WHITE PAPER

Preparing Your Organization for Incident Response: Best Practices and Lessons Learned

GUIDEPOINT
SECURITY

Attacks happen, and when they do, your incident response plan needs to be ready for action. With the full scope of the incident defined, you can start developing an eradication and remediation strategy to effectively address the threat, such as:

Multiple access points and entrenchment mechanics an attacker has created

More than one threat actor who may have gained access into your environment

It's been repeated, it's not if you'll be a victim of an attack, but when?

However, it is how you handle the incident once it's been identified, or you've been notified, that will mean the difference between regaining your security or continuing to be a victim.

No matter how you find out about an incident, there are industry-standard response processes involving steps for identification, containment, eradication, and recovery, but specific considerations and methodologies should be followed when dealing with targeted threat activity. The methodology is designed to address a threat's remediation effectively, by covering all bases and understanding the full scope of an incident within your organization, whether on-prem, in the cloud, or both.

When it comes to incident response, you should follow a best-practices methodology that requires obtaining the Full Incident Scope - only after you have a complete historical and current environmental awareness of threats.

Looking at real-life scenarios and coming away with lessons learned is an excellent opportunity to integrate information that will improve your IR strategy and tactics, to ensure efficacy of your plan. With this information, you can better prepare for future attacks and have a functional plan addressing requirements during and after future incidents.

While using IR best practices from a preparedness perspective is essential, you also want to implement a robust, proactive threat hunting process. Rather than waiting for an alert to be triggered, threat hunting and mass triage allow you to actively hunt for anomalies and suspicious behaviors that indicate advanced threats, which may have evaded detection using traditional reactive alert-based monitoring.

Opportunistic and Targeted Incidents and Attacks

There are different types of incidents and attacks which warrant various response activities. Breaking it down to its most basic form, we can identify two specific models: opportunistic and targeted:

- **Targeted** – These types of incidents and actions are pointed where the goal is to gain information, money, or to reach the masses with messaging serving a specific purpose. In a targeted incident, the threat actors are commonly categorized as:
  - **Nation-State -** With a particular plan or motive for pursuing a specific victim, typically for the theft of information or intellectual property.
  - **Cybercriminals -** Are looking for explicit information, data, or other items of value in possession by a specific victim, most commonly motivated by monetary gains.
  - **Hacktivists -** May want to target an identified victim as a means of political activism, mass messaging, or civil disobedience.
- **Opportunistic** – Incidents of opportunity are random where there is no specific motivation other than an attacker seeing an opportunity to exploit. In this type of attack, the attacker could be anyone, and the potential victims are everyone.

  For example, an actor who sends out hundreds or even thousands of similar phishing emails to random businesses hoping that someone will open the email and click on a link, allowing entry into the entity's infrastructure. In this case, the actor is not selective in terms of their victim, and their motives are often financial. They may try to steal information or data which they believe they can sell.

These targeted incidents may involve R & D, government or corporate intelligence, infrastructure information, records, ICS, POS, or any other valuable and in-demand data.

Incident Alerts Come in Many Forms

For most, the first question is, “How do you know that you have an incident, or if there something is going on in your environment that you are unaware of?” These questions are particularly relevant when dealing with targeted attacks.

When an incident occurs, there are a multitude of ways an organization may find out about it.

1. **Law Enforcement Notifications** – Sometimes, law enforcement officials from entities such as the DHS or FBI may notify you that your organization has potentially been affected by a particular threat that requires investigation.

2. **Internal Identification** – Other times, the notification may come from within your organization. It may be through internal identification of the threat, or because your team picks up anomalous activities, network degradation, or other types of actions that have alerted teams to the fact something is going on, requiring further investigation.

3. **Proactive threat hunting** – is another means of finding out about an incident, rather than depending on an alert system that may not identify a particular attempted intrusion or attack, through a more sophisticated and advanced proactive threat hunting process. Organizations can identify and investigate suspicious activity that could indicate targeted threats that are going unidentified.

