SOPHOS

FOUR KEY TIPS FROM INCIDENT RESPONSE EXPERTS

Responding to a critical cyber incident can be an incredibly stressful and intense time. While nothing can fully alleviate the pressure of dealing with an attack, understanding these key tips from incident response experts will help give your team advantages when defending your organization.

This document highlights the biggest lessons everyone should learn when it comes to responding to cybersecurity incidents. They are based on the real-world experience of the Sophos Managed Threat Response and Sophos Rapid Response teams, who have collectively responded to thousands of cybersecurity incidents.

Tip #1: React as quickly as possible

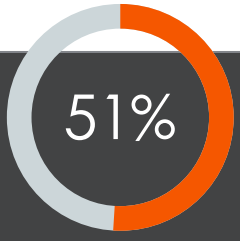
When an organization is under attack, every second matters.

There are a few reasons why teams may take too long to react. The most common is that they don't understand the severity of the situation they find themselves in, and that lack of awareness leads to a lack of urgency.

Attacks tend to hit at the most inopportune times: holidays, weekends, and in the middle of the night. Since most incident response teams are significantly understaffed, this can understandably lead to a "we'll get to that tomorrow" attitude. But unfortunately, tomorrow may be too late to do something to minimize the impact of the attack.

Overwhelmed teams are also more likely to react slowly to indicators of attack because they suffer from alert fatigue, which means signals get lost in the noise. Even when a case is initially opened, it may not be correctly prioritized due to a lack of visibility and context. This costs time, and time is not on a defender's side when it comes to incident response.

Even in situations where the security team is aware that they are under attack and something needs to be done immediately, they may not have the experience to know what to do next, which also makes them slow to respond. The best way to combat this is by planning for incidents in advance.



More than half of organizations were hit by ransomware last year – and attackers succeeded in encrypting files in 73% of cases.[1]

Tip #2: Don't declare "mission accomplished" too soon

When it comes to incident response it's not enough to only to treat the symptoms. It's important to treat the disease as well.

When a threat is detected, the first thing to do is triage the immediate attack. This could mean cleaning up a ransomware executable or a banking Trojan or blocking the exfiltration of data. However, often teams will stop the initial attack but not realize they haven't really solved the root cause.

Successfully removing malware and clearing an alert doesn't mean the attacker has been ejected from the environment. It's also possible that what was detected was only a test run by the attacker to see what defenses they're up against. If the attacker still has access, they'll likely strike again, but more destructively.

Incident response teams need to ensure they address the root cause of the original incident they mitigated. Does the attacker still have a foothold in the environment? Are they planning to launch a second wave? Incident response operators who have remediated thousands of attacks know when and where to investigate deeper. They look for anything else attackers are doing, have done, or might be planning to do in the network – and neutralize that, too.

For example, in one instance, Sophos incident response specialists were able to thwart an attack that lasted nine days and saw three separate attempts by the attackers to hit an organization with ransomware.

Since they were not yet a Sophos MTR customer, the Sophos Rapid Response team was first engaged.

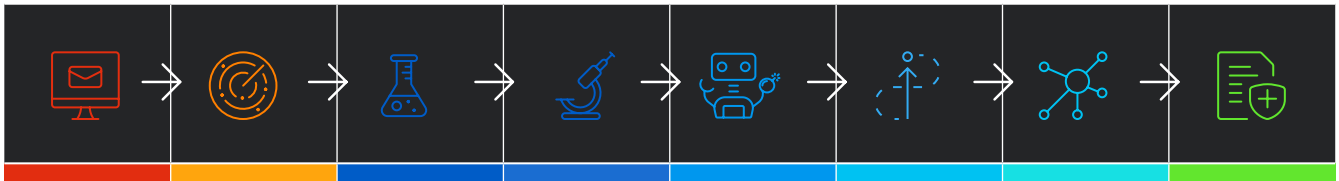
In the first wave of the attack (which was ultimately blocked by the organization's endpoint protection solution) attackers targeted 700 computers with Maze ransomware and were making a ransom demand of US$15 million. Realizing that they were under attack, the target's security team engaged the advanced incident response skills of the Sophos Managed Threat Response (MTR) team.

