Security Connected Reference Architecture
Technology Blueprint

Combatting Advanced Targeted Attacks: CORRECT

Part III of the Combatting Advanced Targeted Attacks Blueprint Trilogy

Intel® Security recommends a three-pronged approach for stopping advanced targeted attacks. This document describes ways to facilitate triage and prioritization for fluid investigation and rapid remediation. As you learn, your solution should apply insights immediately throughout a collaborative infrastructure. To see the entire story, read the two companion Protect and Detect blueprints.

Compress Response Time

The Situation

It's the call all security teams dread, "We've been compromised." Now that you know an attacker is in your environment, what's next? What should you do to neutralize an attack before it starts causing harm? Are you prepared to respond and remediate? You know that the longer it takes to resolve the issue, the more damage will be done to your organization. Where should you start? Is there anything you can do to 'stop the bleeding' immediately? You need to act quickly but you also need to make sure you don't overreact and cut access or shut down production systems unnecessarily. It's a fine balance. Once you've provided the first response, you still have to investigate the attack, clean it up, and find a way to ensure that the threat is no longer in your environment.

Driving Concerns

Responding to incidents as fast as possible is crucial to disrupting the attack and preventing extensive damage. Yet, the entire resolution process can take weeks and even months to complete. According to a Ponemon Institute 2014 report, "The average time to contain a cyberattack was 31 days."[1] Here are some of the challenges that make responding to incidents a difficult task.

- **Manual process.** For many security teams, responding to incidents is a manual process, which can cause a rapid incident detection to be impaired by a slow response process. A fully manual response process usually relies heavily on the security team's expertise to identify what needs to be done and in which order of priority. Unfortunately, security teams are a limited resource. Security teams cannot scale easily when incidents spike in volume or complexity, which might happen during an attack. In some situations, the team needs to drop one incident resolution to deal with the next incident. And it's typical that the team will turn to 'surge' resources from other departments for investigation and cleanup, which is not a sustainable solution and adds time to the resolution process.

What resources does your organization utilize in responding to incidents? Select all that apply.

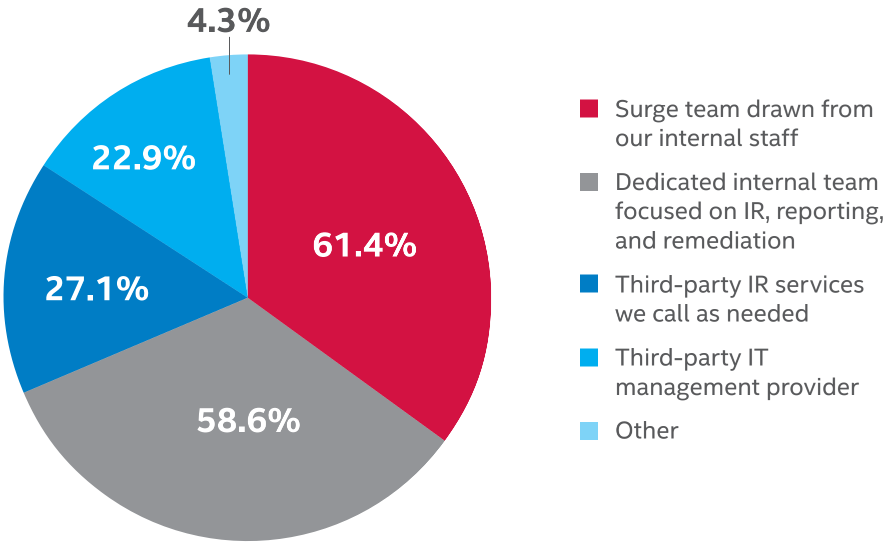


Figure 1. Types of IR Resources Utilized by Organizations. Source: *SANS Incident Response Survey, 2014*

