Putting Together an Effective Incident Response Plan

What You Will Learn

In this white paper, IT and security team members will learn about the necessary components of an effective incident response plan:
Understanding why current incident response plans are failing
Putting together the right incident response team
Developing successful response procedures
Selecting appropriate security technologies
Dramatically improving incident response and forensics with NetFlow and security analytics

Attacks Are on the Rise

From large-scale retailers to healthcare providers and government agencies, no one remains safe from today’s sophisticated, targeted cyber attacks. Whether the attackers are after financial data, trade secrets, or classified information, the ever-evolving threat landscape and rapidly growing network environments are providing more ways for them to break in.

It is no longer a matter of if, but when, attackers will break into your network. They’ll use zero-day attacks, stolen access credentials, infected mobile devices, a vulnerable business partner, or other tactics.

Security success is not just about keeping threats out of your network. Instead it’s about quickly responding to and thwarting an attack when it happens.

According to Gartner, “Organizations are failing at early breach detection, with more than 92 percent of breaches undetected by the breached organization.”¹ It is clear that we need to play a far more active role in protecting our organizations. We need to constantly monitor what is going on within our infrastructure and have an established, cyclical means of responding before attacks wreak havoc on our networks and reputations.

Incident Response Shortcomings

In a survey conducted by the Ponemon Institute, most respondents agreed that the best thing their organization could do to mitigate future breaches was to improve their incident response capabilities. Yet at that time, half of the respondents indicated that spending on incident response was less than 10 percent of their overall information security budget (Figure 1).² According to another survey, 90 percent of large businesses said they experienced major IT incidents throughout the year, yet only about half have an incident response team in place to handle such incidents.³
Incident response encompasses the people, processes, and technology used to detect and respond to security incidents. Each of these pieces of the puzzle—people, processes, and technology—is equally important in establishing and carrying out an effective response plan.

The People

Who should be involved in an organization's incident response plan? Everyone.
The CSIRT

First and foremost, enterprise organizations need to have a fully functional Computer Security Incident Response Team (CSIRT) consisting of trained, dedicated security professionals. Every organization, no matter how small, should have at least one designated person who is responsible for computer security incident response. Unfortunately, being an expert in security does not necessarily mean that you are an expert in incident response. Incident responders must possess specific background in, or be trained to handle, high-pressure response scenarios. It is also important to have committed incident responders who are not also responsible for myriad other IT and security functions.

The incident response team should have an in-depth understanding of the network and its assets. In many cases today, attackers conduct thorough reconnaissance and know more about their target network than the victim's own IT or security team. The right technologies can help incident responders discover assets on their network, determine which ones are most critical to protect, and baseline normal behaviors to more quickly identify anomalies that could signify an attack.

Beyond IT

But there's more to incident response than having the right technical team in place. Beyond the IT team, key stakeholders in the legal, executive management, HR, public relations, and other departments should play an integral role in an organization's incident response plan. Organizations need to figure out what these groups need to do in the event of an incident. They need to establish roles and responsibilities before an incident occurs, and bring these individuals into the fold early on. It is also important to keep upper management informed about incident response procedures, successes, and challenges to make sure that these efforts receive the appropriate amount of attention and funding needed to be effective.

Lastly, in an ideal world, each and every employee—and even third party—that an organization works with should help support the incident response team. Train employees so that they know what to look for in the event of a social engineering attempt. Carefully screen, conduct background checks, and inquire about the security of any third party that has access to your network or even just confidential information about your company. And do not forget about the insider threat. Train managers to look out for and report suspicious employee behaviors to HR, and train HR to communicate these concerns to IT.

“Stealthwatch enables security and incident response teams to remediate incidents faster than before, reducing downtime and the overall costs of managing networks and network services.”

— Telenor Norway
The Processes

Incident response cannot be an afterthought. Enterprise organizations need a firmly established, well thought out response plan that incorporates key individuals and groups from across the business.

In order to be truly effective, incident response plans should include:

1. **VERY CLEAR ROLES, RESPONSIBILITIES, AND APPROVAL PROCESSES** for all players, and defined rules for when specific actions can and cannot be taken. For example, is the incident response team permitted to take machines offline without additional approval in order to contain an attack? What about wiping computers or blocking access to specific services? Are these actions permitted when necessary? Additionally, what are the company's legal, regulatory, and contractual obligations when a breach occurs? It is critical to have these types of questions answered in writing before an incident happens. Ideally, your incident response plan should strike a comfortable balance between having policies in place to ensure that the right decisions are made in a crisis, yet not having so many layers of approval that you hinder the efficacy of skilled responders.

