cybereason

The Incident Response Success Checklist

Nine Critical Steps Your Current Plan Lacks

Details matter when developing an incident response (IR) plan. But, even the most successful IR plans can lack critical information, impeding how quickly normal business operations are restored.

This quick guide takes a closer look at nine of the often forgotten, but important steps that you should incorporate into your IR plan.

- ✓ PREPARATION ACROSS THE ENTIRE COMPANY
- ✓ IDENTIFY MEASUREMENTS AND MATRICES
- ✓ HOLD TEST RUNS
- ✓ CHECK THE ALERTS THAT APPEAR BENIGN
- ✓ CREATE A CONSOLIDATED DATA REPOSITORY
- ✓ DON'T OVERLOOK INDUSTRIAL CONTROLS
- ✓ CONTAINMENT AND REMEDIATION
- ✓ PLAN FOR A FOLLOW-UP BUDGET AND RESOURCES
- ✓ FOLLOW-UP ACROSS THE ORGANIZATION

1. PREPARATION ACROSS THE ENTIRE COMPANY

Involving key people from every department is often an overlooked part of the preparation process. Often times, only IT and security staff participate in building a company's IR plan, since they are the individuals who deal with the situation and its consequences. However, breaches impact the entire organization, not just the departments that handle computers and servers. Good security leaders should be able to get people from across the company to help develop the IR plan. While CISOs will most likely manage the team that handles the threat, dealing with the fallout from a breach requires the efforts of the entire company.

For instance, a bank handling the impact of a breach may need help from its public relations staff if the organization is legally required to publicly disclose the incident. The bank's Web development team may also need to be involved if the adversaries carried out their attack by exploiting a vulnerability in the company's website, like a WordPress flaw. Additionally, the company's human resources department may need to be contacted if employees' personal information was disclosed. The bank's incident response plan should include input from all of these departments.

A thorough incident response plan lays out what key personnel should be notified when a breach is detected and how information on the breach is communicated throughout the organization and externally. During the preparation phase, a communication timeline and the contact information for key staff should be added to the plan.

2. IDENTIFY MEASUREMENTS AND MATRICES

A successful incident response plan defines in advance the key performance indicators (KPIs) that the security team will measure during the event. Some good time-related measurements to track include time to detection, time to report an incident, time to triage, time to investigate, and time to response. On the qualitative side, some figures to track include the number of false positives, the nature of the attack (malware vs. non-malware based) and the tool that spotted the incident.

3. HOLD TEST RUNS

Companies should use the preparation phase to consider the various breach scenarios that could play out. These scenarios should be reviewed in activities like team training, tabletop exercises and blue team-red team exercises. Businesses should even simulate a breach so employees know their roles when a real breach occurs.

This is the phase when companies identify their weak points and risk factors, figure out what activities need to be closely monitored and decide how to spend their security budgets. An IR plan should be revised yearly or more frequently if the company grows rapidly. Additionally, the incident response plan should incorporate any business regulations.

4. CHECK THE ALERTS THAT APPEAR BENIGN

Threat detection can come from situations that initially appear benign and not related to security. An IT investigation into a slow computer could reveal that the machine is infected with malware, for example, prompting fears of phishing attacks and an investigation to see if anyone clicked on a suspect link. IT professionals should always check for signs of compromise when looking into a tech issue, even if the incident doesn't seem to be connected to security.

A company' best defense against adversaries is well-trained users who, for instance, know to contact security after receiving an email with an odd link. Additionally, IT and security teams shouldn't disregard a user's suspicions. Always investigate a hunch, since a person's intuition can provide a lead that results in a breach being detected.

5. CREATE A CONSOLIDATED DATA REPOSITORY

Whatever methods companies use to detect threats, an important step is consolidating all incidents into a central repository. Companies typically use SIEMs for this but sometimes these aren't enough to get a comprehensive view across an IT environment.

Incident response teams will often try to build a view of everything that was going on in the environment in hindsight. At this point, it is often too late to construct a comprehensive view and what the incident response team ends up with is too partial to be of any value. Building and maintaining a data repository that has continuous and a broad visibility across the full environment is not just essential for regulatory requirements. It is crucial for accelerating investigation and response.

6. DON'T OVERLOOK INDUSTRIAL CONTROLS

Many organizations have facilities that run industrial systems, such as an oil refinery or a factory that manufactures drugs. However, companies may not think attackers will target these locations and not closely monitor them for malicious activity.

In other cases, a department other than IT or security manages the industrial control system infrastructure. The personnel in this department may lack the knowledge needed to closely monitor these systems, potentially leading to security being neglected.

7. CONTAINMENT AND REMEDIATION

A thorough containment and remediation process that stops an entire campaign instead of only solving a symptom of the attack is essential. However, security teams usually provide a specific solution to a very broad problem, leaving ample opportunity for the same attack to re-occur.

The containment and remediation plan must be based on the findings of the security team's investigation of the incident. Often times, the plan that's developed relies on information only gathered during the preliminary detection. For example, if a SIEM detected a malicious connection to C2 server, the typical solution would be to kill the process creating the communication and block the IP address in the firewall. But if the malware is persistent, it will reload when the computer reboots, perhaps with a different process name, and communicate with a different server. The security team then enters an endless loop of detection, containment and eradication for the same threat. On the other hand, if the team was investigating the malware's techniques and infection vector, it would have a better eradication plan and may have developed a prevention plan.

