DARKReading

NOVEMBER 2022

Sponsored by

MANDIANT

NOW PART OF Google Cloud

Creating an Effective Incident Response Plan

Security teams are realizing their organizations will experience a cyber incident and that they need an effective incident response plan — one that takes into account their requirements and has been tested.

INSIDE:

Brought to you by

informa tech

FEATURE

Creating an Effective Incident Response Plan

Security teams are realizing their organizations will experience a cyber incident and that they need an effective incident response plan — one that takes into account their requirements and has been tested.

By Jeffrey Schwartz, Contributing Writer, Dark Reading

Business leaders and the boards of directors they report to are increasingly accepting the uncomfortable reality that there is little question that their organizations will fall victim to a cyber incident — but when, and how material will it be?

Dismissing the current risk of an attack puts leaders at risk of breaching their fiduciary responsibilities to their shareholders, customers, and business partners. Naturally, this requires them to double down on their investments in maintaining comprehensive cyber-protection strategies. But even those who do are never entirely immune to a potential breach. Consequently, no cybersecurity protection plan can be complete without an effective incident response plan.

The Rise in Material Breaches

Despite global spending of $77 billion on cybersecurity protection technology and services in 2022, the number of data breaches — including malware, ransomware, and brute-force attacks — continues to rise. In 2021, there were 15.1% more incidents than the previous year, and material breaches soared by nearly 25%, according to a ThoughtLab survey of 1,200 business and technology leaders. The actual figure is likely much higher because of the number of unreported attacks and breaches.

Ransomware attacks that use more sophisticated social engineering tactics and business email compromise (BEC) techniques are contributing to the surge in incidents.

Security leaders anticipate such attacks will continue to escalate during the next two years. The discovery of new and more pervasive vulnerabilities, such as Log4j, contributed to the sharp rise in attempted cyberattacks in late 2021. According to a Check Point Research survey, the number of attempted attacks per week on corporate networks worldwide increased 50% last year compared with 2020.

An external attacker can breach and gain access to the network resources of 93% of organizations, according to a survey by Positive Technologies. Further, 100% of respondents to the survey acknowledged that an internal attacker could gain complete control of their networks. The survey also revealed that nearly a third of CISOs and CEOs are unprepared to respond to the changing threat landscape.

Growing Focus on Incident Response Planning

Many organizations don't have effective incident response plans. A 2021 Ponemon Institute survey found that only 46% have specific incident response plans for at least one of eight cyberattack types: DDoS, malware, phishing, insider incident, BEC, disaster recovery, supply chain attack, and advanced persistent threats (APTs).

The good news is that organizations are becoming more proactive about creating a plan rather than realizing after an attack that they needed one, says LeeAnne Pelzer, consulting director and leader of Unit 42, Palo Alto Networks' cybersecurity consulting practice. Pelzer notes that, a few years ago, whenever her team was called in to create an incident response plan, it was always after the client had suffered an attack. Now, she adds, "they're starting to allocate time, money, and energy toward getting in front of an incident before it actually occurs."

Many organizations' incident response plans are "shelfware," Pelzer says. "They aren't written in a way that [they] can actually be used when you're going through what could arguably be your worst day at work and your brain is not firing on all cylinders."

> **"What really drives the maturity of companies' incident response plans is going to be the regulations."** —Michael Corcione, Principal of PFK O'Connor Davies

The plans often lack incident categorization and call trees with defined roles and responsibilities, experts say. They also don't always specify procedures for how to address ransomware attacks and whether to pay attackers.

Michael Corcione, principal of the PFK O'Connor Davies cybersecurity and privacy advisory service, conducted 40 different incident response reviews for new clients during a three-month period. Corcione says all of the clients had an incident response plan in some form, but the plans varied in maturity.

"Quite a few have plans, but they are not formalized or documented," Corcione explains. He emphasizes that these are private companies that aren't beholden to industry or SEC regulations. "What really drives the maturity of companies' incident response plans is going to be the regulations," he says. "For example, health care is very heavily regulated, as well as financial services. You won't see a financial service company that doesn't have an incident response plan."

Coordinating an Effective Response Plan

Greg Kelley, founder and CTO of Vestige Digital Investigations, says the first step in creating an incident response plan is to define the prominent people in the organization who will respond to an incident. Typically, that includes the CEO, presidents, or other C-level executives, as well as legal, IT, public relations, and department managers.

Experts widely recommend aligning an incident response plan with the National Institute of Standards and Technology's (NIST's) recommendations published in its Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2). Among its many recommendations, the NIST framework breaks down four steps organizations should take to build their plan:

1. **Preparation:** Build and maintain an incident handler communications plan with contact information, incident reporting mechanisms, an issue tracking system, a war room, and encryption software for communications.
2. **Detection and analysis:** Understand attack vectors such as malware in email, malicious websites, impersonation, removable media, brute force, and unusual activity, and use alerting tools including IDPSs, SIEMs, antivirus and antispam, and logs. For analysis, this should include network system profiling, understanding normal behaviors, creating log retention policies, and performing event correlation.
3. **Containment, eradication, and recovery:** Identify attackers by validating host IP addresses, using incident databases, monitoring attackers' communications channels, and researching through search engines. The response team should conduct eradication and recovery in a phased approach based on prioritization.
4. **Post-incident activity:** Determine how the organization may have avoided an attack by posing questions including: What happened? When? and What steps did the response team take that may have impeded recovery?