2. **REGULAR TRAINING AND ASSESSMENT EXERCISES**. There may be a substantial amount of time between incidents at your company. During that time, it is critical to continue training all relevant staff and to conduct exercises to assess their readiness in the event of an incident. Additionally, when incidents do occur, do not forget to use them as an opportunity to measure the efficacy of your team. Using metrics such as the mean time to identify (MTTI), mean time to know the root cause (MTTK), and mean time to fix (MTTF) a security issue can greatly assist in your efforts to improve your response processes, as well as demonstrate return on investment to upper management.

3. **A REGULAR MEANS OF COMMUNICATING INCIDENT RESPONSE PLANNING EFFORTS AND SUCCESSES WITH UPPER MANAGEMENT** to ensure that the appropriate amount of attention and investment is dedicated to the process, and that its critical role in business continuity is understood.

4. **A FIRM UNDERSTANDING OF THE ORGANIZATION’S INFRASTRUCTURE AND WHERE THE “CROWN JEWELS” LIE**. Visibility into typical activity inside the network, and reliable threat intelligence from the outside world, are both critical components for incident response.

5. **A FEEDBACK LOOP TO ENSURE THAT INCIDENTS ARE NOT JUST SIMPLY CLEANED UP** but also investigated. Key details about the attackers and their methods must be forensically extracted to prevent similar attacks. Military strategist John Boyd developed the OODA Loop as a framework for decision making in combat operations (Figure 2). Today it is applied to many other disciplines, and can serve as a great example of the continuous process needed for effective incident response.
The Technology

Equally important as having the right people and processes in place is having the right technology deployed before an incident occurs.

Threat intelligence from the outside is important for keeping up with known attacks, but without tools that help incident response teams gain critical insight into their own network activity, response efforts will be futile. After all, you can’t protect what you can’t see.

Incidence response is not just about cleaning up malware and getting infected computers back online. Further investigation needs to be done to determine the full extent of the attack, whether additional machines were affected, and the types of tactics used by the attackers. This way you can make sure that you have completely rooted the attack out of your environment and that the same exact attack will not happen again.

“Stealthwatch reduces problem-solving from days to seconds. With Stealthwatch, we can stay ahead of potential attacks and breaches.”
- Edge Web Hosting

Network Audit Trails

The best way to see what is going on within today’s large, complex networks is to collect and analyze network audit trails. In fact, 80 percent of respondents in a Ponemon survey indicated that the analysis of audit trails from sources like NetFlow and packet captures was the most effective approach for detecting security incidents and breaches.\(^5\)
Using network activity logs, organizations can more easily be aware of and shut down attack attempts. NetFlow in particular is a highly effective technology because it can be collected throughout the network without installing dedicated probes. And the data can be stored for long periods of time at an affordable cost.

5 Ponemon Institute, “Cyber Security Incident Response - Are we as prepared as we think?” January 2014

**The Power of NetFlow**

First created by Cisco and now inherent in a wide range of network infrastructure devices, NetFlow (along with other types of network telemetry) provides valuable metadata from existing routers, switches, and firewalls to increase visibility and situational awareness. It provides a record of each connection that occurs over a network, including the ‘to’ and ‘from’ addresses, the port numbers, the amount of data transferred, and other information.

NetFlow can reveal countless valuable details about your network assets and behaviors: who is talking to whom, which applications are being used, and so forth.

Most organizations already have access to NetFlow within their environment. They simply have to begin collecting and analyzing it to achieve new levels of insight into their network. But not all NetFlow monitoring technologies are created equal.

With the constant network evolution we are experiencing today, networks are churning out massive quantities of Big Data. Having access to that data is a good first step, but unfortunately it means nothing if incident response teams cannot make sense of it and use it for improved awareness and better decision making. That is where advanced, flow-based monitoring solutions like Cisco® Stealthwatch come in.

**Cisco Stealthwatch**

Cisco Stealthwatch serves as the eyes and ears of the network. It rapidly collects and analyzes massive amounts of NetFlow data to deliver in-depth visibility and actionable intelligence to security and response teams. It provides the deep network understanding and network activity baselining discussed earlier, which are critical for establishing strong incident response procedures.

Additionally, when combined with other Cisco security technologies, Stealthwatch helps organizations cost-effectively use their existing infrastructure to turn their network into an always-on security sensor for more seamless threat detection. Through sophisticated behavioral analytics, Stealthwatch can automatically detect suspicious behaviors that could lead to a wide range of attacks, from zero-day malware and distributed denial-of-service (DDoS) attacks to advanced persistent threats (APTs) and insider threats.