8. PLAN FOR A FOLLOW-UP BUDGET AND RESOURCES

Follow-up is critical to preventing a security incident from reoccurring. However, companies often don't fully follow through with this step. Some recommendations that come out of the follow-up process entail spending money, making such steps unpalatable to organizations with budget constraints. Less costly options include adding new detection rules to a SIEM, while some of the more expensive follow-up steps entail hiring additional security analysts or purchasing technology to detect attacks.

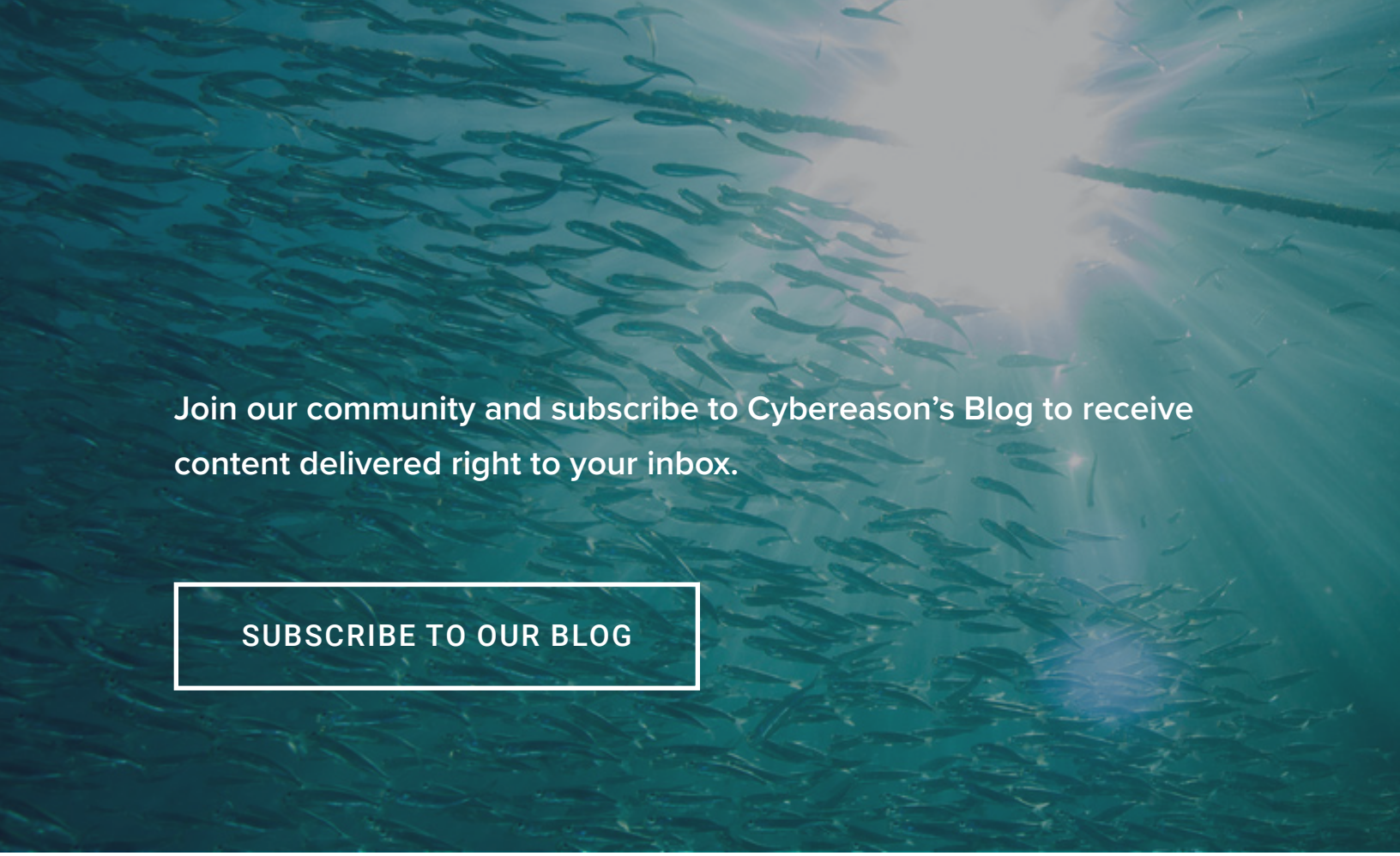
The follow-up phase is also when an organization reviews the performance of its KPIs and determines if they need to be adjusted. A security team, for example, could determine that the detection rules caused excessive false positives, impeding its ability to swiftly respond to the incident. Then, it can go and improve the set of detection rules it has, or upgrade to a different detection systems with better capabilities. The security team could also decide to add a detection rule based on an incident that was reported by a user instead of being detected by the SIEM.

Whether an enterprise goes on an analyst hiring spree or considers a more frugal option, the changes a company makes during the follow-up stage will affect how it prepares for attacks and detects threats. All of these steps are tied together, a point often missed by organizations. Having more analysts and purchasing a next-generation endpoint detection technology can bolster a company's ability to unearth threats, for instance.

9. FOLLOW-UP ACROSS THE ORGANIZATION

Organizations should get ready to spend time and money to learn and improve after a breach.

It is also crucial that the learning and improvement process not only includes IT and security. Similar to the preparation phase, often times, follow-up only focuses on what the security team handles, which is typically containment and detection. Limiting follow-up to the security team's duties makes managing the process easier, but fails to take into account how other departments in a company should get involved to improve their ability to can better react to a security incidents in the future. Incident response requires the cooperation of an entire organization, not just the IT and security departments.



Join our community and subscribe to Cybereason's Blog to receive content delivered right to your inbox.

SUBSCRIBE TO OUR BLOG

cybereason

Cybereason was founded in 2012 by a team of ex-military cyber security experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams.

Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel and Tokyo, Japan.