Leveraging Threat Intelligence In Incident Response/Management

Version 1.5
Released: August 21, 2014

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report is licensed by Bit9 + Carbon Black, Cisco, and Intel Security whose support allows us to release it for free.

All content was developed independently.

www.bit9.com

cisco.com/go/security

intelsecurity.com

Copyright

About our Licensees

Bit9 + Carbon Black offers the most complete solution against the advanced threats that target your organization's endpoints and servers. This makes it easier for you to see—and immediately stop—those threats.

Carbon Black's lightweight endpoint sensor, which can be rapidly deployed with no configuration to enable detection and response in seconds, combined with Bit9's industry-leading prevention technology, delivers four key benefits:

- *Continuous, real-time visibility into what's happening on every computer*
- *Real-time threat detection, without relying on signatures*
- *Instant response by seeing the full "kill chain" of any attack*
- *Prevention that is proactive and customizable*

Thousands of organizations worldwide—from 25 Fortune 100 companies to small businesses—use Bit9 + Carbon Black to increase security, reduce operational costs and improve compliance. Leading managed security service providers (MSSP) and incident response (IR) companies have made Bit9 + Carbon Black a core component of their detection and response services. With Bit9 + Carbon Black, you can arm your endpoints against advanced threats. For more information, visit www.bit9.com.

www.bit9.com

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco provides one of the industry¹s most comprehensive advanced threat protection portfolios, as well as a broad set of enforcement and remediation options that are integrated, pervasive, continuous, and open. This threat-centric security model lets defenders address the full attack continuum across all attack vectors before, during, and after an attack. For ongoing news, go to http://www.cisco.com/go/security

cisco.com/go/security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

intelsecurity.com

Leveraging Threat Intelligence in Incident Response/Management

Table of Contents

The Challenge of Incident Response

It's hard to be a defender today. Adversaries continue to innovate, attacking software which is not under your control. Attacks move downstream as low-cost attack kits put weaponized exploits in the hands of less sophisticated adversaries, making them far more effective. But attackers often don't need innovative attacks, because a little reconnaissance and a reasonably crafted phishing message can target and successfully compromise employees and provide a foothold in your organization. The good news is that we find very few security practitioners still clinging to the hope that all attacks can be stopped by deploying the latest shiny object from a VC-funded startup.

Where does that leave us? Pretty much where we have been for years. It is still about responding faster — the sooner you know about an attack the sooner you can start managing it. In our Incident Response Fundamentals series[1] and subsequent React Faster and Better paper[2], we mapped out a process for responding to incidents completely and efficiently, utilizing tactics honed over decades in emergency response.

> Where does that leave us? Pretty much where we have been for years. It is still about reacting faster — the sooner you know about an attack the sooner you can start managing it.

But the world hasn't stayed still over the past 3 years — not by a long shot. So let's highlight a few things shifting the foundation under our (proverbial) feet.

- **Better adversaries and more advanced tactics:** Attackers continue to refine their tactics, progressing ever faster from attack to exfiltration. As we described in our Continuous Security Monitoring paper[3], attackers can be in and out with your data in minutes. That means that if monitoring and assessment are not really continuous, you leave a window of exposure. This puts a premium on responding faster.

- **Out of control data:** If you haven't read our paper on The Future of Security[4], go do that now. We'll wait. It explains how the combination of cloud computing and mobility fundamentally disrupts the way technology services are provisioned and delivered. They will impact security broadly and permanently, most obviously because you lose most control over your data when it can reside anywhere.

So how can you manage incidents when you aren't sure where the data is, and you may not have seen the attacks before? That could be the puzzle for the next *Mission Impossible* movie — Tom Cruise loves cybersecurity. Fortunately the techniques available to security professionals have evolved as well, thanks to the magic of Moore's Law. Networks are faster, but we can now capture network packets when necessary. Computers and devices are more powerful, but now we can collect detailed telemetry from them to thoroughly understand activity. Most importantly, with an increasing focus on forensics in the security industry, most folks don't need to argue so hard that security data collection and analysis are critical to effectively responding and managing incidents.

More Data

As mentioned above, our technology to monitor infrastructure and analyze what's going on has evolved quickly, offering sufficient granularity to enable faster and more effective identification of the root causes of attacks. Several new data sources provide this boost, including:

- **Full network packet capture:** New technologies have emerged to capture multi-gigabit network traffic and index it in near real-time for analysis. This provides much better data for understanding what attackers might have done. Rather than trying to interpret log events and configuration changes, you can replay the attack to see exactly what happened and what was lost. This provides the kind of evidence essential for tracing the root cause of an attack, as well as for formal investigation.

- **Endpoint activity monitoring:** We introduced this in our Endpoint Security Buyer's Guide[5] and fleshed it out in Advanced Endpoint and Server Protection[6]. This approach enables you to collect detailed telemetry from endpoint devices to see every action performed, including what software was executed and which changes were made to the device and its files. This detailed history enables you to search for attack patterns (indicators of compromise) at any time. Even if you don't know activity is malicious when it takes place, you can identify it later so long as you keep the data — a concept we've been calling retrospective analysis.

- **A ton of data:** The good news is that, between network packets and endpoint telemetry, you have much more data to analyze. The bad news is that now you need technology that can actually analyze it within a reasonable timeframe. So we hear a lot about "big data" for security monitoring these days. Regardless of what it's called by the industry hype machine you need technologies to index, search through, and find patterns within the data — even when you don't know exactly what you're looking for to start. Fortunately other industries — including retail — have been analyzing data to detect unseen and unknown patterns for years (they call it "business intelligence"), and many of their analytical techniques are available for security.

As a defender it is tough to keep up with attackers, but these new technologies help fill the gaps. Technology is no longer the biggest issue for detecting, responding, and managing threats and attacks. The biggest problem is now the lack of skilled security professionals to do the work.

In Search of… Responders

It seems like these days every conversation with CISOs and other senior security professionals turns inevitably to finding staff to handle attacks. Positions stay open for extended periods. Organizations need to be creative to find promising staffers, and to invest in training them, even though they often soon move on to higher-paid consulting jobs or other firms. If you are in this position you aren't unique. Even the incident response specialist shops are resource constrained. There just aren't enough people to meet the demand.

It seems like these days every conversation with CISOs and other senior security professionals turns inevitably to finding staff to handle attacks.

The industry needs to address this on multiple fronts:

- **Education:** Continued investment is required to train people in core skills. More importantly, these folks need opportunities and resources to learn on the job — which is really the only way to keep up with modern attackers anyway.
- **Automation:** The tools need to continue evolving, to make response more efficient and accessible to less sophisticated staff. We are not talking about dumbing down the process, but about making it easier and more intuitive so less skilled folks can do the job, and more skilled folks can be much more efficient.
- **Prioritization:** Even skilled responders need to start somewhere when they think there has been an incident. Where do they start? Far too often it's a gut feeling. Experienced folks just know where to look. Unfortunately that's not a scalable process. The entire incident management function happens much faster and better when responders have a better idea of where to look, and of what to look for. That's where external data, also known as threat intelligence, comes in.