Setting Expectations and Customizing the Response Playbook

"NIST and other frameworks definitely set the foundation, and they give you the guardrails to stay within," PFK O'Connor Davies' Corcione says. "But when doing an assessment and review with a company, it's much better for us to have a dialogue with them."

The first important step is that the sponsor of an incident response plan must have the full support of leadership. Without leadership buy-in, the incident response plan will be destined to fail. Leadership must be on board with the overall approach and strategy, and willing to allocate budgets and resources toward the procedures that the incident response plan will include.

The first important step is that the sponsor of an incident response plan must have the full support of leadership.

It's critical to understand what company leaders want to get out of an incident response plan. They may want something like a granular playbook for different attack types, or they may be looking for a more generic "drive the ship" plan.

There are five other base components of an incident response plan:

1. Definitions and categorizations, such as what constitutes an event versus an incident and at what point is it a crisis?
2. A severity matrix that prioritizes each incident category. It should be clear when an incident falls into the different severity categories.
3. Roles and responsibilities that specify the core incident response team, including the decision authorities, senior executives, directors, external counsel, forensics, public relations, and insurance providers.
4. Communications plan that includes internal stakeholders as well as a lawyer-approved template specifying an appropriate plan of whom to contact first and when.
5. A training, testing, and maintenance schedule that includes simulated tabletop exercises that address the different attack vectors.

Testing and Tabletop Exercises

Developing a plan doesn't end once everyone has signed off on it and created playbooks for various scenarios. Experts say organizations should update the plan at least once yearly or after a significant event, including an incident or major infrastructure changes.

To ensure that an incident plan will actually work requires testing it under various simulated attacks.

"If the team feels comfortable leveraging these documents, it's usually a pretty seamless process," says Unit 42's Pelzer. "However, they might find that depending on their unique processes, or their tech stack, that maybe the incident response plan is not resonating with them as much."

While some organizations may find tabletop exercises too difficult or cumbersome to run, they play an important role in defense and incident response. It is essential to test all aspects of an incident response plan to verify that the executed actions generate the expected results. For instance, many organizations rely on the offline backup capabilities with their disaster recovery systems to recover their data in the event of a ransomware attack. However, failing to test that process during a ransomware response tabletop exercise can have devastating consequences.

Vestige Digital Investigations' Kelley points to an incident where a client asked his firm to determine what caused an attack. The client wanted to determine if someone intentionally created the vulnerability that was exploited, or if it was an oversight. Kelley's firm found that the attacker gained access because the Active Directory domain settings gave every employee admin rights. Effectively, this meant that every employee had access to everything on the system, a practice no organization would intentionally permit.

To determine what happened, Kelley wanted to see the backups of the Active Directory domain controllers. Kelley recalls: "The top executive said, 'Sure, we back up our domain controllers.' So, he called in the manager one level down, who then brought in the backup administrator. And the admin said, 'Oh, that process has been broken for six months, and we don't know why.' And the IT director turned to him and said, 'So, if Active Directory completely crashed, we would have to build [the controllers] from scratch?' And he said, 'That's right.' It was an uncomfortable moment."

Kelley notes that such failures often happen in organizations because administrators are good at what they do but don't understand the bigger picture. "He knows it's important that those servers are backed up, but what he doesn't know is what reliance the people up the food chain are putting on that process to work and how important it is to them that that process works," he says. "It's the two-way communication that breaks down."

The first important step is that the sponsor of an incident response plan must have the full support of leadership.

Corcione frequently sees the same types of issues. "There's definitely a challenge with organizations doing role-based training, specifically for the people in incident response," he says. "What you have in the security world is a lot of people who have moved up through the information technology space. But the response is a little bit different mindset. When you get into incident response, it's really a big part of what's going on from a business perspective. It's not just a system that went down; we must bring it up. It's the prioritization around the system."

An incident response plan must prioritize what business processes are most important, with an understanding of what systems must be restored first. Corcione emphasizes that this process must be incorporated into the tabletop exercises and should include representatives from across the business.

"A lot of times, the IT team will go out and do an exercise and then say, 'OK, technically, we took care of it all,' but they didn't involve the line of business. Communicating through those plans and doing role-based training on those responses is important but is an area where many firms lag."

Previous Next

Putting Disclosure Policy into the Plan

Response plans should include an intra-organizational protocol for informing stakeholders of an incident, but they also must address disclosure to affected parties, including customers, partners, and suppliers. Insurance companies often require that their clients contact them before anyone else, though most experts say the first call should be internal and go to legal counsel. The decision-making on what to disclose and when is increasingly falling under the auspices of industry regulations, as well as state and federal laws.

