CounterTack®

Containing Targeted Cyber Attacks: Best Practices for Gaining Control over the Enterprise Endpoint Environment

WHITE PAPER

TABLE OF CONTENTS

Executive Summary

An incident response capability is necessary for organizations of all sizes so that they may rapidly detect incidents, minimize disruption to the business, address the vulnerabilities that were exploited, and get employees working again. Having an incident response process is a critical security function that all organizations need to address. Beyond that, according to numerous studies, a rapid response can make the difference between effective containment and eradication and having a full-blown data breach[1,2]. Unfortunately, most organizations implement only log correlation and report automation capabilities to enable security teams to respond to incidents. While in theory this represents a potential for success, in reality it is far from an effective solution.

Security teams often lack context around what the attack is, what the overall impact might be if executed completely, what the magnitude and reach of the attack are, and how to effectively implement countermeasures. In a large enterprise environment, security teams often receive an unmanageably high volume of alerts from a vast array of sources. Those alerts are usually not prioritized, leading to increased workloads for responders. Because of limited security budgets and the high cost of experienced IR professionals, this often results in organizations unknowingly letting threats successfully infiltrate and achieve their objectives without ever being detected.

This paper addresses the phases of the incident response process and some common pitfalls of their implementation. It also introduces the concept of a layered approach to cybersecurity and incident response including Endpoint Detection, Malware Hunting, and Deep Memory Forensics and their roles in every phase of the incident response process. These three layers combine to provide continuous protection from advanced threats including improved security monitoring, threat detection, and incident response capabilities. An effective endpoint detection system records numerous endpoint and network events and stores this information in a centralized database. Malware hunting tools are then used to provide deeper context and proliferation information. Finally, deep memory forensics provide keys to malware intent including artifacts that can lead to further discovery on other endpoints, and linkages to related malware tools trying to perform reconnaissance.

If implemented correctly, data can be shared between the three levels in both directions to provide an ironclad defense against threats and a swift, effective response to any infections that do occur. These tools also help with rapid investigation into the scope of attacks, and provide a remediation capability.

Introduction to Incident Response

With the concept of a security perimeter disappearing, more complex threats emerging, and the cost of data breaches skyrocketing, incident response has become a fundamental requirement for any successful information security program. Much has been written over the last 15 years about the ineffectiveness of incident prevention and even the inability to detect every piece of malware. Because all enterprises will eventually experience malware infiltration and no detection system is perfect, Incident Response becomes the only remaining weapon against data breaches[3].

Incident Response is defined as the process of detecting and analyzing incidents and limiting each incident's effect, and ordinarily includes four phases: Preparation, Detection & Analysis, Containment, Eradication, and Recovery, and Post-Incident Activity. The figure below illustrates the Incident Response Life Cycle.

Integration and intelligence-sharing to other security data collectors and aggregators is a critical functionality for any endpoint platform. An effective threat solution must be able to work within an organization's broader ecosystem to add more value.

1. "2015 Data Breach Investigations Report," Verizon Enterprise Solutions, http://www.verizonenterprise.com/DBIR/2015/
2. *Mandiant Threat Report "M-Trends 2015: A View from the Front Lines," https://www2.fireeye.com/WEB- 2015-MNDT-RPT-M-Trends-2015_LP.html
3. "On Importance of Incident Response," Anton Chuvakin, http://blogs.gartner.com/anton-chuvakin/2013/07/15/on-importance-of-incident-response/