What's Missing: a Crystal Ball

This paper won't address basic education for responders. Instead, by updating research from our React Faster and Better paper, we can account for how tools are evolving and impact the effectiveness/efficiency of the response/management process. Ultimately incident management is about being efficient and productive, so we will focus on helping responders prioritize their work and investigate more efficiently.

Let's set the stage for the rest of this paper by digging out one of the great sports quotes:

> *A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be. — Wayne Gretzky*

This applies to incident response/management because responders need to see into the future. To know where the attack is going to be, not merely to react to what is already visible — which, by the way, is what traditional security technologies do. Obviously you cannot *actually* see into the future, but you can at least benefit from the misfortune of others.

This is how we described the concept in our recent Leveraging Threat Intelligence in Security Monitoring[7] paper:

> *By understanding attack patterns and other nuggets of information gleaned from attacks on other organizations, you can be better prepared when they come for you.*
>
> *Though to be clear, you cannot actually get ahead of threats without a time machine, regardless of what vendors tell you. The threat already exists, but wouldn't it be great to know about it before it is used against you?*

Let's apply those concepts to the process of responding to and managing security incidents.

Really Responding Faster

Adversaries are getting better and using more advanced tactics. The difficulty is compounded by corporate data escaping our control into the cloud, and the proliferation of mobile devices. When we started talking about reacting faster[8] in early 2007, few folks were talking about the futility of trying to block every attack. That is less an issue now that the industry understands security is imperfect, and continues to shift resources to detection and response. But the problem grows more acute as the interval between attack and exfiltration continues to decrease.

> The ultimate goal of any incident management process is to contain the damage of attacks. This requires you to investigate and find the root causes of attacks faster.

The ultimate goal of any incident management process is to contain the damage of attacks. This requires you to investigate and find the root causes of attacks faster. That's easy to say, but how? Where do you look? The possible attack paths are infinite.

To really respond faster you need to streamline investigations and make the most of your resources. That starts with an understanding of what information would interest attackers. From there you can identify potential adversaries and gather threat intelligence to anticipate their targets and tactics. With that information you can protect yourself, monitor for indicators of compromise, and streamline your response when an attack is (inevitably) successful.

Adversary Analysis

We suggest starting with adversary analysis because the attacks you will see vary greatly based on the attacker's mission, and their assessment of the easiest and most effective way to compromise your environment.

- **Evaluate the mission:** To start you need to learn what's important in your environment, so you can identify interesting targets. They usually break down into a few discrete categories including intellectual property, protected customer data, and business operations information.

- **Profile the adversary:** To defend yourself you need to not only know what adversaries are likely to look for, but what kinds of tactics the various types of attackers typically use. So figure out which categories of attacker you are likely to face. Types include unsophisticated (using widely available tools), organized crime, competitors, and state-sponsored. Each class has a different range of capabilities.

- **Identify likely attack scenarios:** Based on the adversary's mission and general tactics, put your attacker hat on and figure out the path you would most likely take to achieve it. At this point the attack has already taken place (or is still in progress) and you are trying to assess and contain the damage. Hopefully investigating your proposed paths will prove or disprove your hypothesis.

Keep in mind that you don't need to be exactly right about the scenario. You need to make assumptions about what the attacker has done, and you will not predict their actions perfectly. The objective is to get a head start on response, narrowing down the investigation by focusing on specific devices and attacks.

Gathering Threat Intelligence

Armed with context on likely adversaries we can move on to intelligence gathering. This entails learning everything we can about possible and likely adversaries, profiling probable behaviors, and determining which kinds of defenses and controls make sense to address higher-probability attacks. Be realistic about what you can gather yourself and what intelligence you may need to buy. Optimally you can devote some resources to gathering and processing intelligence on an ongoing basis based on your organization's needs, but you will likely need to supplement your resources with external data sources.

Threat Intelligence Indicators

We offer a high-level overview of the kinds of threat intelligence you can leverage to streamline incident response/management.

Malware

Malware analysis is maturing rapidly: it is now possible to quickly and thoroughly understand exactly what a malicious code sample does, and define both technical and behavioral indicators to seek within your environment — as described in gory detail in Malware Analysis Quant[9]. More sophisticated malware analysis is required because classical AV blacklisting is no longer sufficient in the face of polymorphic malware and other attacker tactics for defeating file signatures. Instead you identify indicators of what malware did to a device. Malware identification has shifted from what a file *looks like* to what it *does*.

As part of your response/management process you will need to identify the specific pieces of malware you have found on compromised devices. You can do that via a web-based malware analysis service. You upload a hash of a malware file; if the service recognizes the hash you get its analysis within minutes, and if not you can upload the file for analysis. These services run malware samples through proprietary sandbox environments and other analytics to figure out what each sample does, build a detailed profile, and return a comprehensive report including specific behaviors and indicators to scan for.

Malware also provides additional clues. Can you tie it to a specific adversary? Or at least a category of adversaries? Do you see these kinds of activities during reconnaissance, exploitation, or exfiltration? Any of those would be useful clues to how far the attack has progressed.

Reputation

Since its emergence as a primary data source in the battle against spam, reputation seems to have become a component of every security control. This is hardly surprising — entities which behave badly are likely to continue doing so. The most common reputation data is based on IP addresses, available as a dynamic list of known bad and/or suspicious addresses. As with malware analysis, identifying an adversary helps you look for associated tactics.

Aside from IP addresses, pretty much everything in your environment can and should have a reputation. Devices, URLs, domains, and files, for starters. If you see traffic going to a site known to be controlled by an adversary, look for other devices communicating with that adversary. Containing damage requires identifying and understanding all compromised devices, and reputation can help pinpoint them.

C&C Traffic Patterns

One specialized type of reputation which is now often offered as a separate feed is intelligence on Command and Control (C&C), or botnet networks. These feeds track global C&C traffic and use it to pinpoint malware originators, botnet controllers, and other IP addresses and sites your devices should avoid. They also help identify likely compromised devices within your network by their communication with malware controllers. Integrating this kind of network-based threat intelligence into your investigation provides key information about adversaries, as well as identifying devices which are clearly compromised for quarantine and further investigation.

Phishing Messages

Most advanced attacks seem to start with a simple email. Given the ubiquity of email and the ease of adding links to messages, attackers typically use email as the path of least resistance to a foothold in your environment. Isolating and analyzing phishing email can yield valuable information about attackers and their tactics.

Given the ubiquity of email and the ease of adding links to messages, attackers typically use email as the path of least resistance to a foothold in your environment. Isolating and analyzing phishing email can yield valuable information about attackers and their tactics.