The decision-making on what to disclose and when is increasingly falling under the auspices of industry regulations, as well as state and federal laws.

New York was the first state to formalize regulations requiring banks and insurers, among others, to report cybersecurity incidents. The New York Department of Financial Services (NYDFS) regulation was enacted in 2017. "It is, in my view, still the strictest in the world because it requires somebody to sign off on an attestation," Corcione says.

Nearly two years after the NYDFS regulation went into effect, the enforcement team found that 80% of the incidents reported were preventable if the affected firm implemented multifactor authentication, according to Corcione. "That intelligence really helps the community, and that's what we're trying to get at," he says.

The unprecedented ransomware attack against Colonial Pipeline in May 2021, which shut down the 5,500-mile fuel pipeline for nearly a week, showed the catastrophic implications of an incident. President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) in March. The new law mandates that providers of infrastructure in 16 industries identified by the federal government report a cyberattack to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and within 24 hours of making a ransomware payment.

A month after that law was enacted, similar regulations went into effect for banks. As of April 1, all banks covered by the Federal Deposit Insurance Corp. are required to notify the agency of a cyber incident within 36 hours of discovering it.

Now pending is a proposal by the Securities and Exchange Commission (SEC) that would mandate disclosures of incidents by all publicly traded companies and other companies for which it has oversight. SEC chair Gary Gensler issued a statement on the proposal in March, just after Biden signed the CIRCIA legislation. "A lot of issuers already provide cybersecurity disclosure to investors," according to Gensler's statement. "I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."

Concerns About Disclosure Requirements

There are conflicting issues regarding required disclosures, especially regarding timing. The concern is that premature disclosure could weaken a victim's hand when negotiating with attackers. Worse, it could antagonize attackers into taking severely damaging actions. Corcione notes that cases can occur when an attacker's claims are confirmed as hoaxes after the victim investigates its exfiltration logs. Also at issue, according to Corcione, is the type of attack that is material enough to warrant disclosure.

"Materiality is really big," he says. "The SEC is dealing with the question of what is that definition of materiality. And then, also, when do the clocks start ticking on the reporting requirement? Is it from when the incident started or from when materiality was determined? These are issues that need to be resolved."

Increased Influence of Insurance Carriers

Soaring ransomware attacks have led insurance companies to play a central role in incident response planning. Before underwriting or renewing a cyber insurance policy, insurers have stepped up the requirements they're placing on their clients. Corcione notes that insurers are now requiring clients to validate their claims. "The insurance industry on the cyber side for years has been doing their policy underwriting on a trust aspect," Corcione says. "A client provided self-attestation, and everything was in place."

But as insurers started investigating claims more closely, they discovered that not all their clients' assessments were accurate. "Quite a few cases have come up recently where insurers are looking not to pay because people have said that they have multifactor authentication in their organization, but it turns out there was a breach. And while they had multifactor, they didn't have it across the entire organization," Corcione says. "In these cases, the attackers came in through the area where they didn't have it."

Insurers now require third-party attestation or hire experts to assess a client's cybersecurity infrastructure and incident response plans. "They're asking not only do you have an incident response plan, but are you specifically doing tabletop exercises for ransomware attacks," he says.

Coordinating IT and Business Operations

In addition to requiring buy-in from a board of directors and CEO, effective security incident management plans must include coordination between IT and the business. When IT and top management aren't on the same page, it is challenging to implement a proactive incident response plan.

Insurers now require third-party attestation or hire experts to assess a client's cybersecurity infrastructure and incident response plans.

Braden Perry, a litigation, regulatory, and government investigations attorney with law firm Kennyhertz Perry, says it's vital that the CISO understands business operations and processes and can translate technical issues to the CEO and board.

"It's becoming more critical, and almost imperative, that a committee has an experienced IT and cybersecurity liaison to be the go-between and translate the IT language into business and vice versa," Perry says.

Unfortunately, most CEOs and board members defer on issues they don't understand. "When an IT department presents a robust plan for proactive IT security, it may go ignored or disregarded," Perry says. "This can lead to a reactive plan only that focuses on the when as opposed to prevention."

Similarly, Perry emphasizes that companies should have at least one board member who is knowledgeable about IT security and can communicate it to others. "When I am engaged to investigate and report, it ordinarily is an issue that could have been resolved without outside counsel," Perry says. "But a lack of clear communications between IT and the board stymied that understanding."

About the Author: *Jeffrey Schwartz is a journalist who has covered information security and all forms of business and enterprise IT, including client computing, data center and cloud infrastructure, and application development for more than 30 years. Jeff is a regular contributor to Channel Futures.*

Previous Next

New Cross-Industry Group Launches Open Cybersecurity Framework

Eighteen companies, led by Amazon and Splunk, announced the OCSF framework to provide a standard way for sharing threat detection telemetry among different monitoring tools and applications.