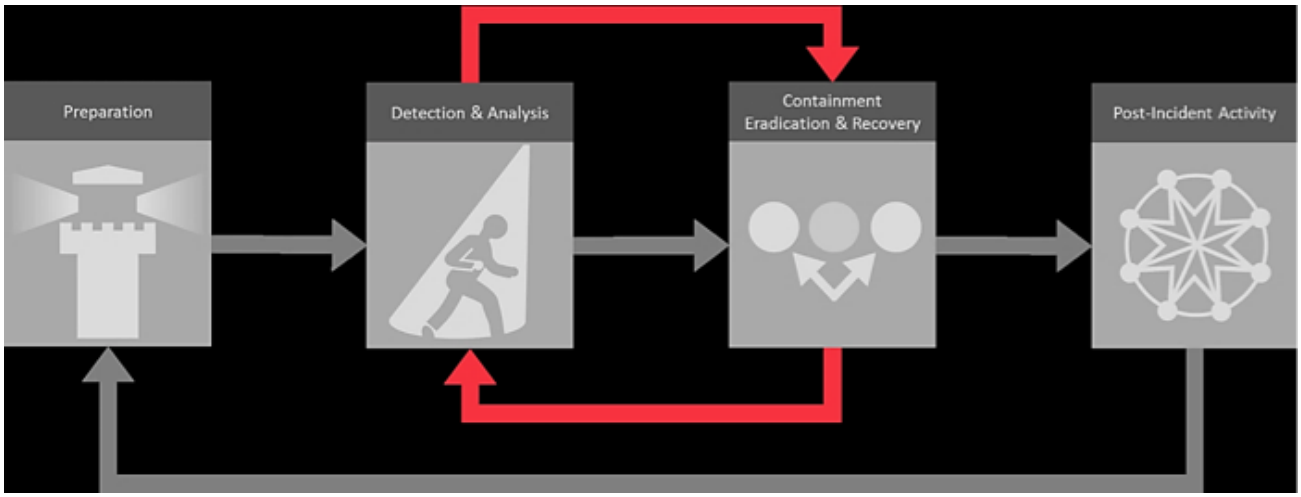

Figure 1. The Incident Response Life Cycle

Cyber-attacks in recent years have become not only more frequent and diverse, but also more harmful and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents. However, a strategy based on prevention is unrealistic and destined to fail in the modern computing environment. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. To efficiently address modern risks, it is important for CISOs to select technology solutions that can be utilized throughout all these phases effectively. Endpoint Detection and Response (EDR) platforms help organizations speed up the ability to investigate security incidents, while also scaling to detect malicious activity across tens and hundreds of thousands of endpoints in enterprise systems.

Preparation

For any organization to build a successful incident response program, preparation is critical. Comprehensive preparation ensures that an organization develops the necessary capability to respond to incidents and that the necessary security safeguards and tools are deployed in order to deliver reliable and sufficient support to all phases of the incident response life cycle.

A specific component of the Preparation phase, after implementing the supporting tools, is managing the integration of those tools to gain true visibility and effectiveness. Enterprise security teams today have sophisticated and broad-reaching security models. Incident Response cannot be managed with a single point solution. The various tools in the process need to work as a security ecosystem, complementing, and augmenting each other's capabilities. For more on integration and common pitfalls, see those two respective sections later in this white paper.

The Preparation phase may be more or less manageable depending on the size of your organization. It is for this reason that management buy-in, appropriate resource allocation, and adoption of industry best practices, methodologies, and principles are key to successful Incident Response preparation. Some milestones in the preparation phase are:

- Developing the Incident Response process
- Appointing and training the Incident Response team

- Developing response plans for different types of incidents
- Establishing communication procedures and protocols during incidents
- Evaluating and implementing the supporting tools for incident response teams
- Implementing policies and procedures for the governance of post-incident activities

Common Pitfalls of Preparation

Selecting the right tools necessary to support incident response is a challenge for any organization. This challenge is compounded with popular EDR solutions becoming increasingly difficult and time consuming to implement and configure. In addition, the implementation of popular endpoint solutions is often constrained and isolated because of the impact they have on system resources and processing power.

Another challenge organizations face is scalability. Tools often lack the ability to scale and tailor themselves to an organization's infrastructure. This is often supplemented with a one-size-fits-all approach. This inability to apply different security profiles to different parts of the organization based on business unit, risk, or system criticality severely impacts the preparation phase. Not all systems, business units, and organizations are created alike and subsequently do not warrant the same types of protections and configurations.

Finally, reliance on one single point solution can be detrimental to one's security posture. No single EDR point solution is capable of detecting, leveraging context, mapping potential other affected endpoints, and reverse engineering malware. A layered approach is necessary, and deployment of security tools without proper integration limits effectiveness. When security products are employed as point solutions and cannot share threat data in real time, analysts lose the ability to see the full scope of the incident.

Detection and Analysis

For many companies, the most challenging part of the incident response process is accurately detecting and analyzing possible incidents, which requires determination of whether an incident has actually occurred and, if so, the type and size of the problem. It is simply not possible for organizations to plan and prepare for the myriad of possible attacks that they might face. Each type of incident introduces unique complexities that require unique response strategies. To this end, the detection and analysis phase represents not only one of the most critical but also one of the most challenging phases in the incident response life cycle.

Nearly all attacks that organizations face today lack any discernible precursors. This places the burden on organizations to ensure that tools are deployed across the infrastructure in such a way that they can quickly identify malicious

Detecting Advanced Threats

In 2014, researchers at RSA discovered a new commercial malware trojan dubbed "Pandemiya," which was designed to steal form data, login credentials, and files, as well as take snapshots of the victim's computer screen and inject fake pages into a browser in an effort to gather additional sensitive information.

The malware took advantage of a Windows function that operates the injection mechanism of itself into every new process opened on the victim's computer and also assured its persistence on a system by checking to ensure that Explorer.exe was injected with its code each time a new process was initiated.

Pandemiya also included protective measures to encrypt the communication with the control panel, and prevent detection by automated network analyzers. Traditional, signature-based endpoint solutions were unable to detect and block this new threat because of the lack of signatures at the time.

signatures or behaviors. These indicators can originate from a variety of sources with the most common being EDR tool alerts, network and software alerts, system logs, and publicly available information.

Each source that provides an indicator will also have varying levels of detail and fidelity. Some incidents have overt indicators that can be easily detected, whereas others are almost impossible to detect. The volume of potential indicators presents a significant challenge for organizations as well. It is commonplace for a Security Operations Center to receive thousands or even millions of alerts every day.

And to ensure malware is unable to evade detection, it is imperative to provide a continuous, uninterrupted, and authentic stream of quality data from endpoints. The data must be received in real time (or near real time) to allow IR to respond promptly, as during a cyber-attack, the data can become stale very quickly. Periodic polling of endpoints results in blind spots, allowing adversaries to execute their intentions and remove traces. The mechanism of data collection on the endpoint must assure continuous operation, therefore being able to resist adversaries' attempts to disable it in any way. If the adversary is successful in preventing data collection, the IR team will face another blind spot and the malicious actions can happen undetected. The data transportation method must be able to resist attempts to alter the data in transit.