The ultimate goal of any incident management process is to contain the damage of attacks. This requires you to investigate and find the root causes of attacks faster. In our Email-based Threat Intelligence paper[10], we used a Who, What, Where, and When approach to this kind of intelligence. Identifying the adversary (*who*) yields a ton of information about motive and tactics. Understanding *what* was attacked and *how* tells you whether they used a standard kit or custom malware. You can also evaluate *where* the phishing message compromised the user for additional context about the attacker's current botnets. Finally, assessing *when* the attack happened and how it has evolved can provide clues to what they will do next. Again, you don't need to be right the first time, but guesses provide a place to start looking.

This is just a short summary of the threat intelligence at your disposal. For more check out our papers on Building an Early Warning System[11], Network-based Threat Intelligence[12], and Email-based Threat Intelligence, which offer detail on specific data sources and indicators.

Challenges

That all sounds good, right? You just hit the EZ button, gather some threat intelligence, and find the attackers in a hot minute, leaving plenty of time for golf. Okay, maybe it won't work out like that. Threat intelligence is an emerging capability with an emerging incident response/management practice. So there are a few challenges to operationalizing this kind of approach:

- **Aggregating the data:** Where do you collect the intelligence? You already have systems that can and should automatically integrate intelligence, and use it within rules or an analytics engine. The more automation the better you can handle the urgency of incident management.

- **Analyzing the data:** How do you know what's important within the massive quantity of data at your disposal? You need to continue refining rules and tuning your intelligence feed. As you leverage intel during real responses you get a feel for what works and what isn't so useful, along with opportunities to refine the data and your process. You can also leverage intelligence providers' analyses of data from other customers for ideas about where to focus.

- **Actionable data:** This relates directly to intelligence aggregation — taking it to the next level where tools can automatically search your environment, based on intelligence feeds, to identify attack indicators… perhaps even before the attacker goes operational. Existing tools such as SIEM, network operations devices, and even GRC-type reporting can (and should) leverage this intelligence, as they may all be used during investigation. You will want your forensics tools to play along, with the ability to leverage external intelligence as well.

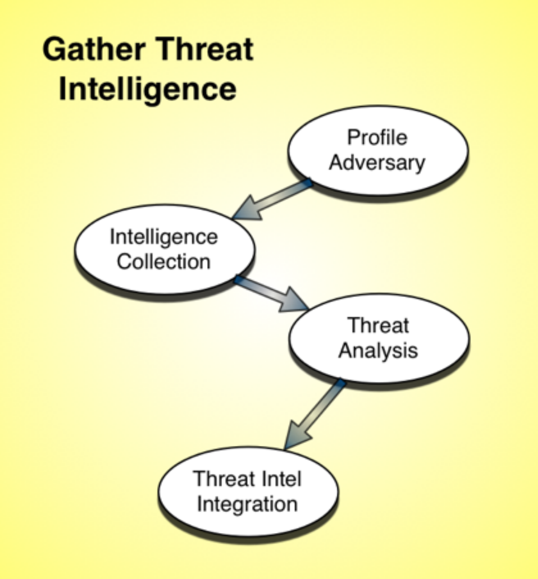
- **False positives/false flags:** Unfortunately threat intelligence is still more art than science. See if your provider can prioritize or rank alerts. Then you can use the most urgent intel earlier and more extensively. Another aspect of threat intelligence to beware is disinformation. Many adversaries shift, using tactics associated with other adversaries to confuse you. That is another reason to not just profile an adversary, but cross-reference them against other information to make sure that adversary makes sense in your environment.

Threat Intelligence + Data Collection = Responding Better

Now let's peel back the next layer of the onion to delve into collecting data that will be useful for investigation, both internally and externally. This starts with gathering threat intelligence to cover the external side. It also involves a systematic effort to gather forensic information from networks and endpoints while leveraging existing security information sources including events, logs, and configurations.

External View: Integrating Threat Intelligence

We described the kinds of threat intelligence at your disposal above, along with how they can help in incident management. But that doesn't address how to gather this information, or where to put it so it's useful when you are knee-deep in response.



First let's discuss the aggregation point. In our Early Warning System paper we described a platform to aggregate threat intelligence. You need it to aggregate third-party intelligence feeds and scan your environment for indicators of potentially compromised devices. To meet these goals a few major capabilities stand out:

- **Open:** The first job of any platform is to facilitate and accelerate investigation — so you need the ability to aggregate threat intelligence and other security data quickly, easily, and flexibly. Intelligence feeds are typically just data (often XML), and increasingly distributed in industry-standard formats such as STIX, which makes integration relatively straightforward.

- **Scalable:** You collect a lot of data during investigation so scalability is essential. Keep in mind the difference between data scalability (the amount of stuff you can store) and computational scalability (your ability to analyze and search it).

- **Flexible search:** Investigations still involve quite a bit of art, rather than being pure formal science. As tools improve and integrated threat intelligence helps narrow down targets for investigation, you will rely less on forensic 'artists'. But you will always be mining collected data and searching for attack indications, regardless of the capabilities of the person with their hands on the keyboard. So your investigation platform must make it easy to search all your data sources, and then identify assets at risk based on what you found.

The key to making this entire process run is automation. We talk about automation a lot these days, for good reason. Things happen too quickly within your technology infrastructure to do much of anything manually, especially in the heat of an investigation. You need to pull threat intelligence in a machine-readable format, and then pump it into an analysis platform without human intervention. So let's dig into the threat intelligence sources for perspective on how to integrate their data into your platform.

- **Compromised devices:** The most actionable intelligence you can get is a clear indication of compromised devices. This provides an excellent place to begin investigation and manage your response. There are many ways you might conclude a device is compromised. The first is clear indicators of command and control traffic in the device's network traffic, such as DNS requests whose frequency and content indicate a domain generating algorithm (DGA) for finding botnet controllers. Monitoring network traffic from the device can also catch files or other sensitive data being transmitted, indicating exfiltration or a remote access trojan.

> The key to making this entire process run is automation. Things happen too quickly to do much of anything manually, especially in the heat of an investigation.

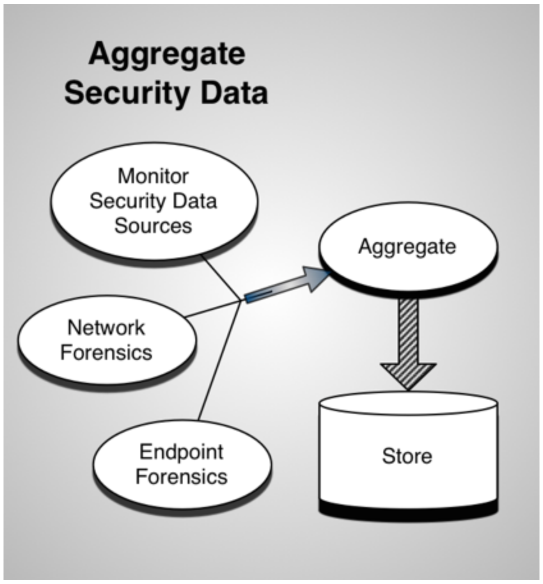
- **Malware indicators:** You can build a lab and perform both static and dynamic analysis of malware samples to identify specific indications of how malware compromises devices. This is a major commitment — thorough and useful analysis requires significant investment, resources, and expertise. The good news is that numerous commercial services now offer those indicators in a format you can use to easily search through collected security data.