By Jeffrey Schwartz, Contributing Writer, Dark Reading

Amazon Web Services (AWS) and Splunk are leading an industry effort of 18 systems and security vendors to standardize how different monitoring systems share security alerts. The goal is to deliver a simplified and vendor-agnostic taxonomy to help security teams ingest and analyze security data faster.

The companies announced the Open Cybersecurity Schema Framework (OCSF) during the Black Hat USA conference. The participating companies are Broadcom (Symantec), Cloudflare, CrowdStrike, DTEX, IBM Security, IronNet, JupiterOne, Okta, Palo Alto Networks, Rapid7, Salesforce, Securonix, Sumo Logic, Tanium, Trend Micro, and Zscaler.

Detecting and stopping today's cyberattacks requires coordination across cybersecurity tools, but many of these tools are not interoperable, and there are too many different data formats. The OCSF specification will normalize security telemetry across various security products and services, Mark Ryland, director of the office of the CISO at AWS, wrote in a [blog post announcing the project](#).

"Security teams have to correlate and unify data across multiple products from different vendors in a range of proprietary formats," Ryland wrote. "Instead of focusing primarily on detecting and responding to events, security teams spend time normalizing this data as a prerequisite to understanding and response."

OCSF, which extends the [ICD Schema specifications](#) originally developed by Broadcom's Symantec division, offers a collection of data types, an attribute dictionary, and a taxonomy written in JSON, according to an [overview of the specification](#) available on GitHub. Contributors can utilize and extend the framework and map the various data ingestion and normalization schemas in a common threat detection language.

"As practitioners, one of the most challenging problems in technology is connecting finding and event information across multiple vendor tools, operating systems, and versions," says Jamie Scott, product manager at Endor Labs. "A standard data format will reduce cost and accelerate incident triage for our industry as a whole,"

An Extensible Framework for Interoperability

As an open source project, OCSF seeks to provide an extensible framework for providing interoperable core security schema not tied to a specific provider, Splunk distinguished engineer Paul Agbabian wrote in a white paper documenting OCSF. Licensed under the Apache License 2.0, OCSF features an agnostic storage format, data collection, and extract, transform, and load (ETL) processes. The schema browser represents categories, event classes, dictionaries, data types, profiles, and extensions.

"Vendors and other data producers can adopt and extend the schema for their specific domains," Agbabian explained in a separate blog post. "Data engineers can map existing schemas to help security teams simplify data ingestion and normalization so that data scientists and analysts can work with a common language for threat detection and investigation."

"Having a common data format for these events to be shared across tooling will make both consumers' and producers' lives easier. Producers can more easily integrate with other solutions and consumers can aggregate and triage incidents," Scott says.

The OCSF shares some similar taxonomy with the widely used MITRE ATT&CK Framework, according to the white paper, though it also noted some stark differences. The most notable is that OCSF is extensible by vendors and customers, while MITRE releases all content for ATT&CK.

An Enterprise Strategy Group and Information Systems Security Association (ISSA) survey found that 77% of cybersecurity professionals want to see the industry forge support for open standards. The same survey found that 85% see integration among products as essential.

"Cybersecurity is ready to move on from silos and into an open, integrated era of interoperability and cooperation," Agbabian noted.

Normalizing Security Telemetry

The project is open to other providers wishing to participate and contribute, according to Ryland.

"We see value in contributing our engineering efforts and also projects, tools, training, and guidelines to help standardize security telemetry across the industry," he wrote. "Although we as an industry can't directly control the behavior of threat actors, we can improve our collective defenses by making it easier for security teams to do their jobs more efficiently."

The status of the OCSF and when vendors will begin testing wasn't immediately apparent. And it remains to be seen to what extent the vendors will ultimately contribute to OCSF and implement it.

"The biggest threat to an early-stage effort like OCSF is the steering committee composition itself. Since the committee is made largely of vendors, representative consumer organizations will need a seat at the table to help drive adoption across vendors," Scott says. "As the OCSF continues to collaborate with the industry, it should ensure that the steering committee has reserved spots for industry practitioners who are willing to make an investment in their mission."

Erkang Zheng, founder and CEO of cyber operations platform provider JupiterOne, is pledging to embrace and participate in extending OCSF.

"Over time, we will continue to contribute to the OCSF initiative by extending the framework to cover both time-series event data and stateful/structural asset data, leveraging JupiterOne's open-source data model," Zheng wrote. "Our hope in participating in this initiative is to inspire more cross-industry collaboration."

Scott adds: "Solving a problem like this is a journey that will require learnings across the industry. But the destination makes the journey worth it."