An effective detection platform also should provide contextual information, allowing for easy correlation of detected actions. This also helps less experienced operators successfully triage alerts. When information is collected and presented in individual pieces, it requires a concentrated effort by experienced personnel to correlate those 'atoms' of information and rebuild them into 'molecules.' Thus, a security tool that correlates 'atoms' and provides 'molecules' of information to the analyst is guaranteed to make analysts more efficient and the investigation faster. That correlation ability allows even the less experienced analyst to quickly determine the maliciousness of the alert, thereby successfully triaging alerts. Not only does this increase efficiency, but more importantly, it allows Incident Responders to focus on time-sensitive, serious incidents rather than exhausting resources triaging old data or false positives. Proper prioritization of alerts helps eliminate "noise" and hones in on real threats. The positive side effect of adequate context is the shortened time to detection – otherwise known as dwell-time. Currently, on average, it takes roughly 180 days to identify adversarial activity in the organization[4].

How Uroburos Evades Detection

Using signatures or other IOCs has opened the door for stealthy malware like Uroburos to evade detection. Uroburos has a number of key traits that allow it to evade signature-based solutions including persistence, a stealth position in kernel mode, and the effective use of Command and Control (C&C). Its persistence is achieved by creating a service on the Windows OS using a downloaded driver. If your detection platform cannot detect all new services and provide adequate context for each, it won't be effective.

Uroburos also uses its rootkit qualities to remain undetected by most systems so it is necessary for your detection platform to have library (DLL) injection detection capabilities.

Uroburos hides its own network traffic to its C&C by mixing with other legitimate network traffic. It is critical, then, that your detection platform be able to capture events for any outbound communication and correlate host and network data.

Common Pitfalls of Detection and Analysis

Organizations are faced with the challenge of translating these large volumes of indicators (alerts, logs, etc.) into consumable material for security professionals. This means that the various sources for indicators with varying levels of detail and fidelity must be aggregated and correlated to enable both automation and human interpretation.

4. "Data Breaches from Nowhere – Most Compromises Still Being Discovered by Third Parties," John E. Dunn, Computerworld, 6/15/15, http://www.computerworlduk.com/news/security/most-data-breaches-still-discovered-by-third-parties-3615783/

Unfortunately, the traditional EDR products in use today do little to address this challenge. Today's security professionals receive thousands of alerts from multiple sources that are often unmanageable based on volume, lack of detail, and complexity of the tools. Without clear and actionable information returned from the endpoints delineating how that incident might be prioritized, responders are not able to quickly identify, validate, and classify attacks.

This points out the clear need for constant data collection and relevant contextual data with which to make good decisions. Without this, analysts must investigate often thousands of alerts through manual, homegrown research means, or compilation of available information from Google and community sites. Without clear direction and context around the alert, responders spend too much time analyzing and investigating low-risk or even no-risk activity when they should be prioritizing high-risk behavior. It is for this reason that having a layered combination of detection, analysis, and forensics is critical in order to provide context, filtering, and effective triage of events.

Containment, Eradication, and Remediation

These steps represent a robust three-pronged incident response approach. While each component of this phase is vital to incident response, each is also dependent on the other's success.

Containment represents the surgical tourniquet that an organization must apply. It focuses on containing an incident before it is able to overwhelm organizational resources or further damage organizational assets. Containment planning should begin shortly after an incident has begun. This includes making important decisions, such as shutting down critical resources that may impact customers in order to prevent further damage to IT infrastructure in an attempt to sever the kill chain of the Advanced Persistent Threat (APT).

Containing malware on workstations can sometimes be accomplished by simply removing the infected system from the network and eliminating the threat by quarantining it or killing the process. It is therefore critical that your detection layer have the ability to kill a malicious process.

This method is effective if an organization knows which, among its thousands of endpoints, are infected and remediates them all, preventing further spread across the network. Containment is more complex on servers that host popular and often critical applications, as shutting the system down is often not an option. Security teams must work with the infrastructure teams to apply temporary ad hoc containment methods that allow the operation of the applications while attempting to prevent the spread of the malware and its payload.

Letting Some Threats Play Out

Finally, in some situations, analysts may need to let threats play out on non-production endpoints so that they can observe the full functionality of the malware. Effective memory capture and analysis software are critical in this stage of the process. In these instances, by forensically capturing and understanding events in real time, security teams are able to drill into the components of the malware processes or malicious/persistent activity, and significantly reduce incident response investigation cycles, which help to resist future attacks featuring similar behaviors, all without impacting the business. This strategy has to be tempered with the realization that in many cases it is more effective to quarantine a given endpoint thus eradicating the threat, even though all forensic information may not be captured.

Once an incident has been contained, Eradication activities begin. Eradication represents the organization's damage control efforts in response to an incident. Eradication activities may include disabling accounts and shutting down systems until malware can be removed and vulnerabilities can be patched. It is essential that organizations take this time to identify any potential points of compromise within the contained environment and apply the necessary remediation actions to these areas.

