CONTAINING SECURITY INCIDENT RESPONSE COSTS

THE GROWING CHALLENGES RELATED TO INCIDENT RESPONSE AND THEIR IMPACT ON OPERATIONAL COSTS

2019 Whitepaper

ENSILO
REAL-TIME AUTOMATED ENDPOINT SECURITY

CONTAINING SECURITY INCIDENT RESPONSE COSTS

ENSILO

OVERVIEW

Of the many challenges security leaders face, one big issue can often be downplayed: budget. Leaders are expected to manage a large and complex volume of stealthy attacks on endpoints while responding quickly and effectively to incidents without exceeding planned capital expense (CapEx) and operating expense (OpEx) budgets. Compounding this challenge is the significant demand for the narrow supply of security analysts skilled in advanced malware forensics, forcing long recruiting cycles and high wages.

While the cost of a breach is well documented, the operational costs of managing a security team that can prevent known attacks as well as detect, contain, respond and remediate unknown attacks are not.

That's especially problematic given today's threat landscape which includes a range of advanced, unknown and persistent threats such as fileless or memory-b ased attacks and polymorphic malware. These attacks move fast, often in seconds rather than minutes or hours; attackers can dwell in networks for weeks and months before detection. According to the Ponemon Institute's 2018 Cost of a Data Breach Study (July 2018), three critical measurements of time for incident detection and response remain far too high, with no meaningful sign of improvement.

METRIC	DAYS	Y/Y IMPROVEMENT
MEAN-TIME-TO-IDENTIFY (MTTI)	197 DAYS	6 DAYS OR 3.0%
MEAN-TIME-TO-CONTAIN (MTTC)	69 DAYS	3 DAYS OR 4.3%
MEAN-TIME-TO-RESPOND (MTTR)	6 DAYS	N/A

Additionally, in-demand incident response (IR) teams are often overloaded and unable to process all incidents fully. Every incident initiates a chain of events that spiral across a breadth of operations: classification, notification investigation, remediation and more. Increasingly complex attacks lead to more incidents which generate more costs by escalating the burden of human-intensive response operations. Initial cost estimates for endpoint protection and endpoint detection and response solutions often don't factor in these extenuating operational costs, further increasing human intervention when the inevitable happens.

Hiring more experienced security analysts to distribute the workload and reduce response times may provide some relief. But hiring is also challenged by the high salary costs for experienced analysts and the lengthy cycles it can take to find and recruit the right candidates.

The good news is that enSilo directly solves the problem of uncontained and unexpected incident response costs. The enSilo Endpoint Security Platform is a comprehensive endpoint security solution with real-time automated pre- and post-infection protection and orchestrated incident response, that not only contains and caps costs but also makes them predictable before an incident occurs.

"HIRING MORE EXPERIENCED SECURITY ANALYSTS TO DISTRIBUTE THE WORKLOAD AND REDUCE RESPONSE TIMES MAY PROVIDE SOME RELIEF. BUT HIRING IS ALSO CHALLENGED BY THE HIGH SALARY COSTS FOR EXPERIENCED ANALYSTS AND THE LENGTHY CYCLES IT CAN TAKE TO FIND AND RECRUIT THE RIGHT CANDIDATES."

INCIDENT RESPONSE – RESPONSIBILITIES AND STAFFING

The IR function is a critical part of preventing or limiting the damage from a cyber-attack. According to the NIST Framework for Improving Critical Infrastructure Cybersecurity, the goal of this function is to contain the impact of a potential cybersecurity incident; it's also the driver for communications, analysis, mitigation and improvements processes.[1] Staffing estimates for an IR team range anywhere from three to more than nine, depending on the size of the organization, the complexity of the infrastructure and the required amount of hourly coverage.

Each time an incident takes place, malicious activity is detected, and an event is generated, the IR team execute a series of actions, including:

- **Classification -** Assessing the attack as good, bad, false positive or false negative
- **Notification -** Sending alerts to users and support groups
- **Containment -** Isolating endpoints to prevent the spread of the infection
- **Investigation -** Analyzing events and conducting forensics to better understand the complete attack chain
- **Remediation -** Terminating malicious processes, deleting persistent data and settings
- **System Tuning -** Creating policy exceptions to allow for approved applications as well as reduce false positives and false negatives
- **Reclassification -** Modifying incident classifications when new intelligence is available, which can trigger additional response actions

BASIC TECHNICAL KNOWLEDGE NEEDED FOR IR

- Security Principals
- Security Vulnerability & Weaknesses
- Internet Infrastructure
- Computer Security Risk Analysis
- Common Network Applications & Services
- Network and host-level security
- Malicious code
- Programming
- Incident-handling interpersonal skills

DRIVERS OF UNPREDICTABLE INCIDENT RESPONSE COSTS

Building an IR team requires overcoming two challenges: responding to increasingly sophisticated and stealthy attacks that evade detection and are difficult to analyze, and supporting the number of skilled, in-demand security analysts needed to operate each step in the IR process. Both of these challenges place tremendous pressure on CapEx and OpEx budgets.