   Vendor Services – Vendor services, such as compromise assessments, penetration testing, and threat discovery engagements, can play a role in this process by identifying threats, vulnerabilities, or insecure control sets that have enabled adversaries to gain access into an environment.

4. **3rd Party Notification** – When we respond to a customer incident, we will often run across data and information associated with other organizations. Attackers will leverage infrastructure and drop sites that might disclose intel about other victims. We also encounter files uploaded to 3rd party analysis sites, which inadvertently reveal that a company has been compromised. In these instances, service providers will commonly reach out to organizations to ensure they’re aware they might be dealing with targeted threat activity.

Distribution of Notifications

Regarding notifications for targeted threat activity, there are various methods by which information can get distributed, which include – by hand, email, or via phone. In most instances, those issuing the warning will opt for hand delivery or an initial phone call in order not to tip off the attacker, who may be monitoring corporate emails - mainly if it involves a more advanced threat. Regardless of how you’re contacted, it’s what is done with the information that will make the difference.

Defining Your Response Methodology

When it comes to an investigation associated with a targeted attack, a full incident scope is required.

Advanced threat actors targeting your environment will ensure they have multiple persistence mechanisms to retain access to that environment.

They're deploying web shells, leveraging malware, putting in various other types of backdoors – all to ensure they can continue to access the environment regardless of what remediation efforts are initiated, purposeful or not.

You may have found four persistence mechanisms in a targeted attack scenario, but what if the attacker deployed five? They'll use that remaining persistence mechanism to get back into the environment.

Key Considerations When Thinking About Attackers

- **Subsidiary/Partner organizations used for access -** These are commonly used to access customer environments. We also see this action occurring during mergers and acquisitions. Before being merged into their infrastructure, an attacker might target a specific company to ensure that they can get into the parent infrastructure. This also happens after an adversary has been kicked out of a particular customer environment. If they're unsuccessful with re-entry, they might try a partner or subsidiary to get back into the primary environment.

- **Post-remediation monitoring is critical -** Once all of the remediation and eradication tasks have been successfully executed, you want to continue to watch the environment and look for indications of attacker activity.
  It is very likely the attacker will attempt to come back. This is especially true with targeted attacks as long as you continue to have something that they want.

Because they are familiar with your environment, they can quickly re-entrench themselves and use different techniques to move laterally and evade detection. Having the full incident scope before considering remediation efforts is required to minimize the risk of continued compromise due to lack of understanding of every persistence mechanism.

To ensure you have covered the full incident scope, you must have enterprise-wide visibility, and look at the environment from multiple perspectives.

For example, you can't focus strictly on endpoints, network traffic, or logs - you need a combination of all those data sources and various tools to help you paint that big picture as to what exactly has occurred. Once you know how the adversary accessed the environment, you need to determine what activities they performed, what data they tried to steal or access, and if they attempted to exfiltrate that data.