Once the environment has been cleaned of any remaining threats and vulnerabilities, the Recovery activities begin. Recovery is solely focused on returning the business back to normal operations. This might mean restoring entire environments and systems through new hardware or clean backups, or entail ensuring that network boundary defenses are hardened against future attacks.

Common Pitfalls of Containment, Eradication, and Remediation

Incidents inherently disrupt and introduce chaos making them that much harder for an organization to efficiently and appropriately manage. Understanding not only the context but also the scope of a threat represents a prevalent challenge organizations are facing today. Without proper context around the attack—either through big data correlation or some level of reverse engineering, the appropriate containment strategy cannot be chosen and most incident responders default to a "pull-and-wipe" process of disconnecting and reimaging any infected systems. This decision leads to significant and unnecessary business disruptions and has the potential to cause more harm than the actual incident itself.

Post-Incident Activities

As painful as incidents are, they also introduce the opportunity to learn and improve. Within a few days of successfully completing the Containment, Eradication, and Remediation phase, a lessons-learned meeting should be held with all applicable incident response stakeholders attending. This meeting should address the effectiveness of existing security controls, any communication issues experienced during the incident, techniques to mitigate future incidents, and any ways to better improve the incident response process. Here is a general list of questions that should be answered during this phase:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What infrastructure deficiencies caused either extra work or lack of visibility such that they should be improved?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurred?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Common Pitfalls of Post-Incident activities

Organizations often fail to grasp the importance and urgency requirements surrounding post-incident activities. More often than not, this means that the lessons-learned meeting is postponed to such a time where the inherent

value and overall purpose of the meeting are completely diminished. Post-incident review meetings should happen very soon after the incident while memories are fresh and relevant data is still available. Waiting months or even weeks after the incident occurred opens up the organization to risks associated with lost experiential data, disappearance of system and state data, and the chance that a similar incident could not only occur but could sweep through the enterprise causing more damage than the original incident.

Integration is a Necessity

As we've discussed, the ability to simply detect is not enough, nor is a deep forensics platform if the data isn't used to adjust scans or explore related—and possibly infected—hosts. And the information is only valuable if one can access it easily in context. For this reason, it is critical in the Incident Response business to integrate the various tools together. This means aggregating data using SIEM as well as using EDR and Network Security techniques in tandem. In addition to the ability to remediate after the fact, one needs to be able to sandbox suspected applications, users, and sites.

Considering the complexity of modern cyber-attacks, especially those performed by well-organized and well-funded adversaries, a successful defense requires a holistic approach. This means a variety of tools must be deployed, accompanied by well-established actions, procedures, and correlation rules. When properly executed, the integration yields results resembling a finished puzzle, each tool representing a piece, which in turn enables the IR team to accurately complete the picture.

Security Information and Event Management (SIEM)

Large enterprises first and foremost need to integrate their EDR solutions with their SIEM. Today's Security Operations Centers often utilize SIEMs as their "single pane of glass" for incident response, and it is important that data received about endpoints is accessible and actionable. The endpoints also need to integrate with other security telemetry such as threat source services, reputation lists, intrusion prevention and detection systems, anti-virus, and firewalls. Finally, the security tools they employ must, when possible, use standardized language to represent structured cyber threat information. Efforts such as CYBOX, STIX, and TAXII enable sharing of actionable cyber threat information across product/service boundaries.

Security analytics and big data management tools correlate all types of endpoint events over long periods of time. Any effective detection platform must have APIs that allow security professionals to integrate other detection and alerting sources in order to deliver the holistic perspective that is key to successful developing and managing your organization's incident response model.

Sandboxing

Any effective integrated suite includes sandboxing capabilities. Any non-validated code from vendors or other outside organizations can be executed to look for malicious behavior. Once codes become suspect, they are then disallowed at the network level. (Complete solutions will include using scratch space on disk at the endpoint level as well.) For this to work effectively, there needs to be solid communication between the sandbox tool and the EDR system and the network security servers.

Network Monitoring

Rather than having separate and independent EDR and Network Monitoring, these two capabilities need to speak to each other and share data. This gets even more critical as enterprise network admins deal with BYOD and the Internet of Things. Bringing network Security Analytics together with Endpoint Detection and Response allows security professionals to view incidents on the network and the endpoint real time. When this integration is done