The Sophos incident response specialists quickly identified the compromised admin account, identified and removed several malicious files, and blocked attacker commands and C2 (command and control) communications. The Sophos MTR team was then able to defend against two additional waves of attacks by the adversary. If the attackers had succeeded and the victim had paid, this could have been one of the most expensive ransomware payments to date.

In another example, the Sophos MTR team responded to a potential ransomware threat but quickly realized there was no evidence of ransomware. At this point, some teams might have closed the case and moved on to other work. However, the Sophos MTR team continued investigating and uncovered a historic banking trojan. Fortunately for this customer, the threat was no longer active, but it serves as an example of why it's important to look beyond the initial symptoms in order to determine the full root cause, as it could be an indicator of a broader attack.

SOPHOS MTR CASEBOOK:

The ransomware hunt that unearthed a historic banking trojan



START	15 MINUTES	38 MINUTES	1 HOUR 11 MINUTES	1 HOUR 32 MINUTES	1 HOUR 45 MINUTES	1 HOUR 52 MINUTES	2 HOUR 6 MINUTES
Customer emails in to say their vendor has been hit by ransomware. Sophos MTR team immediately starts investigating to determine if the customer is a related target.	The MTR team finds no evidence of ransomware, but does see a behavioral detection for a highly obfuscated .js script that Sophos had previously blocked on execution.	The MTR team sends file samples to SophosLabs for analysis and to request Indicators of Compromise (IOCs) to continue the hunt.	SophosLabs provides further information and IOCs for the MTR team. A new detection is created for the .js script to protect all customers.	Using the IOCs, the MTR team locates a process that previously called out to a C2. The team has high confidence this threat is a Qbot variant.	SophosLabs provides further IOCs of file paths and details of a scheduled task the script interacted with. The MTR team continues to investigate.	The MTR team uses the IOCs to locate historic executions, and the threat's update and persistence mechanism.	Case closed. The MTR team has removed all remaining artifacts from the host and provided the customer with full details.

Undiscovered Discovered Triage/Analysis Containment/Neutralization

Tip #3: Complete visibility is crucial

While navigating an attack, nothing makes defending an organization more difficult than flying blind. It's important to have access to the right high-quality data, which makes it possible to accurately identify potential indicators of attack and determine root cause.

Effective teams collect the right data to see the signals, can separate the signals from the noise, and know which signals are the most important to prioritize.

Collecting signals

Limited visibility into an environment is a sure-fire way to miss attacks. Over the years, many big-data tools have been brought to market to try and solve this specific challenge. Some rely on event-centric data like log events, others utilize threat-centric data, and others rely on a hybrid approach. Either way, the goal is the same: collect enough data to generate meaningful insights for investigating and responding to attacks that would otherwise have been missed.

Collecting the right high-quality data from a wide variety of sources ensures complete visibility into an attacker's tools, tactics, and procedures (TTPs). Otherwise, it's likely only a portion of the attack will be seen.

Reducing noise

Fearing they won't have the data they need to get the full picture of an attack, some organizations (and the security tools they rely upon) collect everything. However, they're not making it easier to find a needle in a haystack; they're making it harder by piling on more hay than is necessary. This not only adds to the cost of data collection and storage, but it also creates a lot of noise, which leads to alert fatigue and time wasted chasing false positives.

Applying context

There's a saying among threat detection and response professionals: "Content is king, but context is queen." Both are necessary to run an effective incident response program. Applying meaningful metadata associated to signals allows analysts to determine if such signals are malicious or benign.

One of the most critical components of effective threat detection and response is prioritizing the signals that matter the most. The best way to pinpoint the alerts that matter the most is with a combination of context provided by security tools (i.e. endpoint detection and response solutions), artificial intelligence, threat intelligence, and the knowledge base of the human operator.

Context helps pinpoint where a signal originated, the current stage of the attack, related events, and the potential impact to the business.

Tip #4: It's OK to ask for help

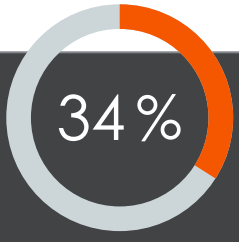
No organization wants to deal with breach attempts. However, there's no substitute for experience when comes to responding to incidents. This means that the IT and security teams often tasked with high-pressure incident response are thrown into situations that they simply don't have the skills to deal with; situations that often have a massive impact on the business.