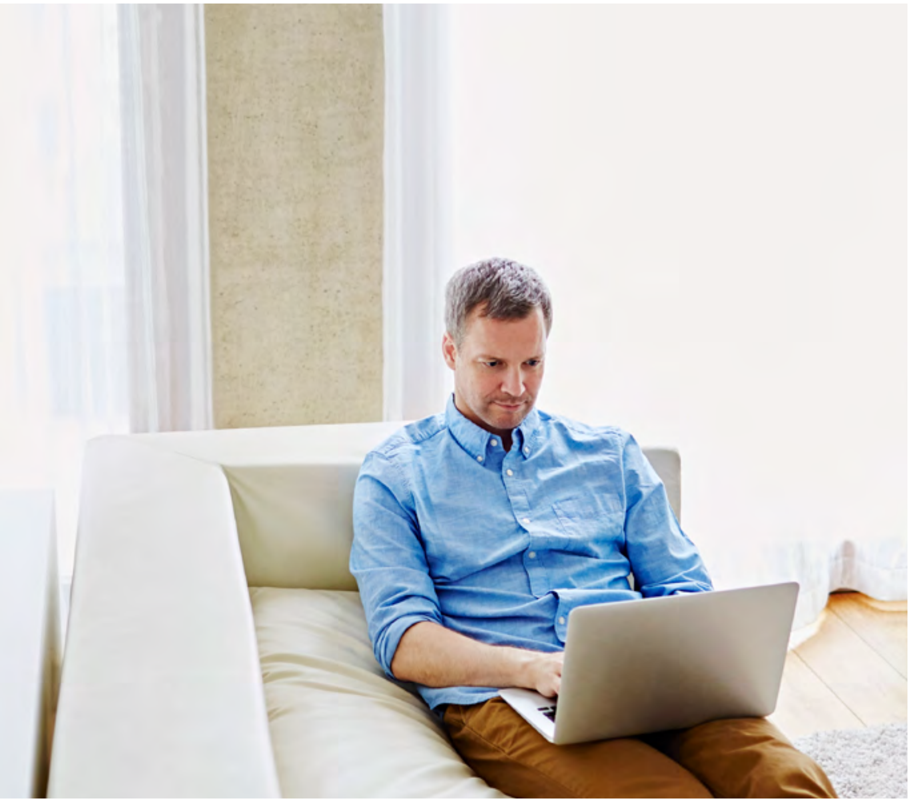
About the Author: *Jeffrey Schwartz is a journalist who has covered information security and all forms of business and enterprise IT including client computing, data center and cloud infrastructure, and application development for more than 30 years. Jeff is a regular contributor to Channel Futures.*

ANALYSIS

Applying Behavioral Psychology to Strengthen Your Incident Response Team

A deep-dive study on the inner workings of incident response teams leads to a framework to apply behavioral psychology principles to CSIRTs.

By Kelly Sheridan, Contributing Writer, Dark Reading



Cybersecurity incident response teams (CSIRTs) rely on technical and social skills. But focusing mostly on technical knowledge can come at the expense of communication and teamwork, according to a study.

This idea was the focus of a five-year study analyzing incident response teams from a social-behavioral perspective. From 2012 to 2017, a team of researchers funded by the US Department of Homeland Security interviewed more than 200 people and led 80 focus groups across 17 international organizations to identify the key drivers of teamwork within and between teams.

The researchers included several people from George Mason University (GMU) who teamed up with Dartmouth and HP, and received funding from the Swedish and Dutch governments, says Dr. Daniel Shore, chief research officer at Leadership & Effective Teamwork Strategies (LETS), who worked on the study while he was at GMU.

"Across our team of researchers and practitioners, we put in over 56,000 hours of analysis and interviewing, to data gathering and analysis, to understand … not only what an individual on the team does but the team they represent, or the multiteam system they represent," Shore says.

Bionic CEO Mark Orlando discovered this research as part of his own work looking into how security teams can better work together. "It really resonated with me," he says. "I thought the research was great; there were a lot of very practical things in there that I was able to use in my work." He began to reference the research and as a result, he was later connected to Shore.

"What was identified early on that spurred that research …was the idea that in cybersecurity, there are lots of analysts and front-line eyes-on-glass people who are very egocentric — not to say they're egotistical, but egocentric," Shore explains. "They see things from their own perspective; they're used to being able to say, 'I can handle this challenge on my own.'"

It makes sense, he continues. Many security pros are trained individually; they learn how to hack, investigate, and test on their own. Then they're dropped into situations in which they face complex problems and challenges that require collaboration, but they don't have the background and habits that come with working collaboratively in a multiteam system.

Orlando says it's natural for relationships to form, and for trust to form, in an incident response team and within a larger organization. In his experience, he often encounters what he calls the "rock star problem."

"You've got one or a few people [who are] very, very capable, very knowledgeable, and the team sort of coalesces around those individuals," he says. "Which is not necessarily a bad thing, but it can create issues when those individuals inevitably move on, or maybe they [have] less than optimal work habits, or behaviors, or things we want to try to account for."

Compounding CSIRTs' collaboration issues is a prominent focus on technical tools and skills, Orlando adds. Incident response teams are "often inundated" with tools to address technical problems in security and incident response; however, there is a "definite lack" of tools to address some of the social and collaboration challenges CSIRTs face in operating within the context of a multigroup, multiteam system as they need to do.