- **Adversary networks:** IP reputation data can help you determine the extent of compromise, especially if it is broken up into groups of adversaries. If during your initial investigation you find malware typically associated with Adversary A, you can look for traffic going to networks associated with that adversary. Effective and efficient response requires focus, and knowing which devices may have been compromised in a single attack helps isolate and dig deeper into that attack.

Given the demands of gathering sufficient information to analyze, and the challenge of detecting and codifying appropriate patterns and indicators of compromise, most organizations look for a commercial provider to develop and provide this threat intelligence. It is typically packaged as a feed for direct integration into incident response/monitoring platforms. Wrapping it all together we have the process map above. The map encompasses profiling the adversary, collecting intelligence, analyzing threats, and then integrating threat intelligence into the incident response process.

Internal View: Collecting Forensics

The other side of the coin is making sure you have sufficient information about what's happening in your environment. We have researched selecting and deploying SIEM and Log Management[13] extensively, and environmental information tends to be the low-hanging fruit for populating your internal security data repository. To aid investigation you should monitor the following sources (preferably continuously):



- **Perimeter networks and devices:** The bad guys tend to be *out there,* so they need to cross your perimeter to achieve their mission. Look for issues on devices between them and their targets.

- **Identity:** *Who* is as important as *what,* so analyze who accesses specific resources — especially privileged users.

- **Servers:** We are big fans of anomaly detection, configuration assessment, and whitelisting on critical servers such as domain controllers and app servers, to alert you to funky stuff to investigate at the server level.

- **Databases:** Likewise correlating database anomalies against other types of traffic — such as reconnaissance and network exfiltration — can detect breaches in progress. Better to find out *before* your credit card brand notifies you.

- **File integrity:** Most attacks change key system files, so monitoring their integrity can pinpoint when an attacker tries to make changes. You can even block these attacks using technology like HIPS, but that is a story for another day.

- **Applications:** Finally, you should be able to profile normal transactions and user interactions for your key applications (those accessing protected data) and watch for non-standard activities. That doesn't necessarily indicate a problem, but helps prioritize investigation.

Network Forensics

Now let's go one level deeper, into what's happening in your environment. We can start at the lowest level of the stack: the network. Network forensics tools basically capture all traffic on a given network segment, because the only way to really piece together exactly what happened is to review real traffic. In a forensic investigation this is absolutely crucial, providing detail you cannot get from log records. Capturing *all* network traffic isn't really practical in an organization of scale, but perimeter traffic should be feasible.

Eventually adversaries need to get to the important data to achieve their mission, so if you capture data from key internal networks as well as perimeter traffic — what we call a full packet capture sandwich — you have a better chance of piecing together what happened.

Along with traffic into and out of the perimeter, we recommend capturing packets on critical internal segments as well, typically within the data center. Eventually adversaries need to get to the important data to achieve their mission, so if you capture data from key internal networks as well as perimeter traffic — what we call a full packet capture sandwich — you have a better chance of piecing together what happened.

What about less critical internal networks? You can reduce the amount of data collected by sticking to smaller data streams like IDS alerts, device logs, and NetFlow records — together they provide sufficient detail to pinpoint egregious issues for investigation and subsequent full packet capture. This enables you to focus on areas where attackers are sure to be active (data center and perimeter) without going beyond the point of diminishing returns.

Endpoint Forensics

The hard truth of today's malware is that malicious code might not *look* malicious when it enters your network. But you might later determine it is malicious based on new threat intelligence, and then you will want to know where (if anywhere) that file has been active in your environment. Endpoint forensics, like network forensics, tracks activity on each endpoint at a very granular level at all times, so you can pinpoint what malware did in your environment, and on which devices. This imposes a computational burden on devices and generates a large amount of data, but fortunately we have fancy big data and cloud analytics technologies to ingest and analyze it all, right? During incident response, if you have a malware profile, you can query endpoint forensic data to identify devices which show indications of that infection — regardless of when they were infected.

The objective of endpoint forensics, like network forensics, is to track activity on each endpoint at a very granular level at all times, so you can pinpoint what malware did in your environment, and on which devices.

This kind of information is critical to containing the damage of an attack. The ability to search all devices for indicators found on other compromised devices, or from a threat intelligence feed, can get you past whack-a-mole: finding and dealing with one compromised device at a time.

Single Aggregation Point

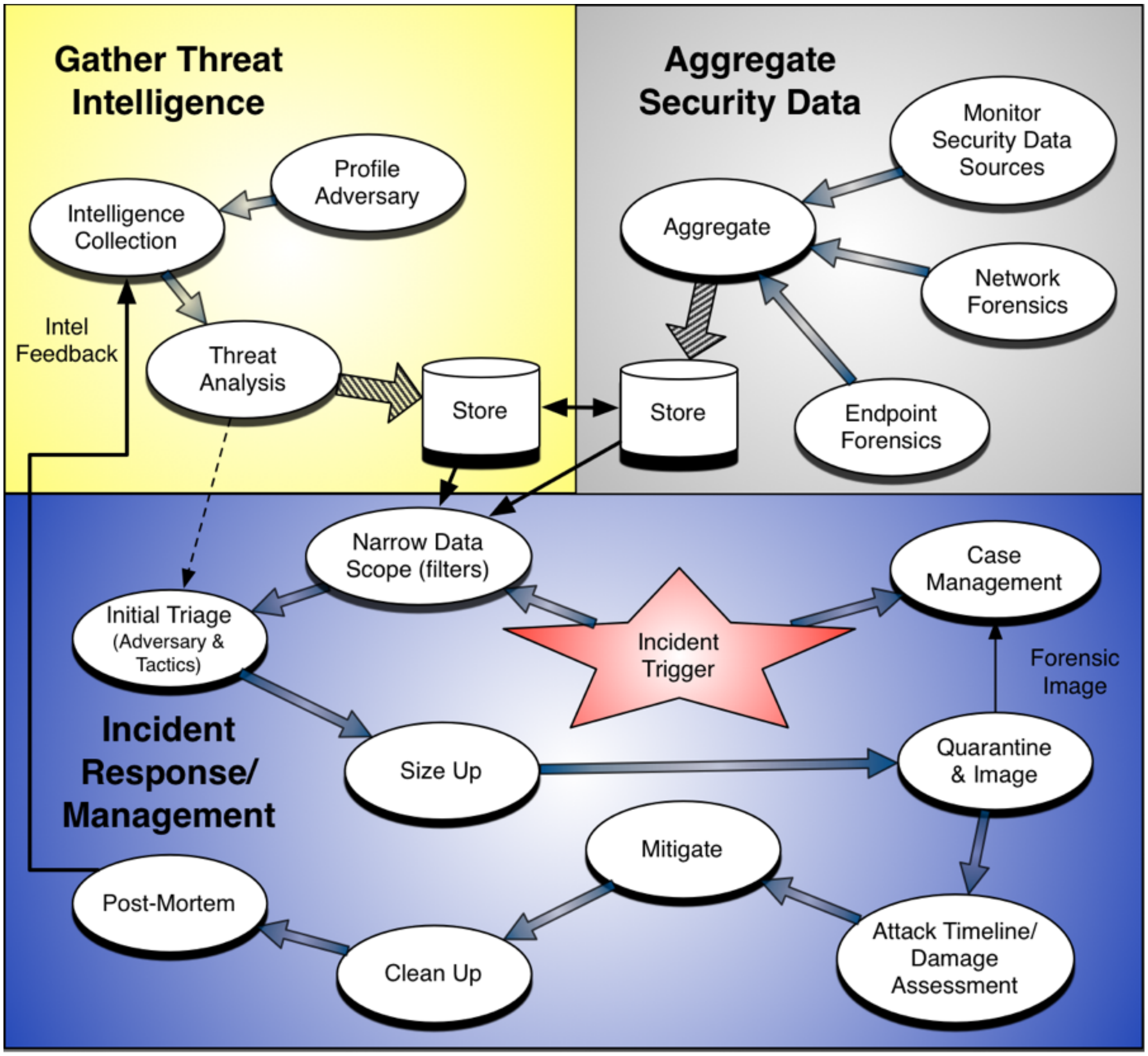
We have used the word *aggregation* multiple times in different contexts in this paper. Incident response/management is driven by data, so you shouldn't be surprised by the need to aggregate threat intelligence and internal security data at multiple layers of this process. At some point you will probably need to aggregate both internal and external data, somewhere you can mine it to accelerate your investigation.