Stealthwatch dramatically reduces the manual analysis associated with incident investigation. It often reduces troubleshooting down from days or even months to just minutes. Intuitive dashboards and reports help security and incident response professionals rapidly get to the information they need with just a few clicks, whether it’s an overall picture of network activity, a list of potential issues, or a view into a specific host (Figure 3). This information can also be easily shared with other stakeholders such as upper management.
Figure 3. Stealthwatch Dashboard

Cisco Stealthwatch provides advanced network visibility and security intelligence for accelerated incident response.

Perhaps an insider is repeatedly trying to access restricted areas of your network. Or maybe unusually large amounts of data are being sent out of your network, or an internal host is communicating with a suspicious IP address in a foreign country. An effective network visibility and security analytics tool can pick up on these behaviors and alert administrators to investigate further.

“80% of respondents indicated that analysis of audit trails from sources like NetFlow and packet captures was the most effective approach for detecting security incidents and breaches.”

- Ponemon Institute

The Stealthwatch Difference

Unlike many other technologies that only monitor traffic going in and out of the network, Stealthwatch also monitors lateral (east-west) traffic to detect attacks spreading inside the network and identify insider threats. By constantly monitoring the network for anomalous behavior—and using
advanced security analytics, alarming, and reporting to alert administrators to potential issues—Stealthwatch enables faster, more efficient incident response.

Processing NetFlow is generally less resource-intensive than alternatives such as full packet capture. But pervasive logging on a global enterprise may still generate record volumes exceeding one million flows per second. An effective solution must be able to scale appropriately to cut down on storage and power consumption. Stealthwatch’s massive scalability and ability to de-duplicate and stitch unidirectional flow records together results in cost-effective flow monitoring and storage for even the largest, most complex enterprise networks.

In addition to improving real-time threat detection, Stealthwatch also helps you conduct faster, more thorough forensic investigations. It can store flow data for months or even years and use its advanced querying capabilities to quickly extract pertinent information about previous attacks. This historical look-back is critical for fine-tuning incident response procedures to improve threat defenses. The ability to efficiently collect, analyze, and interpret huge volumes of network and security data will become even more important as networks continue to grow and evolve through cloud, software-defined networking (SDN), and Internet of Things (IoT) architectures.

“Before Stealthwatch, we manually analyzed and correlated our network activity data. Stealthwatch automatically gives us detailed network insight through a single, easy-to-use interface, aiding our security, network operations, and compliance efforts.”

- BlueCross BlueShield of Tennessee

**Enhanced Security Context and Integrations**

Research reveals that 69 percent of organizations say their security tools do not provide enough context for them to understand their risk.⁶

Through both its own technologies and industry collaborations, including tight integration with other Cisco technologies, Stealthwatch brings in additional layers of security context to further accelerate and improve incident response and forensics.

Examples of these value-added layers of intelligence include:

- User and device awareness
- Cloud visibility
- Application awareness
Threat feed data
- Endpoint security integration
- Proxy visibility
- Packet capture

Having access to all this information from a single console dramatically streamlines threat investigation and remediation. In fact, according to the Enterprise Strategy Group, 80 percent of organizations believe that their incident detection and response processes are hindered by a lack of security technology integration. Unfortunately, disjointed solutions slow down threat mitigation and leave security gaps that attackers can more easily exploit. Enhanced layers of context and deep integrations enable a more automated, fluid, and effective response to the full spectrum of threats facing today’s organizations.

6 Ponemon Institute, “Privileged User Abuse & The Insider Threat,” May 2014

Conclusion

Unfortunately, no technology today can completely keep hackers out of enterprise networks. However, if an organization is regularly monitoring its own environment with the right mix of people, processes, and technology, the security team will be better equipped to pinpoint and stop an attack while it’s still happening, avoiding the disastrous results and costs associated with a data breach.

For More Information

Combined with Cisco’s broad security portfolio, Stealthwatch can provide comprehensive protection and streamlined incident response from edge to access: across the network, data center, endpoints, mobile devices, and the cloud.

Click here to read how Cisco’s own CSIRT uses Stealthwatch to detect and analyze malicious traffic for improved incident response and forensics.

Learn more. Request a demo.

stealthwatch@cisco.com

“80% of organizations believe that their incident detection/response processes are hindered by a lack of security technology integration.”

- Enterprise Strategy Group