CHALLENGE #1 INCREASINGLY COMPLEX AND STEALTHY ATTACKS

IT Security and dedicated IR teams have to analyze more threats; those threats are increasingly complex and capable of evading detection by traditional endpoint security tools. But human-driven analysis consumes precious time during which attackers can have access to your systems and data. Analysis is a manual process of painstakingly reviewing atypical compromise indicators and determining the appropriate response. For example, how many indicators of compromise do you have? How many do you need to warrant investigation? How does one even come to be an indicator? Threats are just moving too quickly to tolerate the delays inherent in manual response.

> "THREATS ARE JUST MOVING TOO QUICKLY TO TOLERATE THE DELAYS INHERENT IN MANUAL RESPONSE."

CHALLENGE #2 SKILLED SECURITY ANALYST SHORTAGE

Staffing for this wide range of needs can feel uncontrollable. It's expensive to build an army; well-qualified security pros are among the most elite and hard-to-find workers in technology. According to the Software Engineering Institute at Carnegie Mellon University, home of US-CERT, other than necessary personal and incident handling skills, the basic technical skills for IR professionals include an understanding of security principles, security vulnerabilities and weaknesses, internet infrastructure, computer security risk analysis, network protocols and their related specifications, common network applications and services, network and host-level security and malicious code. Also, some programming experience is required.[2] That is quite a list.

Today's most-coveted SOC skill involves human eyes darting between screens and deciding what to do first when attempting to make sense of anomalies. Aside from that being mostly a reactive exercise taking place after the damage is done, the labor shortage of people with these skills makes them costly to hire and retain. Also, because it's nearly impossible to predict the number of analysts needed to analyze the increasing volume of cyber attacks and their corresponding indicators, operational expenditures (OpEx) related to salary costs are continual wild cards.

A DETECT-THEN-DECIDE APPROACH ONLY INCREASES COSTS

Among the many things that keep security leaders up at night is the possibility of their systems failing to spot the signal in the noise and respond to a breach quickly enough, while there is still time to protect the data and contain the incident. However, most incident detection and response processes use a detect-then-decide approach. Today, attacks occur in seconds, which is faster than an IR team can detect and then decide how to respond. The Ponemon Institute's well-known data breach cost study puts the price at $3.86M per incident for large enterprises.[3] Once a breach and potentially a theft have occurred, the opportunity to prevent the threat has passed. Your valuable IR resources are now focused on cleanup and damage control rather than on preventing future cyber attacks and breaches.

> "RESEARCH BY ENSILO DEMONSTRATED HOW FILELESS MALWARE ATTACKS, WHICH USE ADVANCED TECHNIQUES TO EXECUTE IN MEMORY, CAN BYPASS TRADITIONAL USER-MODE ENDPOINT PROTECTION PLATFORMS, SUCCESSFULLY EXECUTE RANSOMWARE AND ENCRYPT A WORKSTATION IN LESS THAN THIRTY SECONDS."

Several types of malware detected in 2018 reveal methods used by attackers to evade detection and strike faster than IR teams can respond. Research by enSilo demonstrated how fileless malware attacks, which use advanced techniques to execute in memory, can bypass traditional user-mode endpoint protection platforms, successfully execute ransomware and encrypt a workstation in less than thirty seconds.

Another discovery by enSilo involved a technique for bypassing Windows kernel protections which expose kernel-mode functions to interception by malicious actors and potentially allow malware to go undetected by third-party security products that rely on user-mode hooks to monitor the Operating System (OS). DarkGate Malware, a sample discovered in the wild by enSilo, employs a bypass technique to evade identification by various endpoint protection platforms for an extended period and can deploy multiple cryptominer and ransomware payloads.

Given these sophisticated and fast-moving attacks, it's easy to see how the strategy of detecting first and then manually deciding deciding how to respond attributes to more incidents and greater incident response costs. While large enterprises with bigger OpEx budgets and mature security operations centers (SOCs) can adjust or add resources to address problems as they arise, mid-sized companies may not have the same staffing and financial resources. That leads to significant tradeoffs in their security investment decisions.