Physical integration is putting all your data into a single repository, and then using it as a central repository for response. *Logical* integration uses valuable pieces of threat intelligence to search for issues within your environment, using separate systems for internal and external data. As usual, we are not religious about how you do this. There are clear advantages to having all data centralized in one place. But as long as you can do your job — collect TI and use it to focus investigation — either way works. Vendors providing big data security all want to be your physical aggregation point, but *results* are what matters — not where your data resides.

For sizing data collection it is important that you be able to analyze log data over at least a 90-day period, with network and endpoint forensic data going back 30 days or more. Today's attackers are patient and persistent, meaning they don't just try smash-and-grab attacks — they stretch attack timelines to 30, 60, and even 90 days. You have two vectors for sizing your system: the number of critical segments to analyze and how long to keep the data. We prefer greater retention for more critical resources such as perimeter and data center devices, rather than analyzing everything quickly and only retaining briefly to make room for newer records.

The (New) Incident Response / Management Process Model

Now that we have the inputs (both internal and external) to our incident response/management process, we are ready to go operational. Let's map out the IR/M process in detail to show where threat intelligence and other security data enable you to respond faster and more effectively.



Trigger and Escalate

You start the incident management process with a trigger that kicks it off, and the basic information you gather depends on what triggered that alert. You may get alerts from all over the place, including monitoring systems and the help desk. Nobody has a shortage of alerts — the problem is figuring out which are critical and then taking immediate action. Moreover, not all alerts require a full incident response — much of what you deal with on a day-to-day basis is handled by existing security processes.

Where do you draw the line? That depends entirely on your organization. In a small business a single system infected with malware might require a response because all devices have access to critical information. But a larger company might handle the same infection within standard operational processes. Regardless of where the line is drawn, communication is critical. All parties must be clear on which situations require a full incident investigation and which do not before you can decide whether to pull the trigger.

> All parties must be clear on which situations require a full incident investigation and which do not before you can decide whether to pull the trigger.

For any incident you need a few key pieces of information early on to guide the following steps. These include:

- What triggered the alert?
- If someone was involved or reported it, who are they?
- What is the reported nature of the incident?
- What is the reported scope of the incident? This is basically the number and nature of systems/records/people involved.
- Are any critical assets involved?
- When did the incident occur, and is it ongoing?
- Are there any known precipitating events for the incident? Is there a clear cause?

Gather what you can from this list to provide an initial picture of what's going on. When the initial responder judges an incident to be more serious it is time to escalate. You should have agreed-upon guidelines for escalation, such as:

- Involvement of designated critical data or systems.
- Malware infecting a certain number of systems.
- Sensitive data detected leaving the organization.

- Unusual traffic/behavior that could indicate an external compromise.

Once you escalate it is time to assign an appropriate resource, request additional resources if needed, and begin the response with triage.

Triage

Before you do anything you need to define accountabilities among the team. That means specifying the incident handler, or the responsible party until a new responsible party is defined. You also need to line up resources to help based on answers to the questions above, to make sure you have the right expertise and context to work through the incident. Our Incident Response Fundamentals series offers more detail on staffing the response.

The next step is to narrow down the scope of data you need to analyze. As discussed earlier in this paper, you spend considerable time and energy collecting events and logs, as well as network and endpoint forensics. *This is a tremendous amount of data so narrowing down the scope of what to investigate is critical.* You might filter on the segments attacked, or logs of the application in question. Perhaps you will collect forensics from all endpoints at a certain office, if you believe the incident was contained. This is all to make the data mining process manageable.

The most important aspect is to have flexible filters so you can see only items relevant to this incident in your forensic search results. Time is of the essence in any response, so you cannot afford to get bogged down with meaningless and irrelevant results as you work through collected data.

Analyze

Once you have filters in place you will want to start analyzing the data to answer several questions:

- Who is attacking you?
- What tactics are they using?
- What is the extent of the potential damage?

Every adversary has their preferred tactics, and whether through adversary analysis or via discovered indicators, you want to leverage external information to understand the attacker and their tactics.

You may have an initial idea based on the alert that triggered the response, but now you need to prove that hypothesis. This is where threat intelligence plays a huge role in accelerating your response. Based on the indicators you found, a TI service can help identify a potentially responsible party, or more likely a handful of candidates. Every adversary has their preferred tactics, and whether through adversary analysis or via discovered indicators, you want to leverage external information to understand the attacker and their tactics. This is the closest we can get to a crystal ball, enabling you to focus your efforts on what the attacker likely did and where.

Then you need to *size up* and scope out the damage. This comes down to the responder's initial impressions as they roll up to the scene. The goal is to take the initial information provided and expand on it as quickly as possible to determine the incident's true extent.

To determine scope you start digging into data to establish the systems, networks, and data involved. You won't be able to pinpoint every single affected device at this point — your goal is to get a handle on how big a problem you are facing, and generate ideas on how best to mitigate it.