A Framework to Tackle the Problem

In a Black Hat Europe briefing, "Building Better CSIRTs Using Behavioral Psychology," Orlando and Shore discussed these challenges in depth and provided a framework for applying behavioral psychology principles to improve CSIRTs' social maturity, as well as tools to improve the skills defenders need to more effectively work together.

"You can be a little bit more deliberate, and a little bit more focused, about how those relationships form and about how knowledge is shared," says Orlando, noting the importance of how CSIRTs work together with other teams across the business. Having an effective incident response team doesn't necessarily mean you'll be successful as a security organization, he adds.

"You have to work as part of a larger ecosystem; security doesn't just happen in a vacuum," Orlando says.

One of these tools, for example, is called a goal hierarchy. Everybody has their own goals, team goals, and organizational goals, says Shore. Most people have already thought about this concept, but the idea here is to expand on the way businesses think about these goals from an individual's perspective.

"The team goals don't matter to the individual if the individual's not part of the team goals," he explains. "When you structure this goal hierarchy, it's all stemming from the individual perspective. So what is the individual's opportunity to give input to their own goals, to the team's goals, to the organization's goals?"

An individual can be given chances to understand this through all-hand meetings, cross-training, and shadowing other people's work. At the organizational level, consider where there are opportunities for a person to be involved and feel invested in the organization's goals.

"What happens is we end up in crisis after crisis," Shore says, "and if we're reactively trying to involve people in setting goals and validating those goals, it doesn't play into the strength of what could be done proactively."

About the Author: ***Kelly Sheridan is the former senior staff editor at Dark Reading.***

Previous Next

NEWS

What the Newly Signed US Cyber-Incident Law Means for Security

Bipartisan cybersecurity legislation comes amid increased worries over ransomware, and fears of cyberattacks from Russia in the wake of its invasion of Ukraine.

By Steve Zurier, Contributing Writer, Dark Reading

When President Biden signed the omnibus spending bill in March, he also put the bipartisan Cyber Incident Reporting Act into effect, which requires critical infrastructure companies in the 16 industry sectors identified by the federal government to report to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours if they are experiencing a cyberattack and within 24 hours of making a ransomware payment.

While this wasn't the all-encompassing data breach law that has been stalled in Congress for many years, it was notable in that the Senate passed the legislation unanimously. The bill was championed by Sen. Gary Peters (D-Mich.) and Sen. Rob Portman (D-Ohio); it covers a broad swath of the economy, including the defense industrial base sector, which has more than 100,000 companies alone.

Game Changer

"It's a game changer," says Tom Kellermann, head of cybersecurity strategy at VMware. "It's a fundamentally important strategic decision made by the federal government to finally eliminate the plausible deniability that had existed for far too long. ...Corporations have [for some time] underinvested in cybersecurity because they could always maintain plausible deniability."

Kellermann argues that the new law will force companies to hire a CISO, give that person a budget, and provide detection response oversight.

"Companies need to show that they are taking this seriously," Kellermann says. "They will either have to hire a CISO, or if they already have one, promote the CISO and make sure they have veto authority over the CIO. The general counsel will also have to become more familiar with privacy and cyber laws. They will need to work hand-in-hand with the CISO in their information-sharing efforts in public-private partnerships with the ISACs and working with CISA."

The new law gives CISA the authority to subpoena companies that fail to report cybersecurity incidents or ransomware payments. Organizations that fail to comply with the subpoena can be referred to the Department of Justice.

The provision requires CISA to launch a program that will warn organizations of vulnerabilities that ransomware actors exploit, and directs CISA Director Jen Easterly to establish a joint ransomware task force to coordinate federal efforts — in tandem with industry — to prevent and disrupt ransomware attacks. The omnibus law also authorizes $2.59 billion in funding to CISA, which was $300 million above the Biden administration's proposal.

"This is very significant legislation as it addresses the increasing cybersecurity threats amid rising concerns that Russia's invasion of Ukraine could lead to Kremlin-backed hackers attacking critical infrastructure such as hospitals, power plants, and fuel pipelines," notes Chris Cruz, SLED CIO at Tanium.

Centralized Repository

CISA will have a centralized repository of information on threat-actor plans, programs, and operations, he notes. "This will allow information sharing among the critical agencies like the DoJ and FBI and provide a standardized method in which to deal with these attacks, prosecute these perspective cyber hackers, and ensure that each reporting entity has a well-defined cybersecurity strategy that integrates security and operations across their respective networks."

Davis McCarthy, principal security researcher at Valtix, adds that the new incident reporting law stands as a proactive, collaborative approach by the federal government to combat the booming cybercrime industry. McCarthy says data has become a valuable commodity in both traditional and criminal markets.

"They say that 'knowing is half the battle,' and this law will improve our collective understanding of who stole the data, what data they want next, and what they stand to gain by possessing it," McCarthy says. "However, the law uses policy to make a valuable security process available to the public and critical infrastructure organizations. The law does not enforce the output value: No one has to patch a critical vulnerability, harden their cloud infrastructure, or threat hunt for recent ransomware [indicators of compromise]."