Remediation and Eradication

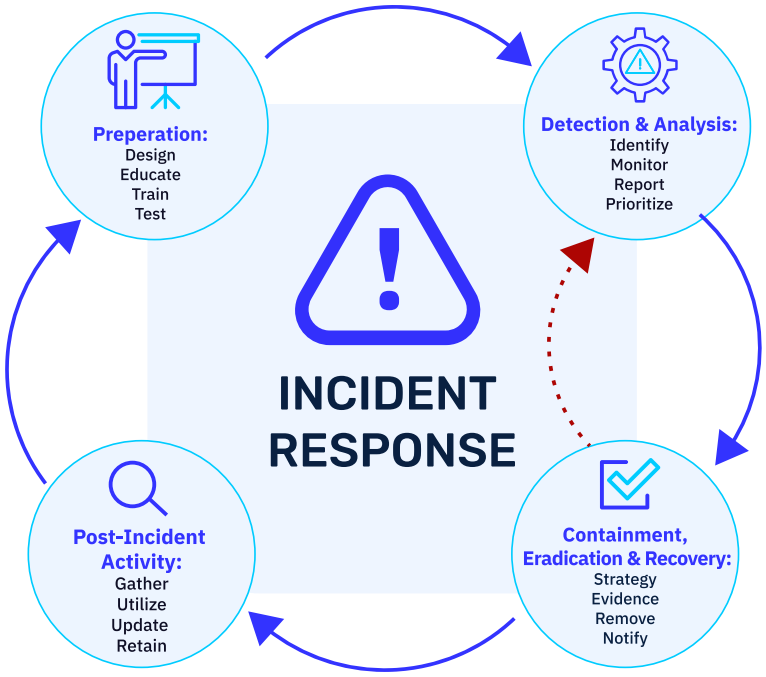
Once you have the full incident scope defined, you can start thinking about a remediation strategy. In the interim, it's a game of cat and mouse in a targeted attack where you don't want to tip your hand to the adversary while the investigation is ongoing.

When you're ready to remove an attacker from the environment, you must have a very specific and documented plan, including preliminary objectives, sequential steps to be completed as part of an eradication event, and post-eradication requirements.

Activities might include:

- Ensuring the setup and availability of additional systems to replace old systems, so you're ready to implement new technologies on the eradication date
- Execution of enterprise-wide password resets
- Providing help desk and desktop support resources so that when you go into that eradication event, you have a sequential list of activities to perform and appropriate staff on hand to perform them

Once those are completed, you must go through post-eradication requirements to ensure that you're actively identifying threat actor activity to quickly and effectively address their attempted re-entry. This post-remediation success monitoring is critical. When you're dealing with a targeted threat, they don't simply walk away if you cut off their access. That threat actor has potentially been in your environment for an extended period, targeted your environment for a reason, and they will make more attempts to regain access.



Incident Response Examples

To help make all of the provided content more tangible, we'll jump into some specific incident examples that demonstrate the reasoning for this methodology.

EXAMPLE ONE

Proactive Engagement

In this example, we reached out, and proactively notified an organization that there was a potential issue in their environment that should be reviewed. The organization responded with “Thank you very much,” and nothing else until a couple of months later. They came back saying they identified strange activity in their environment and wanted our help.

The organization had us come in to do a proactive service engagement to determine if there was presence of any threats. Once we confirmed the targeted threat and its intent, we quickly transitioned into an incident response effort.

What We Discovered

The adversary had been in their environment for more than 2.5 years and had been embedded in the environment for so long; they knew timing of code releases and when to access the staged QA server to exfiltrate data.

We were able to look back historically and find that the initial attack vector was a Spear-phishing campaign that included multiple exploitation methods against targeted users.

This phishing campaign attempted to:

- Exploit a user’s browser if it had a vulnerability
- Harvest credentials by having the user enter their credentials into a fake site
- Steal session cookies from the browser

Time to Remediate

Once we uncovered the full scope of the incident, we developed a remediation strategy for the customer. The customer said they needed two weeks before we could get to that eradication event, so we continued to monitor the environment during that time. During the period when the customer was preparing for remediation, we saw the adversary package and attempt to exfiltrate a significant amount of data (multiple GB) from an Executive’s mailbox.

The customer wasn’t ready for remediation because they hadn’t completed all of the prerequisite tasks, which would have lead to premature and unsuccessful remediation. At the same time, we couldn’t let this executive’s email with valuable information walk out the door. We decided to kill the session where the adversary was performing the upload and modified the RAR files to corrupt the data. The adversary believed the session timed out and needed to be restarted, which bought the customer additional time. While this was going on, the customer expedited their pre-eradication requirements, allowing us to perform the eradication in a shortened timeline.

We’re Not Done Yet

Post eradication, we had set up listeners where the threat actor’s web shells were located, and we could see them attempting to connect to the environment and troubleshoot their access. When their webshells weren’t working, they immediately attempted to use VPN access, which was now configured with two-factor authentication. We assume they then checked their malware, which had been disabled, and then saw them attempt to actively troubleshoot their webshell access.