Finally, based on the incident handler's initial assessment, you need to decide whether this requires a formal investigation — perhaps due to potential law enforcement impact. If so you need to start thinking about chain of custody for the evidence so you can prove it was not tampered with, and tracking the incident in a case management system. Some organizations treat every incident this way, and that's fine. But not all organizations have sufficient resources or capabilities for that, so they need pre-defined criteria to determine whether to pursue a full-blown formal incident response.

Quarantine and Image

As you get deeper into response you have more decisions to make. The first is how to most effectively contain the damage. Will you take the devices offline? Or will you leave them on and monitor the crap out of them to see what you can learn about your adversary? Another option if you run an advanced security program is to distribute disinformation to your adversary, sending them down a false path or enticing them to further identify themselves.

There are many options for quarantining a device to contain an attack. You could move it onto a separate network with access to nothing real, or disconnect it from the network altogether. You could turn the device off. What you cannot afford to do is act rashly — you need to make sure things do not get worse. Many malware kits (and attackers) will wipe a device if it is powered down or disconnected from the network to self-destruct and destroy the evidence. This is a time to think before you act.

> What you cannot afford to do is act rashly — you need to make sure things do not get worse. Many malware kits (and attackers) will wipe a device if it is powered down or disconnected from the network to self-destruct.

This brings us to your next task: taking forensic images of affected devices. This is especially important if you are thinking about chain of custody for a formal investigation. In this case *how* you capture and store images is as important as *what* you find. You need to make sure your responders understand how the law works and what can provide a basis for reasonable doubt in court. Yes, it sucks that responders need to worry about this stuff, but better learn ahead of time than when a perpetrator walks off with your data, scot-free due to a technicality.

Investigate

Once images are taken and devices are quarantined (or at least safe so they cannot cause more damage), it is time to dig deep into the attack to understand what exactly happened. Our research has shown that timelines are useful because they provide a clear path to figuring out what happened. You start with the initial attack vector and follow the adversary as they systematically work toward achieving their mission. The investigation tracks them moving laterally within your environment, and compromising additional devices on the way to their target. To ensure a complete cleanup you will want to pinpoint exactly which devices were affected, and preferably to review the exfiltrated data via full packet capture from perimeter networks.

Again, investigation is more art than science. Sometimes you lack a clear timeline because a lot of stuff happened at the same time, so focus on what you know. At some point a device was compromised. At another subsequent point data was exfiltrated. Systematically fill in gaps to understand what the attacker did and how. Focus on *completeness* of the investigation — a missed compromised device is sure to mean reinfection somewhere down the line.

Next you'll perform a damage assessment. What was lost? How much data? Exfiltrated data tends to be encrypted by attackers, and you may not be able to break the crypto during your investigation, but the files will yield clues. You know how big the exfiltration was. Your investigation identified the impacted devices. So get out your detective hat and start putting pieces together. If 2gb of data was exfiltrated from the finance network, it probably wasn't the 4tb schematics to your new product on the research segment. Common sense goes a long way during investigation.

Mitigation

Now that you have a better handle on the attack, and are equipped with a timeline of attacker activity, you can begin mitigation. There are many ways to ensure the attack doesn't happen again. Some are temporary, including shutting down access to certain devices via specific protocols. Or locking down traffic in and out of critical servers. Or disabling email attachments to prevent exfiltration of data. Or even blocking outbound communication to certain regions based on adversary intelligence. There are also more 'permanent' mitigations, such as putting in place a service or product to block denial of service attacks. Or possibly wiping affected devices and starting over.

Regardless, you need to establish a list of mitigation activities to address the incident, and marshal resources to get them done. These resources may be internal or external, depending on the extent of the compromise and the availability of resources. We favor *big bang* device remediation, rather than a *rolling thunder* approach of incremental cleaning/reimaging. You want to *eradicate* the adversary from your environment — tipping them off that you know about the attack and are cleaning it slowly just provides opportunity for them to dig deeper.

Of course if it's a widespread attack that will cause unplanned or extensive downtime you won't be popular with either affected employees or the Operations team who has to make your changes. As you manage incidents remember that your objective is to contain the damage to the organization and ensure it doesn't happen again — not to get Christmas cards from everyone.

When is your mitigation done? Once you have halted the damage and regained the ability to continue operations. Your environment may not be pretty as you finish the mitigation, with a bunch of temporary workarounds to protect information and make sure devices are no longer affected. But you don’t get points for elegance — always favor speed over style.

Clean up

Once operations are back online and the damage is contained, it is time to take a step back and clean up any disruptions to normal business operations, making sure you are comfortable that particular attack will not happen again. This might involve leaving in place new controls or policies implemented during the response. For example during an incident you might block all traffic on a certain port to disable the command and control network of a malware infection, or make certain servers read-only to avoid an adversary downloading malware to their file systems.

The clean-up is complete when you have restored all changes to where you were before the incident, or accepted specific changes as a permanent part of your ongoing standards and configurations. Some changes — such as updating patch levels or configurations on devices — will clearly stay, while short-term workarounds need to be backed out to return to your (revised) normal.

While incident managers focus on completing the investigation and cleaning out temporary controls, Operations handles updating software and restoring normal operations. This could mean updating patches on all systems, checking for and cleaning malware, restoring systems from backup and bringing them back up to date, etc.

Postmortem

At this point you have completed your investigation and any remaining activities are out of your hands and the responsibility of Operations. You know what happened, why, and what needs to be done to minimize the chance of a similar incident in the future.

Your last step is to analyze the response process itself. Did you detect the incident quickly enough? Respond fast enough? Respond effectively? What do you need to learn to improve the process? The upshot might be that you are happy with how your team managed the incident. But there are always opportunities for improvement — which may involve changes to the team itself, changes to technology usage or configurations, or broader organizational changes (education, network configuration, and so on). During this analysis you cannot have any sacred cows. No one is perfect and it is okay to make mistakes — once. You don’t want to make the same mistake again.

You cannot completely prevent attacks, so the key is to optimize your response process to detect and manage problems as quickly and efficiently as possible, which brings us full circle back to threat intelligence. You also need to learn about your adversary during this process. You were attacked once and will likely be attacked again. How will you stay on top of adversaries’ tactics, make sure you are keeping up, and stay ready for the new attacks that will be coming your way?

Threat intelligence drives that feedback loop to make sure you are adapting your controls as often as needed to be ready for adversaries, rather than learning what needs to change during another incident response.

Quick Wins

The best way to understand how threat intelligence impacts your incident response/management process is to actually run through an incident scenario with commentary to illustrate the concepts. For simplicity's sake we assume you are familiar with our recommended model for an incident response organization and the responsibilities of the tier 1, 2, and 3 response levels. You can get a refresher in our Incident Response Fundamentals series if necessary.

For brevity we will use an extremely simple high-level example of how the three response tiers typically evaluate, escalate, and manage incidents. If you are dealing with an advanced adversary things will be neither simple nor high-level. But this is an overview of how things come together.