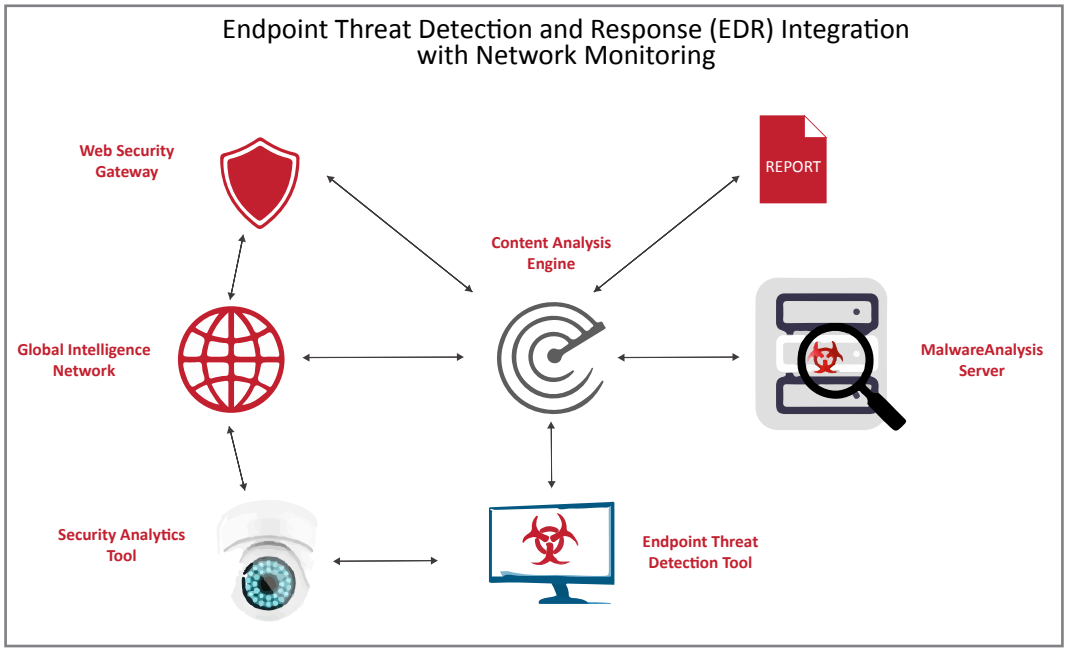

Figure 2. Integrated Network Monitoring and EDR

effectively, operators are able to detect and analyze threats, quickly quarantine endpoints, surgically remove files, and update or re-image any infected endpoints.

For example, identified attack artifacts can be used to enhance perimeter defense tools and prevent further attack spread. When a process running from a file with a known bad hash connects to a remote server, artifacts of the connection (such as remote server name, IP address, and port numbers) can be used to block further infection by modifying firewall rules or port mirroring the connection for deeper packet inspection.

An example use case might involve malware being detected by the network monitoring tool, and this information being sent to the content analysis system as depicted in Figure 2. In an integrated implementation, the content analysis system would then query the EDR system to determine if the malware had reached any endpoints. A report would them be generated which would outline which endpoints are impacted and provide embedded links to remediate. Security Analysts investigating the breach could then pivot into the analytics engine for a holistic network view. This new malware would also be uploaded to the intelligence network such that subsequent attacks can be stopped by the security/ gateway server.

Integrated Detection and Validation Process	
1	Network monitoring system detects new malware and sends information to content analysis
2	Content analysis automatically queries EDR tool to determine if malware reached the endpoint
3	Report generated which provides information on malware detected, which endpoints are impacted, and an embedded link to remediate & quarantine
4	Security Analyst investigating endpoint breach can automatically pivot into security analytics tool for holistic network view
5	New malware is uploaded to global intelligence network; subsequent attacks will be stopped by security gateway

Working Together as a Complementary Suite

Integration also improves the responders' efficiency. For example, resolving incidents by utilizing information from threat intelligence sources allows lower skilled personnel (usually Tier 1) to make educated decisions and alleviate the load that would otherwise fall into the IR team's lap. Suppose the analyst has noticed the execution of a file with a

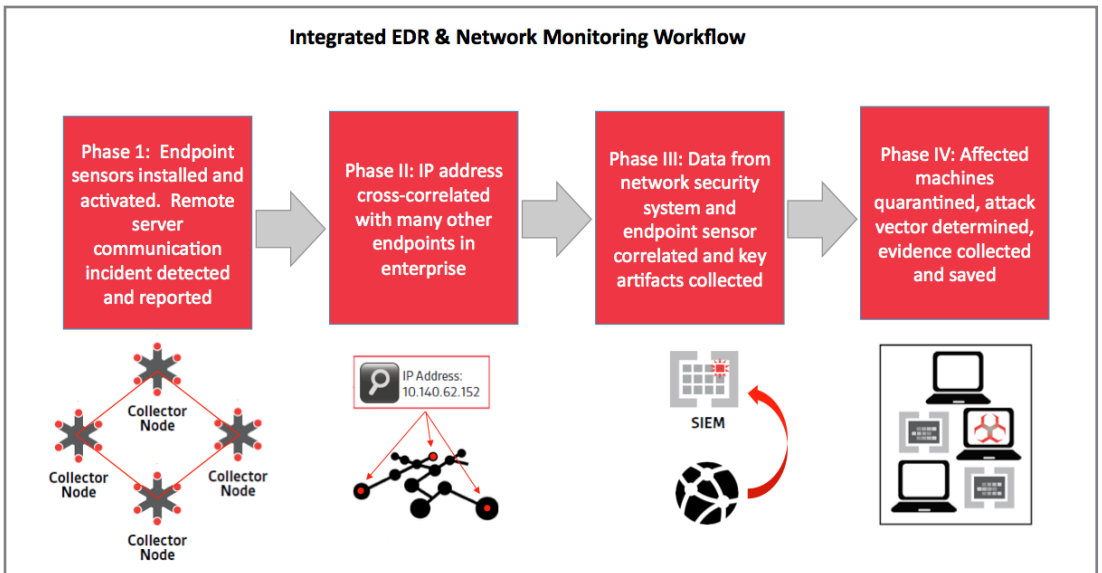

Figure 3. Customer Example of Endpoint and Network Integration Workflow

One integration workflow that has been successfully deployed at customer sites includes a kernel mode detector which dovetails with a network sensor. When an incident is reported by the network sensor, this is reported through to the endpoint sensor/data collector which provides operators information on the affected host, process, file names, and other contextual data. Other information is then offered about other hosts that have communicated with the affected host. The affected machine(s) are then quarantined and remediated. The origins of the attack are then explored based on the preserved data.

strange name. It would require further investigation to find out if the resulting running process is malicious or not, or if the file itself is malware or not. However, threat intelligence source may be able to instantly determine maliciousness of the file by reporting that the file hash matches a known bad hash.