We eventually knew our remediation efforts were successful when we received communications from the threat actor in the customer’s VPN logs, and saw them attempting to spear-phish users again.

Key Lessons:

Threat actor activity had gone unnoticed within this environment for multiple years. Remediation efforts were only successful because we identified and addressed all of the threat actor’s entry points. Additionally, attempted remediation without completing all of the prerequisite steps would have led to continued compromise and additional investigation requirements.

EXAMPLE TWO

Known Threat Actors

Company A

In response to a notification associated with a specific threat actor, a customer made substantial investments in incident response efforts to ensure there was related activity in their environment. While there was no activity associated with that specific adversary, we found artifacts of a previous campaign associated with a different adversary from multiple years prior. Luckily, in this instance, those were inactive, and though the notification was incorrect, there was more going on in their environment than expected.

Company B

We saw an instance where a threat actor was present in the environment, but because we looked more widely across the environment to achieve full environmental awareness - not just specifically for the known threat – we also found a backdoor open on a still-active system. It was not associated with the known threat actor, and ultimately was identified that the customer's red team had installed a backdoor on a system and forgot to remove it.

Company C

We were brought in to examine a notification associated with a nation-state actor and their particular tactics and techniques. By looking more widely across the environment, we discovered a secondary actor leveraging different TTPs and a two-year difference between the two actors. Both actors were present in the customer's environment, working independently of each other.

Key Lessons:
In all of these examples, it's crucial to integrate the known information and Intel into your investigation, but not to focus solely on just known adversary activities. Leveraging the requirement for full incident scope through complete environmental awareness ensures you will not miss related and potentially unrelated activities within the environment.

EXAMPLE THREE

An "Unhackable" Solution

Company D

In this scenario, the customer told us they had an "unhackable solution." We got brought in to assist with investigation of anomalous activity associated with on-demand VPN authentication. They were seeing successful inbound authentication, but not seeing evidence where the tokens were being issued to the associated users before that step.

In the investigation, we identified a subsidiary relationship where one of their subsidiaries had become compromised, and they leveraged that access to get into this customer's environment. The adversary found a backup of the authentication server, exfiltrated that backup, stood up that backup somewhere else, and then issued their own authentication tokens to successfully authenticate to the customer environment. The only indication was that there was no outbound issuing of the codes for those authentication attempts.

Key Lessons:
Partners provide actors with another way to access your environment. Make sure you cover those access points as part of your investigation process. Proactive Threat Hunting is critical for identifying advanced threats based on the identification of anomalies and suspicious activities. For more information on dealing with partners and vendors, check out our white paper: "Key Components to Addressing Third-Party Risk."

EXAMPLE FOUR

Malware Remediation

Company E

A service provider evaluated a technology that picked up malware on some of their endpoints, and they asked us to assist by analyzing the malware. We confirmed that the malware was targeted at their environment and made recommendations for an incident response effort. The customer attempted to do the investigation and remediation on their own, but ultimately reengaged us many months later to confirm their attempted efforts were successful.

We identified continued access from the threat actor because they had not identified all attacker activity. We developed a comprehensive remediation strategy based on full incident scope, which allowed them to remove that adversary effectively. The duration of this incident was over the course of a year and a half due to multiple premature and unsuccessful remediation attempts by the customer.

Key Lessons:
Ensuring you have full incident scope to develop a complete remediation strategy is essential. Otherwise, you have a false sense of security and can lead to a threat actor's extended presence in your environment, siphoning out valuable data.

Conclusion

In the examples we reviewed, customers had the technology, and in some instances, everything was up to date from a patching perspective. It's not just about your technology, but also about proactive threat hunting where you are looking throughout the environment for the unknown – and feeding that intel back into your IR process. Look at some of these key considerations from the examples reviewed and other organizations that have gone through an Incident.