The Trigger

Intellectual property theft is a common mission for advanced attackers so we will use it as the basis for our scenario. You can configure your monitoring system to look for suspicious IP ranges from adversary analysis, based on information from a threat intelligence service provider. But let's not put the cart before the horse. Knowing you have valuable IP (intellectual property), you can infer that a well-funded adversary (perhaps a nation-state or a competitor) has a deep and unwelcome interest in it.

So you configure your monitoring process to look for connections to networks where those adversaries are known to hang out. You get this information from a threat intelligence service and integrate it automatically into your network monitoring environment so you are constantly looking for suspicious network traffic.

Let's say your network monitoring tool fires an alert for an outbound request on a high port to an IP range which threat intelligence has identified as suspicious. The analyst needs to validate the origin of the packet, so he looks and sees the source IP is in Engineering.

The tier 1 analyst passes this information along to a tier 2 responder. Important intellectual property may be involved and he suspects malicious activity, so he also phones the on-call handler to confirm the potential seriousness of the incident and provides a heads-up. Tier 2 takes over and the tier 1 analyst returns to other duties.

The outbound connection is the first indication that something may be funky. An outbound request very well might indicate exfiltration. Hopefully it's not a problem, but you need to assume the worst until proven otherwise. Tracing it back to a network that has access to sensitive data means it is definitely something to investigate more closely. *The key skill at tier 1 is knowing when to get help.* Confirming the alert and pinpointing the device provide the basis for hand-off to tier 2.

Triage

Now the tier 2 analyst is running point. Here is their sequence of steps:

1. The analyst opens an investigation using the formal case process because intellectual property is involved and the agreed-upon response management process requires proper chain of custody when IP is involved.

2. Next the analyst begins a full analysis of network communications from the system in question. The system is no longer actively send data to the suspicious IP addresses, but just in case she blocks all traffic sent there by submitting a high-priority firewall management request for the perimeter firewall.

3. She starts to capture traffic to and from the targeted device. The good news is that all devices within engineering already have active endpoint forensics agents, so a detailed record of device activity is already being captured. The analyst then sets an alert for any other traffic to the suspicious address range to identify other potentially compromised devices.

4. At this point it is time to call or visit the user to see whether this was legitimate (though possibly misguided) activity. The user denies knowing anything about the attack or the networks in question. During that discussion the analyst learns the user doesn't have legitimate access to sensitive intellectual property, even though they work in engineering. Yet their device was compromised and sending information to a command and control network. This might indicate privilege escalation or that the device is a staging area before exfiltration — both bad signs and warranting the analyst to dig deeper.

5. The Endpoint Protection Platform (EPP) logs for that system don't indicate any known malware on the device and this analyst doesn't have access to endpoint forensics, so she cannot dig deeper into the device. She has tapped out her ability to investigate so she notifies her tier 3 contact and the incident handler, apprising both of the severity of the incident.

6. After processing the hand-off she figures she might as well check out the network traffic she started capturing at the first attack indication. The analyst notices outbound requests to a similar destination from one other system on the same subnet, so she informs incident response leadership that they may be investigating a more serious compromise.

7. By mining some logs in the SIEM she finds that the system in question logged into a sensitive file server it doesn't normally access, and then transferred/copied entire directories. It will be a long night.

As we mentioned, tier 2 tends to focus on network forensics and fairly straightforward log analysis because those are usually the quickest ways to pinpoint attack proliferation and gauge severity. The first step is to contain the issue, which entails blocking traffic to the external IP to eliminate any immediate data leakage. You might not know the full extent of the compromise but that shouldn't stop you from taking decisive action to contain the damage as quickly as possible — per the guidance laid down when you designed the incident management process.

Tier 3 is notified at this point — not necessarily to take action, but so they are aware of a potentially serious incident. Proactive communication streamlines escalation.

Next the tier 2 analyst needs to assess the extent of the damage, understanding they cannot have a full picture without the expertise and sophisticated investigation tools used at tier 3. So she searches through the logs and finds similar indicators on another device, which is not good. More than one compromised device might means a major breach. Worse yet, she sees that at least one involved system connected to a sensitive file store and grabbed a large chunk of data.

Digging Deep

Given this new information about the large chunk of content from a key data store, she now needs to hit the PANIC button, escalate, and fully engage tier 3.

- Tier 3 begins in-depth analysis of involved endpoints and network activity, leveraging information provided by the tier 2 analyst. Given the potential adversaries indicated by the outbound connection destination and adversary analysis, tier 3's first step is to analyze those adversaries' recent and favorite tactics. The threat intelligence service identifies five common tactics, with indicators and C&C patterns to look for.

- The search of endpoint forensics data identifies the malware that initially infected a user system, showing a few of the indicators identified by threat intelligence. The malware was delivered via drive-by download after clicking a phishing link. With the primary files and behavioral indicators known — at least for the initial attack — a quick search shows that malware file was delivered to eight devices on the network. But only four devices actually executed it, became compromised, and showed the indicators. Of those four only one additional device has communicated externally (as identified by the tier 2 analyst), which is why network forensics didn't catch the others.

- At this point it is clear that law enforcement will be involved. So forensic images of all impacted devices are taken and stored securely within the case management system. This probably could have been done earlier, but the original focus was on determining the extent of infiltration.

- A deeper dive into the first compromised device shows what appears to be a large encrypted `.rar` file. This could be the exfiltration package. The analyst searches network forensics for that particular file or other movements of a file that size, but analysis shows no evidence that file was transferred out through the perimeter. It appears the organization dodged a bullet and detected the command and control traffic before exfiltration took place.

- The tier 3 analyst now has enough information to fill in the attack timeline. They know where the attack started, the malware used, the lateral movement to compromise other devices, the path to sensitive data, and even the packaging of the exfiltration package. Now they can talk to senior management about how to move forward.

- There is no proof of data loss, so senior management decides to learn what they can about this adversary. Encrypted command and control traffic over a non-standard port is allowed to continue, but all outbound file transfers from the compromised device are blocked. Yes, they run the risk of blocking something legitimate, but senior management has decided this is a worthwhile risk. To make sure nothing is missed additional network forensics gear is deployed to capture all traffic from the affected segments.

- The motivation for allowing C&C traffic is to avoid tipping off attackers that they have been discovered. Experience warns us that prematurely disrupting communications only prompts adversaries to burrow in deeper, making them harder to eradicate.

- The response team moves the sensitive data off that subnet to prevent further loss. Forensics investigators turn the infected system image over to a threat intelligence provider for much deeper malware analysis. The goal is to develop a coordinated plan to clean up and expel the attacker, but to do this they need to fully understand the depth of compromise and identify all involved systems and malware variants.

At the same time outbound transfers are blocked, the response team acts decisively to remove sensitive data from the reach of attackers. This helps contain the damage until the threat can be fully neutralized.

You don't need to do all the analysis yourself either. Threat intelligence providers are usually happy to assist in investigation. The benefit to them is in learning about new tactics, and the benefit to you is that providers perform a more sophisticated analysis than just detonating (executing) a malware file in a on-premise sandbox. You can leverage different providers who focus on phishing packages (the initial attack vector), C&C traffic patterns, and custom malware, for full details of exactly what an attack did and how.