Common Pitfalls of Integration

The lack of integration of the detection, analysis, and forensics tools with other systems like SIEM can increase the burden placed on security professionals. Simple alerts in the SIEM from traditional endpoint protection tools demand that an analyst return to the detecting tool to gather more information that was not passed on to the SIEM. The lack of contextual information then results in the lack of a holistic view of the threat. While a SIEM can correlate events among disparate sources, it is not well-suited to analyzing endpoint behavior directly. APTs can spread out activities to escape notice of detection tools and subsequently an organization's SIEM. Contrast this with the workflow shown in Figure 3 wherein the network security system, EDR and SIEM all work together in a complementary fashion.

In discussing the necessity of having a comprehensive picture of an organization's state of security, the importance of log aggregation provided by SIEM must be stressed. SIEM offers a singular location where information from all other security tools flows in, thus allowing security personnel to create correlation rules that generate information which would otherwise consume serious resources and negatively impact the performance of the IR team. SIEM tools can be used to increase the confidence level of an alert. Suppose a network monitoring tool reported suspicious content on the wire – without knowing if it actually executed on the endpoint. In this case, we couldn't be sure of the seriousness of the alert, but if the endpoint monitoring tool has reported suspicious execution that correlates in time with an alert from the networking tool, the confidence in the alert's importance can be elevated.

5. Tech Target "Is Your SIEM Security Stuck in a Rut?" Anton Chuvakin, November 2014, http://searchsecurity.techtarget.com/feature/SIEM-evolution-Is-your-SIEM-security-stuck-in-a-rut

Scanning and Sampling Examples from Real World Customers

While it is essential that layer 1 detection (using your sensor/data collector) be always on, many customers ask about what scanning policy should be used in which situations and across their various devices and organizational structures. Typically memory scans using behavior-based detection are done daily. Deeper scans looking at registry keys, file attributes, and relevant strings and modules may be run less frequently.

In addition, customers with larger deployments will often divide up their network by OS, IP range, and VIP data repositories. Partitioning scans according to IP ranges allows them to quickly identify the physical assets when a host is infected. Content is also partitioned according to the sensitivity and priority of the data. Often CxO and other Executive level folders are attached to a different set of scan policies than lower-level employee data.

In almost all cases, every endpoint is scanned at least once per day, and often IOC scan policies are set to follow-up daily scans and confirm the absence of malware. Scan policies are also adjusted to the type of endpoint involved (e.g. laptop, workstation, server). For example, because servers normally wouldn't have flash installed they would not be scanned for flash exploits.

Many similar scenarios can be constructed, essentially allowing the security team to validate individual alerts and triage appropriately.

Furthermore, many integrations fail because of poorly executed deployments[5]. Often SIEM's solutions are not kept up-to-date. In other cases, data is collected but not used.

Using a Layered Approach to Improve Your IR Capability

Recent breaches and attacks have shown that simplistic approaches to security often fail due to poor coverage of threats and the inability to quickly detect, analyze, and respond when incidents occur. Detecting malware is pointless if one can't quickly understand its context, which hosts are infected, and which other hosts are at risk. Information must be shared across these activities in order to adjust scans and locate, isolate, and remediate the bad stuff.

The true objective of incident response is to limit disruption to the business. Successful incident response programs require endpoint detection and response solutions that can immediately inform responders which systems are infected and most at risk, clearly define behaviors that indicate compromise, and report how these systems became infected. Responders need to be able to identify attack artifacts in real-time and quickly determine if a post-breach forensics investigation is warranted. Further, it is necessary to gain a thorough understanding and context of detected suspicious activity, the short-term impact of that behavior, and visibility into the potential impact on the broader system if a response is not implemented.

Incident Response teams require a complete suite of detection and forensics tools to combat the increasing frequency of attacks and growing skills of the attackers they face. The installation and configuration of endpoint detection and response tools should be easy to manage, enterprise-scale friendly, and completely invisible to end-users, applications, operating systems, and threats.

To wage a successful fight against attacks and be able to effectively respond when they occur requires not only superior detection capability but a significant amount of correlation and context once a breach is discovered in order to both grasp the magnitude of the infection and successfully isolate it.