Key Considerations:

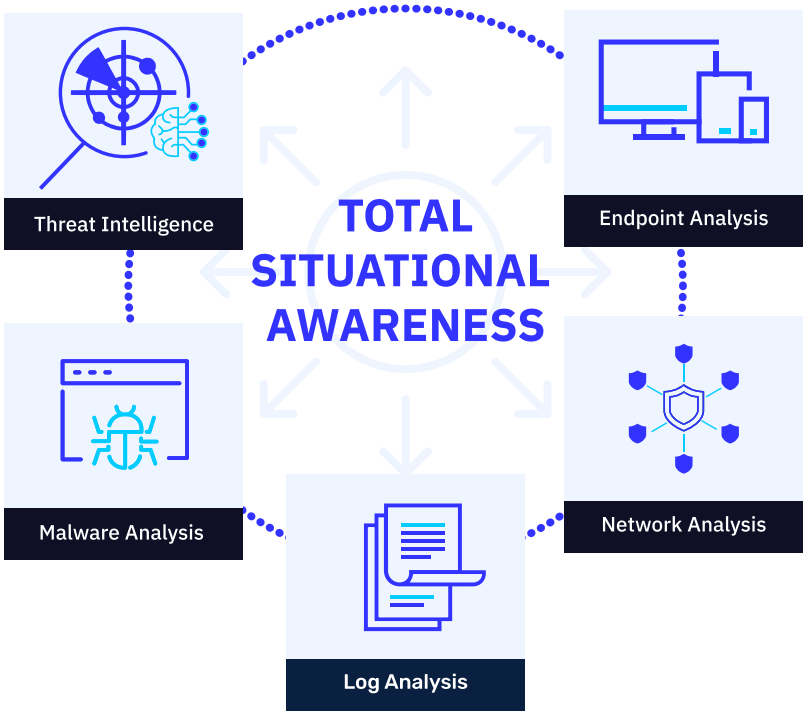
- Some customers had plenty of technology (EDR, NDR, NGAV, etc.)
- Others had 24x7x365 MSS but were not alerted
- Some Malware was detected by 0 of 51 AV Vendors - even when provided directly to AV Vendors for signature creation
- Premature or incomplete remediation efforts were unsuccessful - Full Incident Scope is Required, and Patience is vital
- Subsidiary/Partner organizations were used for access
- Once access is established, attackers live off the land, using admin tools instead of malware to evade detection
- Simple attack vectors, similar to a commodity or opportunistic threats
- Multiple attackers can be working independently
- Post remediation monitoring is critical to see if the attacker comes back
- Visibility is Critical, Look Widely in the environment, turning over every stone
- Implement purpose-defined remediation plans for a Quick and Effective Execution

(Key Considerations Cont.)

- Don’t be Afraid to Ask for Help - work with experienced teams
- Practice Makes Perfect - Test your plan thoroughly and make adjustments as needed

You may not have been able to stop your organization from falling victim to a targeted or opportunistic attack, or in some cases serving as a target to both. Still, there are steps you can take now to minimize the adverse effects of such an incident.

Before undertaking any remediation or eradication tasks, you should investigate to define a Full Incident Scope. Make sure you have enterprise-wide visibility and that there is a combined effort to find every compromised area and all access points. If you proceed to remediation without first purging your environment of such threats, you may be allowing the same actor to gain access again and again. Many targeted attacks are more advanced, and if they have already accessed your environment through one means, chances are they have multiple persistence mechanisms into the same environment.



ABOUT THE AUTHOR

Mark Lance

Lance is the Senior Director, Cyber Defense Practice for GuidePoint Security - Lance brings over 19 years of Information Security experience, spending the last eight years specifically in Incident Response. He has also worked in areas including proactive Threat Discovery services, Traffic Analysis, and Security Analysis.

GUIDEPOINT
SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132

WP-DFIR-052020-02