively, the attacks would have already been stopped.

For example, a next-generation firewall may block known threats and rate additional threats as medium risk, but it will still have let the medium risk attacks pass by design. Further, that medium risk designation will typically not provide a definitive classification and thus require investigation. Otherwise it would have been given a higher risk rating.

In regard to endpoints, an endpoint protection platform (EPP) may stop a lot of known malware or malicious system activity, but it may also raise flags about suspicious behavior based on heuristic scanning that it still allows to run on the machine. Again, further investigation is required.

Organizations must be prepared for these situations and provide the specialized teams with specialized tools for detection and analysis, as well as threat intelligence and hunting.

Detection tools. These should identify threats and atomic indicators such as IP addresses, plus URL- and domain-computed indicators such as file hashes and detailed signatures. Most importantly, they need to identify the behaviors.

Analysis tools. Once something is detected, the right tooling is needed to automate the analysis of files that may be found on disk, or fileless malware in memory. Extracting that information and performing automated and human analysis are required to be able to determine what the malware is actually doing in a timely and effective manner.

Threat intelligence. Once indicators of compromise (IOCs) are discovered, threat intelligence can enrich the information to provide context.

Hunting. A hunting capability will enable the organization to take all the information gleaned from the analysis phase and ensure the full scope of the breach or security incident is understood.

Incident Response Process

All response actions need to occur much faster (and with greater accuracy) than standard operations. Given the high-pressure nature of IR, even the most experienced staff with the proper tools benefit from a well-defined process that is completely different than the norm. Consider:

- Patches come out every month, on a Tuesday, yet organizations still take 30 days or more to deploy them.
- Software upgrades are released multiple times a year, yet organizations often remain one or more versions behind.

The list of standard operational processes goes on and response times are varied—and in many cases that's OK. Not so for IR. As NIST noted in its Computer Security Incident Handling Guide in 2012, "Real-time availability is the best for incident response because the longer an incident lasts, the more potential there is for damage and loss."[4] Not much has changed since then. Accordingly, as soon as an incident is raised, a whole series of activities—many with uncertain outcomes and variable next steps—need to kick off and proceed as quickly as possible. This is why well-defined processes for each potential situation are absolutely essential.

Despite the rapid proliferation of new cyber threats, 77% of business leaders admitted that they don't have a formal cybersecurity incident response plan (CSIRP) that's applied consistently in their organization.[5]

Two Approaches to IR Teams

With today's rapidly expanding attack surface and increasingly sophisticated attacks, enterprises cannot keep out every threat. Fast and robust IR is required to minimize the damage from breaches. It's very important to have the right incident responders, tools, and documented actions. IR teams can be established in-house, or IR services can be contracted. To help you decide which approach is best for your organization, read our checklist, "Top 5 Considerations for Deciding Whether to Outsource Incident Response or Create an In-house Team."

[1] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[2] Lucian Constantin, "Enterprise internet attack surface is growing, report shows," CSO, June 11, 2020.

[3] Dan Swinhoe, "What is the cost of a data breach?" CSO, May 8, 2020.

[4] Paul Cichonski, et al, "Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2," NIST, August 2012.

[5] Conner Forrest, "Report: 77% of companies don't have a consistent cybersecurity response plan," TechRepublic, March 14, 2018.

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

August 21, 2020 5:45 AM

750405-0-0-EN

D:\Fortinet\White Paper\Teal White Paper\TEAL - Fortiguard Incident Response\wp-FA-prepare-for-the-unpredictable-8212020\wp-FA-prepare-for-the-unpredictable-8212020