VMware's Kellermann would have liked to have seen lawmakers get tougher on the ransomware payments and the cryptocurrency operators who manage the ransom payments, many of whom have ties to North Korea and Russia. He says federal officials will collect data and over time prove the correlation between the ransom payments and the bad threat actors.

"I would like to see a banning of ransomware payments and explicit regulation as it relates to the exchanges," Kellermann says. "But I've been in cybersecurity for 23 years. To have true bipartisanship action in this regard is historic."

About the Author: *Steve Zurier has more than 30 years of journalism and publishing experience and has covered networking, security, and IT as a writer and editor since 1992.*

Previous Next

Preparing for Cyber Defense and Maintaining Security Control

Defense capabilities are often siloed, but a unified approach is key to success.

By Jim Meyer, Technical Director; Dan Nutting, Consulting Manager; Jennifer Guzzetta, Senior Product Marketing Manager — Mandiant

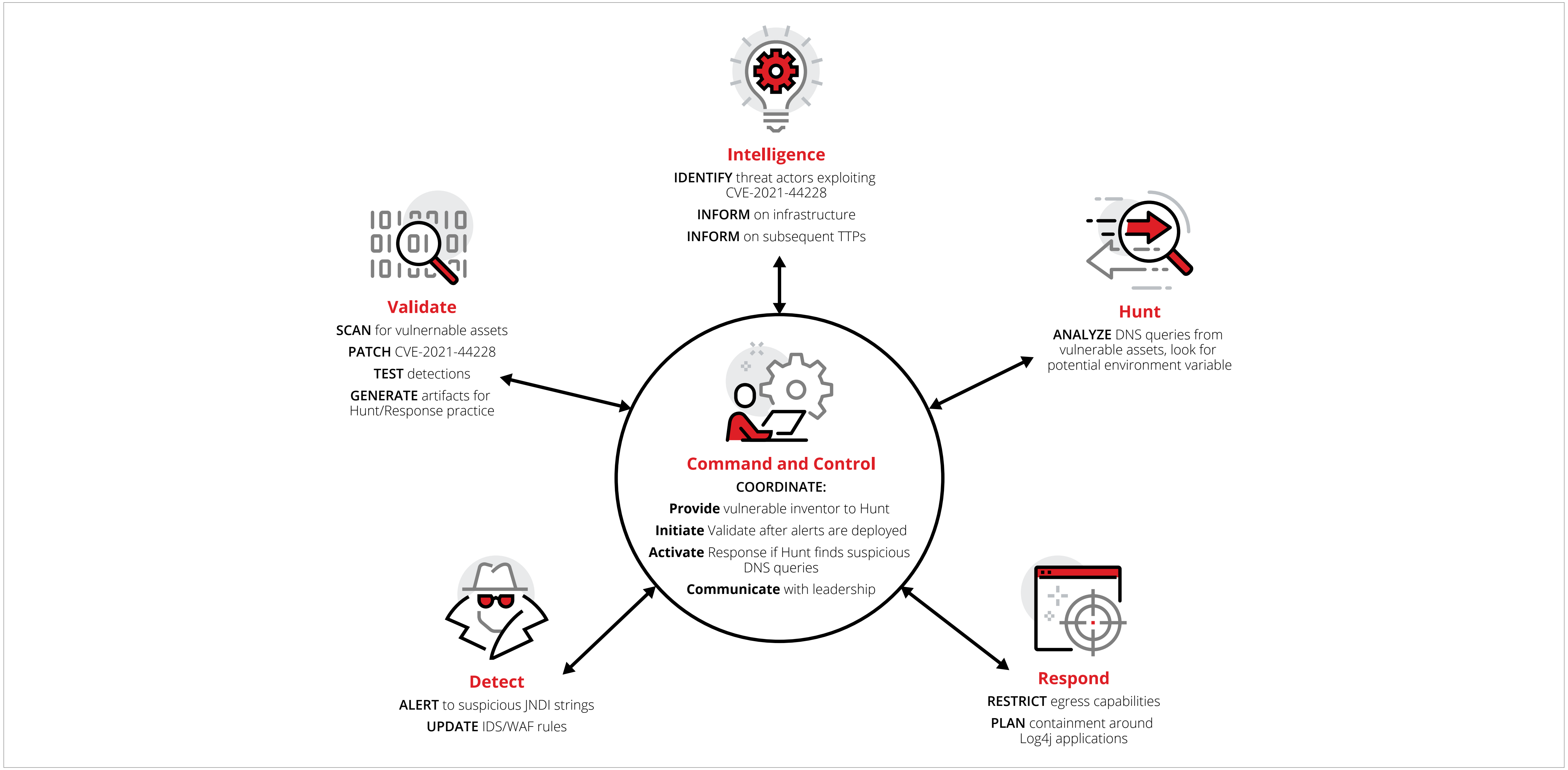
In today's evolving threat landscape, effective cyber defense is a necessity. However, in most organizations, defense capabilities are functionally fractured into silos of expertise and frustratingly disconnected from key objectives and the overall mission. A successful cyber-defense center requires taking a unified approach, spearheaded by a dedicated function.