And you need that information because now you have to mitigate and clean up.

Actual sophisticated attacks are rarely this cut and dried, but response team tactics need to be consistent. The objective is always to contain damage while figuring out the extent of the compromise — then you have remediation options.

Mitigation and Cleanup

- This investigation didn't show any exfiltration of sensitive data, and you moved that data out of harm's way, so now you can start to clean up the mess. The team decides to do a *big bang* cleanup — there are only a handful of affected devices, and you want to expel the adversary quickly and completely.

- First thing on Saturday morning the compromised devices are taken offline. They are totally reimaged, and their base configuration and software reinstalled, then patched. Those devices will remain in the lab for a week just to make sure they don't make further attempts to connect to the C&C network.

- You know the C&C targets and traffic dynamics of this adversary, so you implement a set of egress filtering rules on your firewalls and new attack rules on your IPS to block that activity. You also set up rules in your network forensics tool to detect any signs of adversary activity in case active controls miss anything.

- You cannot afford to assume you found all the compromised devices, so you run a credentialed remote scan on every device in your environment, working with Operations and their configuration management product. Your endpoint forensics tool showed you where the file went in your environment, but you want to be sure and confirm that finding.

- At this point the incident management team believes the attack has been mitigated, so cleanup begins to restore operations. The network forensic gear is redeployed but the egress filtering rules will remain. The SIEM is now monitoring for traces of the attack and outbound file transfer restrictions are loosened. But you keep watching for indications the attacker has returned. Ongoing diligence is key.

The mitigation is pretty straightforward. Based on the attack timeline you know which devices were impacted and clean those up. You know the network traffic dynamics so you can watch for suspicious traffic. And it was a manageable number of devices so you could get it all done quickly, before the attacker had time to burrow deeper.

You keep a close eye on the network to make sure the attackers don't return. Yes, this is a reactive step, and sophisticated adversaries may use a different kind of attack to reestablish presence in your environment. But you can only make sure you don't get hit by the *same* attack, so that's your focus.

Finally, once you are pretty confident the attacker is gone, you can start loosening the controls implemented during your response. You will keep some mitigations but at some point business needs to return to normal, whatever that means for your organization. Until next time…

Postmortem

- The CISO needs to present to the board in a week about the impact and lessons from the breach. A postmortem meeting is arranged, including the response team, Operations, the external forensics team brought in to confirm the cleanup, and the threat intelligence provider.

- There were small issues to facilitate the handoff and exchange of information between responders. The threat intelligence provider has started building a team to focus on assisting customers during incident response. And the incident management process was updated to take a forensic snapshot of the device *before* the responder starts investigating.

- There was apparently no exfiltration so the board will be pretty happy with this response. But these changes will improve things for next time.

The key points in this scenario are rapid identification of a serious issue (outbound IP exfiltration), quick escalation to tier 2 for scoping and initial investigation, threat intelligence leveraged to narrow the scope of searches, and rapidly coordinated investigation and response with high-level resources (both internal and external) once it became clear this attack was sophisticated and advanced. The initial handler did a good job of recognizing the problem and understanding he couldn't handle it himself. The second-level responder didn't fall into the trap of focusing too much on the first device and missing the bigger picture. The containment plan provided breathing space for a full cleansing without tipping off the attackers to rush a deeper penetration, or allowing the loss of important assets.

This scenario shows a well-coordinated response to a fairly simple attack. The real world never works quite this smoothly but the fundamentals are the same. Coordinate response, communicate effectively, and learn what you can before you act to mitigate/remediate.

This scenario shows a well-coordinated response to a fairly simple attack. The real world never works quite this smoothly but the fundamentals are the same. Coordinate response, communicate effectively, and learn what you can before you act to mitigate/remediate. Then monitor to make sure you got everything.

Then move on to the next one — and there always is a next one.

Summary

To contain an advanced attack you need to Respond Faster and Better — detecting every attack before it happens is a pipe dream. By focusing on shortening the window between attack and detection, and having a solid plan to contain and then remediate the attack, you give yourself your best chance to survive to fight another day. That is one of the most significant epiphanies security folks can have. You cannot win, so success is about minimizing damage. Yeah, that's crappy, but it is realistic.

The emergence of useful threat intelligence to help focus and prioritize efforts has favorably changed the dynamics of incident response and management. Whether it is identifying IP addresses typically associated with malicious activity, or looking for indications on devices of adversary activity, you can benefit from the misfortune of others who have already been hit by an attack. Knowing what to look for is more than half the battle.

To take advantage of these capabilities we advocate an institutional commitment to data collection at all levels of the computing stack. Given the usefulness of network-level data throughout the incident response process; monitoring tools such as full packet capture and endpoint activity monitoring provide the best chance of being able to detect, contain, isolate, and remediate today's sophisticated attacks.

But no collection of tools will ever replace a skilled team of incident handlers and investigators. Get the right people, establish the right processes, and then give them the tools and support to do what they do best.

But no collection of tools will ever replace a skilled team of incident handlers and investigators. Get the right people, establish the right processes, and then give them the tools and support to do what they do best. We believe the updated process in this research will make a significant difference in helping you keep pace with attackers in a very dynamic environment.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus <https://nexus.securosis.com>.

References

[1] Incident Response Fundamentals: https://securosis.com/blog/incident-response-fundamentals-index-of-posts/

[2] React Faster and Better: https://securosis.com/Research/Publication/react-faster-and-better-new-approaches-for-advanced-incident-response

[3] Continuous Security Monitoring: https://securosis.com/research/publication/continuous-security-monitoring

[4] Future of Security: https://securosis.com/research/publication/the-future-of-security-the-trends-and-technologies-transforming-security

[5] Endpoint Security Buyer's Guide: https://securosis.com/research/publication/the-2014-endpoint-security-buyers-guide

[6] Advanced Endpoint and Server Protection: https://securosis.com/research/advanced-endpoint-and-server-protection

[7] Leveraging Threat Intelligence in Security Monitoring: https://securosis.com/research/publication/leveraging-threat-intelligence-in-security-monitoring

[8] Days of Incite 2007: securityincite.com/blog/mike-rothman/2007-doi-day-9-help-wanted-fortune-teller

[9] Malware Analysis Quant: https://securosis.com/research/publication/malware-analysis-quant-report

[10] Email-based Threat Intelligence: https://securosis.com/research/publication/email-based-threat-intelligence-to-catch-a-phish

[11] Building an Early Warning System: https://securosis.com/research/publication/building-an-early-warning-system

[12] Network-based Threat Intelligence: https://securosis.com/research/publication/network-based-threat-intelligence-searching-for-the-smoking-gun

[13] Security Management 2.5 Replacing your SIEM: https://securosis.com/Research/Publication/security-management-2.5-replacing-your-siem-yet

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <https://securosis.com>.