Any effective suite of tools must include:

1. **Continuous Detection** — A low-profile, tamper-resistant, always-on detection platform that can not only identify known malware but also new malware for which signatures do not exist. Agent-based tools are typically detrimental to user and network performance and difficult to scale.
2. **Malware Hunting** — A follow-on malware hunting platform that can dive deeper into suspected endpoints and conduct deeper analytics on a regular basis. At this layer, scans are completed on a regular basis and frequently enough to uncover latent malware.
3. **Forensics** — A deep memory forensics capability which can analyze malware, identify names and strings in order to sleuth other endpoints that may have related infections, and reverse engineer the malware in order to determine critical factors such as processes being spawned, methods of surviving reboot, and C&C locations.

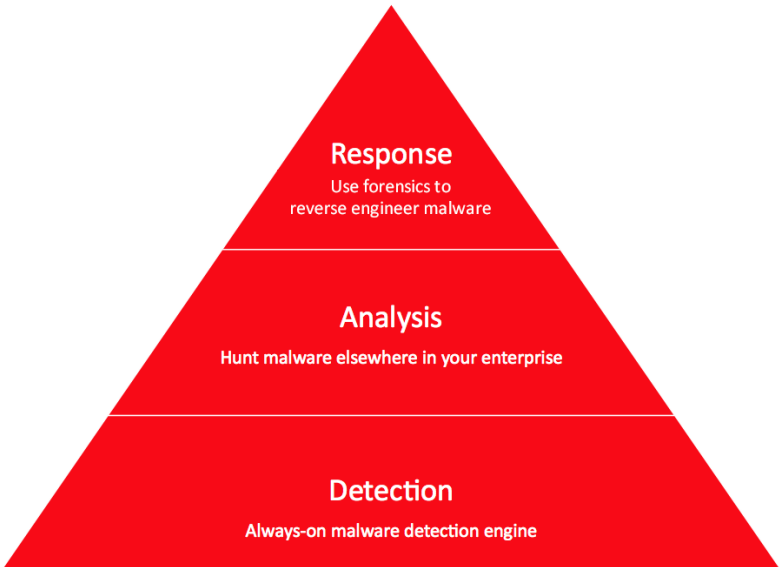

Figure 4. Detection, Analysis, and Response Workflow

Advanced Detection & Contextual Insight

The appropriate solution must provide contextual insight into endpoints.

- It should detect and follow attacks through the entire attack lifecycle to provide comprehensive and actionable intelligence to teams in order to counter threats in real-time.
- It should help teams respond to security incidents of potentially unknown origin, without relying solely on the observation of binaries, or 'known good' databases like whitelists.
- It should use both behavior and algorithmic analysis to determine the potential maliciousness of a set of events and in doing so, identify a set of behaviors as outside normal user behavior.

Scalable, Always-on Detection Platform

The detection platform must include built-in workflows that incident responders and security operations teams can leverage to assign work to each other, mark attacks as remediated, and even automatically provide different behavioral analysis capabilities based on where the endpoint is located.

It must also provide the speed, scale, intelligence, and visibility that organizations need to face today's threats. It has to support organizations in the detection of threats and the analysis of incident-related data, and provide the means to respond with a deeper dive using layers 2 and 3. Indicators of Compromise and signatures are not adequate to catch brand-new threats and relying on them will open up your organization to lengthy dwell times in which malware resides in your organization, scouting, collecting, and preparing for the ultimate breach. It is critical that behaviors (the activities performed by the malware while in memory) be captured and assessed at this layer. And for the subsequent layers to be effective as a follow-on, they too must incorporate in-memory behaviors into their malware detection and analysis.

Continuous Data Collection using a Tamper-Resistant Sensor

A true agentless detection solution should install directly into the kernel layer of your endpoints and allow endpoint behavioral data to be collected without impacting host resources or processing power. This kind of tamper-resistant agent prevents attackers and malicious code from detecting, tampering, and most importantly, evading the sensor. This paradoxical combination of innovative capabilities symbolizes the start of a paradigm shift in how we look at endpoint technologies in today's world.

When analysts receive a clear, undetected view into the attack behavior, they can more accurately determine if there was lateral movement, if data was exfiltrated, or if the attacker attempted to cover their tracks. Consequently, the incident responders can choose an appropriate response strategy rather than just defaulting to the disconnecting and reimaging of a system.

Contextual and Behavioral Analysis

One critically important requirement of a detection platform is the ability to derive contextual and situational awareness about advanced threats. This enables incident responders to not only identify the attack vector but to also understand attackers' motives. It should be able to capture data that enables teams to drill into the components of an attack, malware processes, or malicious and persistent activity, to significantly reduce incident response investigation cycles and to help resist future attacks featuring similar behaviors.

Studies have shown that all enterprises will be infected by some level of malware, and a strategy that relies on protecting the enterprise from malware infiltration will be ineffective. Any successful strategy must incorporate the ability to respond quickly to any suspected attack and delve deeper into the nature, scope, and location of infections. A regular deep dive into a sampling of endpoints will provide significant value in detecting latent malicious code.

Special Considerations: Insider Threats

Defending an organization would be simpler if the adversary invariably came from the outside, but this is not always the case.

What complicates the threat situation is the case of the malicious insider. Even inadvertent actions, either out of ignorance or carelessness, can unfortunately have disastrous consequences. Malicious insiders present a whole new set of enigmas: they are already in the network, rendering perimeter defenses useless; they know the network and where assets of interests are – so there is no need to explore the network; their movement is hard to label as suspicious because it could be part of normal daily activity; finally, they have no need to download any malware or engage exploits to establish foothold in the network.