As stated in *The Defender's Advantage*, cyber defense is one of four closely integrated information security domains, alongside security governance, security architecture, and security risk management. Cyber defense is comprised of six critical functions that enable organizations to operate in the face of threats. A complete cyber-defense center includes threat intelligence, hunt, detect, respond, validate, and command and control.

The command and control function is the nucleus to the unified approach to ensure that each area of expertise can support one another with clear visibility into the knowledge, experience, tools, and processes provided by each specialty. Key duties of this critical function include review of tactical inputs such as escalated incidents, detection of adversary behaviors, and identification of missed indicators of compromise from its neighboring five functions — to then organize, measure, and share orderly information across the holistic cyber-defense center.

For example, when a new threat has been identified (intelligence), the details are used to build new alerts (detect), escalated incidents are triaged and investigated (respond), the presence of adversaries hiding in the network is found (hunt), and new attack patterns are simulated (validate). Although the threat was identified by the intelligence function, it does not serve as the nucleus of all activity. Instead, the command and control function is the hub for tracking the success of each action and brokering the exchange of information that drives resolution.

Sample Log4j Use Case of the Six Critical Functions of Cyber Defense Working Together



Intelligence

IDENTIFY threat actors exploiting CVE-2021-44228

INFORM on infrastructure

INFORM on subsequent TTPs

Validate

SCAN for vulnernable assets

PATCH CVE-2021-44228

TEST detections

GENERATE artifacts for Hunt/Response practice

Hunt

ANALYZE DNS queries from vulnerable assets, look for potential environment variable

Command and Control

COORDINATE:

Provide vulnerable inventor to Hunt

Initiate Validate after alerts are deployed

Activate Response if Hunt finds suspicious DNS queries

Communicate with leadership

Detect

ALERT to suspicious JNDI strings

UPDATE IDS/WAF rules

Respond

RESTRICT egress capabilities

PLAN containment around Log4j applications

The command and control function acts as the central hub of awareness, facilitating and tracking communications between groups handling intelligence, detection, response, hunting, and validation. Command and control defines and sustains the governance, collaboration, and communications for specificized expertise that are potentially insourced or outsourced given the organization's composition. Specialized functions often focus almost entirely on their area of expertise, requiring command and control to provide interconnection and collaboration.

Let's explore a ransomware-related sample use case in which an administrator account was abused by a threat actor who updated a group policy object (GPO) to create a scheduled task on all servers for execution, beginning on Friday and concluding on Sunday. The adversary selected this specific tactic to easily distribute malware across the entire victim environment. On the first day of deployment, the security operations center (SOC) received and escalated endpoint alerts that identified the scheduled task pointing to an unsigned PowerShell script. Based on this incident, the command and control function would assume responsibility to ensure all cyber-defense center functional resources are orchestrated properly and collaborating effectively by enforcing a RACI model to align functional capabilities and responsibilities:

- Share details with the intelligence function, requesting analysis to determine the potential type of threat and motivation behind it.
- Disclose threat context with the detect function to deploy new alerts to scope the attacker's presence and alarm attempted reentry.
- Assign incident prioritization to the hunt function to gather scheduled task configurations and begin analysis of similar server activities.
- Direct the validate function to test the scheduled task in a sandbox.
- Uncover all findings with the respond function to request initiation of rapid remediation.

After an incident is resolved, command and control publishes metrics that showcase the effectiveness of the cyber-defense center's operational workflow. Since many aspects of the process are cyclical, they are measured at smaller units of the cycles. For example, the time-to-incident-creation holds many steps, including the time from log event generation to SIEM alert, SOAR enrichment, and analyst triage and escalation. The measurement of each smaller unit demonstrates where time was lost. Inept transitions from specialized, functional silos wastes significant time, combated by command and control's management.

Outside of incidents, command and control monitors and measures cyber-defense operations. This enforcement of interoperation prevents the functional silos from forming. Without this core function, Mandiant has witnessed immature security teams exacerbate the delay, and at times cause the demise of their security readiness. For example, Mandiant has observed teams forbid the socialization of incident reports, hide penetration test results from the rest of the cyber-defense center, and obscurely publish findings that never become championed and in turn sit dormant without action.

The continuous command and control efforts of assessing, tracking, and measuring cyber incidents and guiding actionable improvements helps mature the holistic expertise of the cyber-defense center's productivity. Ultimately, command and control ensures the necessary governance, processes, and communications are adapted by all critical functions and structured accordingly to guide effective operations for combating sophisticated cyber adversaries.

About the Company: *Since 2004, Mandiant provides unparalleled threat intelligence and incident response to help organizations tackle their top security challenges. Learn how we can assess and improve your cyber defense. Get a copy of the award-winning book The Defender's Advantage. Mandiant is now part of Google Cloud.*

Previous