The lack of skilled resources to investigate and respond to incidents is one of the biggest problems facing the cybersecurity industry today. This problem is so widespread that according to ESG Research[2], "34% say their biggest challenge is that they lack skilled resources to investigate a cybersecurity incident involving an endpoint to determine root cause and the attack chain."

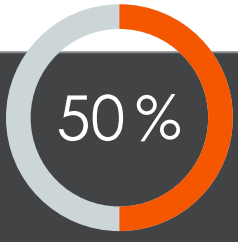
This dilemma has given way to a new alternative: managed security services. Specifically, managed detection and response (MDR) services. MDR services are outsourced security operations delivered by a team of specialists, and act as an extension of a customer's security team. These services combine human-led investigations, threat hunting, real-time monitoring, and incident response with a technology stack to gather and analyze intelligence. According to Gartner, "by 2025 50% of organizations will be using MDR services"[3], signaling a trend that organizations are realizing they will need help to run a complete security operations and incident response program.

For organizations that have not employed an MDR service and are responding to an active attack, incident response specialist services are an excellent option. Incident responders are brought in when the security team is overwhelmed and needs outside experts to triage the attack and ensure the adversary has been neutralized.

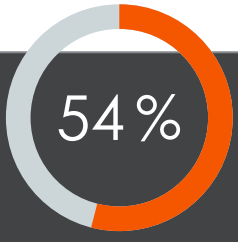
Even organizations that have a team of skilled security analysts can benefit from collaborating with an incident response service to shore up gaps in coverage (i.e. nights, weekends, holidays) and specialized roles that are needed when responding to incidents.



According to analyst firm ESG, 34% of organizations say their biggest challenge is that they lack skilled resources to investigate a cybersecurity incident involving an endpoint to determine root cause and the attack chain."[2]



By 2025, 50% of organizations will be using MDR services (this is up from less than 5% in 2019).[3]



In a 2019 survey of 3,100 IT and security professionals, 54% of respondents claimed they were "unable to take full advantage of their EDR solution" due to a lack of experienced talent.[4]

How Sophos can help

Sophos Managed Threat Response (MTR) service

Concerned about your organization's ability to respond to a potentially serious incident? If so, the Sophos Managed Threat Response (MTR) service is an option worth considering.

Sophos MTR provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service. Going beyond simply notifying you of attacks or suspicious behaviors, the Sophos MTR team takes targeted actions on your behalf to neutralize even the most sophisticated and complex threats. If an incident does occur, the MTR team will initiate actions to remotely disrupt, contain, and neutralize the threat. The team of security operations experts also provide actionable advice for addressing the root causes of recurring incidents.

Learn more at www.sophos.com/mtr

Sophos Rapid Response service

If your organization is under attack and needs immediate incident response assistance, Sophos can help.

Delivered by an expert team of incident responders, Sophos Rapid Response provides lightning-fast assistance with identification and neutralization of active threats against organizations. On-boarding starts within hours, and most customers are triaged within 48 hours. The service is available for both existing Sophos customers as well as non-Sophos customers.

The Sophos Rapid Response team of remote incident responders quickly takes action to triage, contain, and neutralize active threats. Adversaries are ejected from your estate to prevent further damage to your assets.

Learn more at www.sophos.com/rapidresponse

Sophos Intercept X Advanced with EDR

Organizations looking to increase their ability to detect, investigate, and response to incidents in-house should consider adding Sophos endpoint detection and response (EDR) capabilities.

Sophos Intercept X Advanced with EDR enables your team to conduct threat hunting and helps keep IT operations hygiene running smoothly across your entire estate. Sophos EDR empowers your team to ask detailed questions to identify advanced threats, active adversaries, and potential IT vulnerabilities – and then quickly take appropriate action to stop them.

Learn more and try it for free at www.sophos.com/edr

[1] 2020 survey of 5,000 IT managers https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-cybersecurity-the-human-challenge-wp.pdf

[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

[3] Gartner, Market Guide for Managed Detection and Response Services, 26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

[4] 2019 survey of 3,100 IT managers https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20-11-09 WPEN (PS)

SOPHOS