STRATEGIES FOR CONTAINING INCIDENT RESPONSE COSTS

While attackers appear to have the tactical advantages of stealth and speed which can increase IR costs, there are several strategies security leaders can use to overcome these tactics and control IR costs. Paramount to success is the implementation of an endpoint security platform which uses a pre- and post-infection prevention-based approach coupled with automation and orchestration technologies.

#1 PROTECT THE DATA AND STOP THE BREACH

Regardless of whether an attack is vulnerability-based, file-based, fileless or a hybrid, there is a common goal: the theft, modification, and/or destruction of data. The first step is preventing malicious actors from accessing, modifying or exfiltrating data, or communicating externally to download additional payloads and instructions, is critical to defeating the attack and stopping the breach quickly. Correlating OS activities for opening a network connection or accessing a file, and

> "THE FASTER THE THREAT IS CONTAINED THE LESS DAMAGE IT CAN DO, WHICH MINIMIZES THE AMOUNT OF RESOURCES NEEDED TO RESPOND TO IT."

detecting deviations from that designed OS behavior, separate legitimate threats from normal actions. The faster the threat is contained the less damage it can do, which minimizes the amount of resources needed to respond to it.

#2 AUTOMATE ANALYSIS AND CLASSIFICATION

Attackers are increasingly employing automation to target multiple endpoints in a single attack; it's time to fight fire with fire. Automation technologies now make it possible for security teams to be more effective in detecting and mitigating genuine threats, ultimately reducing the costs and limiting the damage of data breaches. Automation frees skilled analysts to move beyond manual correlation of data and focus on more strategic analysis, planning and remediation.

#3 INCREASE EFFICIENCY WITH ORCHESTRATED INCIDENT RESPONSE

Orchestrating response actions across multiple types of endpoints and operating systems dramatically improves efficiency, enabling a single operator to manage IR across several thousand devices or more. For example, establishing incident response playbooks comprised of automated actions which include isolating endpoints, automatically opening tickets, and

> "AUTOMATION CAN VIRTUALLY ELIMINATE THE PAINSTAKING DISCOVERY AND CLEAN-UP STEPS INVOLVED IN REMEDIATION, WHICH CAN BE AMONG THE MOST TIME-CONSUMING AND COSTLY ASPECTS OF INCIDENT RESPONSE."

remediating endpoints by terminating processes and removing persistent data and settings allows a small number of IR investigators to contain and remediate a threat while also being able to focus on more complex systems. Automation can virtually eliminate the painstaking discovery and clean-up steps involved in remediation, which can be among the most time-consuming and costly aspects of incident response.

CONCLUSION

More sophisticated and frequent attacks combined with unpredictable IR costs leave security budgets continually squeezed. The equation needs to change. Security automation and orchestration are the solution for security leaders caught in the balancing act; they also multiply the bandwidth and effectiveness of over-worked, hard-to-find security professionals, freeing their cycles for higher value work. The enSilo Endpoint Security Platform applies automation and orchestration to pre- and post-infection needs, empowering security leaders to both predict and contain IR costs, and solve one of today's biggest security challenges.

> "THE ENSILO ENDPOINT SECURITY PLATFORM APPLIES AUTOMATION AND ORCHESTRATION TO PRE- AND POST-INFECTION NEEDS, EMPOWERING SECURITY LEADERS TO BOTH PREDICT AND CONTAIN IR COSTS, AND SOLVE ONE OF TODAY'S BIGGEST SECURITY CHALLENGES."

ABOUT ENSILO

enSilo protects businesses around the world from data breaches and disruption caused by cyber attacks. The enSilo Endpoint Security Platform comprehensively secures endpoints in real-time pre- and post-infection without alert fatigue, excessive dwell time or breach anxiety while also containing incident response costs by orchestrating automated detection, prevention and incident response actions against advanced malware and ransomware. enSilo's patented approach stops modern malware with a high degree of precision, provides full system visibility and an intuitive user interface and combines next-generation antivirus (NGAV), application communication control, automated endpoint detection and response (EDR) with real-time blocking, threat hunting, incident response, and virtual patching capabilities in a single agent. The platform can be deployed either in the cloud or on-premises and supports multi-tenancy. To learn more visit http://www.ensilo.com/

CONTACT ENSILO

enSilo is headquartered at 182 Second Street, Suite 210 San Francisco, CA 94105
Email us at contact@ensilo.com or call us at 800.413.1782 2018

REQUEST A DEMO

https://info.ensilo.com/schedule-demo

[1]National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.1, April, 2018
[2]Software Engineering Institute, Carnegie Mellon University, "What Skills Are Needed When Staffing Your CSIRT", March, 2016
[3]Ponemon Institute, "2018 Cost of a Data Breach Study", July, 2018