In order to handle an insider threat, the organization must prepare and implement proper IR procedures and protocols, and acquire the adequate tools. Amongst its capabilities, the security tool needs to be able to detect when the insider changes host registry configuration to enable USB key use, or when the user copies data a USB key and removes the data from his/her computer, or when the insider connects to remote shared folders he/she is not supposed to and downloads sensitive information.

6. Webinar presented to ECC Council on 11/12/15, "Fighting Advanced Malware with Responder PRO," http://www.countertack.com/fighting-malware-with-responder-pro-webinar-recording

Insider Threats (Continued)

In addition to the technical aspect of identifying a malicious insider, the organization and its IR team have to have to take into account the legal aspects should the employee get falsely accused. This points back to the importance of collected data – its quality and context. The better context of activity is presented to IR investigators, the better chances of making the right decision. Knowing the circumstances of an activity – the who, when, where, what, how—and whether an administrator or regular user is involved can mean the world of difference, and separates success from false positives. John Doe from the manufacturing department should not be accused of malicious activity (detected by his computer running a remote control tool like 'psexec'), if it was actually the network administrator troubleshooting problems – the distinction easily made by having user account information and SID as part of the available context.

Malware Hunting Engine

As discussed in the Containment, Eradication, and Recovery section, moving to the second layer of incident response requires a more in-depth malware hunting and analysis tool.

This layer of malware hunting software must be able to detect malware never seen before. Due to the analytical requirements of this type of software, there will typically be some performance impact to the network and/or endpoints. For this reason, a sampling strategy for both location and time must be devised. For example, a daily scan of all endpoints, using the right malware hunting software, will provide huge benefits in improving detection and shortening the dwell time or "detection deficit" window[6].

Deep Memory Forensics

The final critical tool needed is a strong forensics platform capable of reverse engineering code, identifying relationships between code modules, divulging strings, and other important malware artifacts. This layer needs to show operators how code modules relate, and provide key intelligence on variants, so teams can proactively hunt down malicious pieces of code across the enterprise. With this tool, teams should have the capability to sleuth modules, Resource Handles, and other system objects, in addition to setting system policies to root out other compromised endpoints. Methods of surviving reboot, OS hooks, spawned processes, and captured passwords are critically important clues to the malware and need to be thoroughly investigated.

And with the rise of nation state attacks in recent years, it is no longer adequate to look for potential breaches that might focus strictly on customer records or financial data, which have been the targets of past years[7]. These cyber warfare attackers have broader motives, use variants of malware that have no signatures and exhibit behaviors that are different than "stock" malware.

Complementary Suite

All three layers need to integrate and work together in a robust, interactive cycle of Detection, Hunting, and Forensics. No one tool can succeed alone. They need to be able to interact and share data. Discoveries through one tool need to drive the deeper dive into the "mind" of the attacker in order to identify the full extent and the intent of the malware infection.

Sending Information Upstream

Just as information can be shared downstream in terms of discoveries in Layer 1 seeding deeper scans in Layer 2, the flow of information in the opposite direction can be extremely valuable. For example, if an anomaly is discovered and analyzed using a Layer 3 memory forensics tool, specific information about strings, processes, and other code relationships can be used to set a sampling scan in Layer 2 to hunt malware.

7. "The Rise of Nation State Attacks," Ponemon Institute, October 2015, http://www.countertack.com/ponemon-rise-of-nation-state-attacks-report

Summary

Effective incident response needs to include the four critical steps from Preparation, through Detection and Analysis to Containment/Remediation, and finally on to Post Incident Activities. As we've discussed, Incident Response cannot be limited to just data collection or only scanning memory. There is no single point product that acts as a silver bullet. Rather, an effective approach needs to not only provide a continuous stream of unabated data, detect malware, and address forensics needs--which in turn feed back into scan policies--but this information should be shared effectively and integrated using a SIEM. Information and context gained in the early stages of detection need to be correlated and used in the latter forensics portion and this fed back to scan policies. While whitelisting alone will not keep your enterprise safe, it is critical that not only known malware be identified (signatures, whitelists) but also unknown malware be hunted down using behavior-based and Big Data methods.

An ironclad defense should provide information about which systems are infected and at risk, as well as what behaviors indicated the compromise. It should provide specific, readily accessible information on with which IP addresses a compromised system communicated and where the various suspicious modules and strings reside.

If this sounds like a lot of work, it can be. This is one area in which partnering with an experienced security company who can both help strategize but also implement the multi-layered solution can be a very effective combatant against being breached.

CounterTack®

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com

References

1. Ponemon Institute Threat Intelligence & Incident Response: A Study of U.S. & EMEA Organizations, February 2014
2. National Institute of Standards and Technology, Special Publication 800-61 Revision 2, August 2012
3. The term "Endpoint Detection and Response Solution" was coined by the industry analyst firm Gartner. See for example the-research note Market Guide for Endpoint Detection and Response Solutions, published May 13, 2014
4. For examples of APTs, see RSA Anatomy or an Attack, https://blogs.rsa.com/anatomy-ofan-attack/and SANS Institute: A Detailed Analysis of an Advanced Persistent Threat Malware, http://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814