- **Lack of central remediation tools.** Siloed operations make it difficult to respond quickly. Often, you have to reach out to and coordinate with multiple departments to get things done. For instance, you might have to call the network team to ask them to block a specific IP address. Unfortunately, it might take them a couple of hours when the action should be taken immediately.
- **Siloed and disparate data sources.** Having standalone security products makes investigation and forensics slow. If you did not have a log collection solution in place before the breach, collecting the necessary data from multiple sources and trying to make sense of it after the fact will take a very long time. That makes it hard, if not impossible, to answer key questions such as: What happened? What was the attacker's trail? How did they get in? Who got exposed? Has damage already been done (data leaks, account compromise, etc.)? If yes, what's the scope? How long has this been going on? Who has been compromised? Which machine, which user?
- **Balancing fast response with accurate decisions.** The most dreaded thing after being breached is false positives. Those can result in disrupting production systems unnecessarily in the process of mitigating the incident. Security teams need to be sure that the servers they are about to quarantine or the IP address that they are about to block absolutely need to be taken offline. Some will even choose to take a wait-and-see approach rather than making a risky move. That validation process can add to the time to resolution and increase risk.

Solution Description

Intel Security recommends an integrated security framework that allows organizations to prioritize and automate attack response and analysis whenever possible, so you can compress incident response time to a minimum. Once the initial responses have taken place, the solution should allow the response team to investigate quickly so they can start the in-depth remediation as early as possible. And finally, the solution should learn from the attack, so the experience makes the approach faster and more efficient at responding to the next wave of attacks. In summary, the proposed framework should enable security teams to move quickly through the following response process: automating containment, investigating as fast as possible, quickly and confidently remediating compromised systems, and learning from that encounter.

1. **Orchestrate immediate response.** Ideally, you should be able to respond instantly to the detection of a targeted attack (described in the related Detect blueprint). Just like antivirus software blocks and deletes malware as soon as it detects it, the solution should act on your behalf to initiate responses that limit or eliminate the attacker's foothold in your environment. For example, the solution should isolate patient zero for you, block communications to the attacker, or temporarily enforce stronger security policies on systems at risk.

   Of course, the solution should have enough intelligence to determine for you who patient zero is, which IP addresses belong to the attacker, and which systems are at risk, saving you hours of manual analysis. Any immediate, automated response can stop an attack in progress within seconds. In order to confidently automate, the solution needs to take advantage of integration with and between security countermeasures. It needs to be configurable on predefined conditions and it needs to allow for granular and risk-based response, so the right balance of acting versus certainty is achieved.
2. **Investigate quickly.** Once you have responded urgently, you can investigate the incident in depth. Investigating means answering questions such as: What is the extent of the breach? How did it happen? Who has been affected?

   Easy access to the right information is the key to fast and thorough investigation. This is why the solution should give you the ability to easily manipulate the data, to look into the past to uncover what happened and how it happened, and to identify root causes. The solution also needs to provide full context so you can quickly answer questions such as: Who was impacted? When were they impacted? How were they impacted? Are the impacted systems critical to the business, and are the impacted users high-profile users, such as executives?

In addition, the solution needs to gather pertinent threat intelligence from all available sources—from third parties such as external threat intelligence feeds, or from internal sources such as a sandbox. Either way, it needs to include indicators of compromise (IoCs), hash values of newly detected malicious files, lists of malicious IPs, and so on. The solution should then evaluate the events it has seen and is seeing against that intelligence to make your investigation faster and more accurate. Finally, the data, context, and intelligence of the solution should facilitate triage and response by prioritizing the most critical incidents so you can apply your limited resources accordingly

3. **Remediate compromised systems.** Now that you have conducted the investigation and fully understand the attack, you can start the remediation process. The solution needs to give you enough centralized control so you can perform the tasks that are necessary to remediate the incident. Some tasks can be as easy as deleting a few files from a computer and patching vulnerable software, or as complex as having to remotely re-image a system that is beyond salvation. As the mitigation process progresses, you also need to make sure that nothing was missed. This is why the solution also needs to let you proactively search your environment for IoCs. That way, you don't have to wait for the threat to reappear to find it—you can perform preemptive searches.
4. **Learn from the encounter.** Every time you block an attack, it gives the attacker information about you. And they will use that information to refine their attack. To keep up with attackers, you and your security infrastructure also need to learn from these encounters. The solution needs to provide you with actionable information about the attack so you can refine your policies and update your defensive and IT strategies, and immediately block this attack or other similar attacks in the future. Where possible, the findings should be shared between IT and security systems to educate and adapt infrastructure on your behalf.

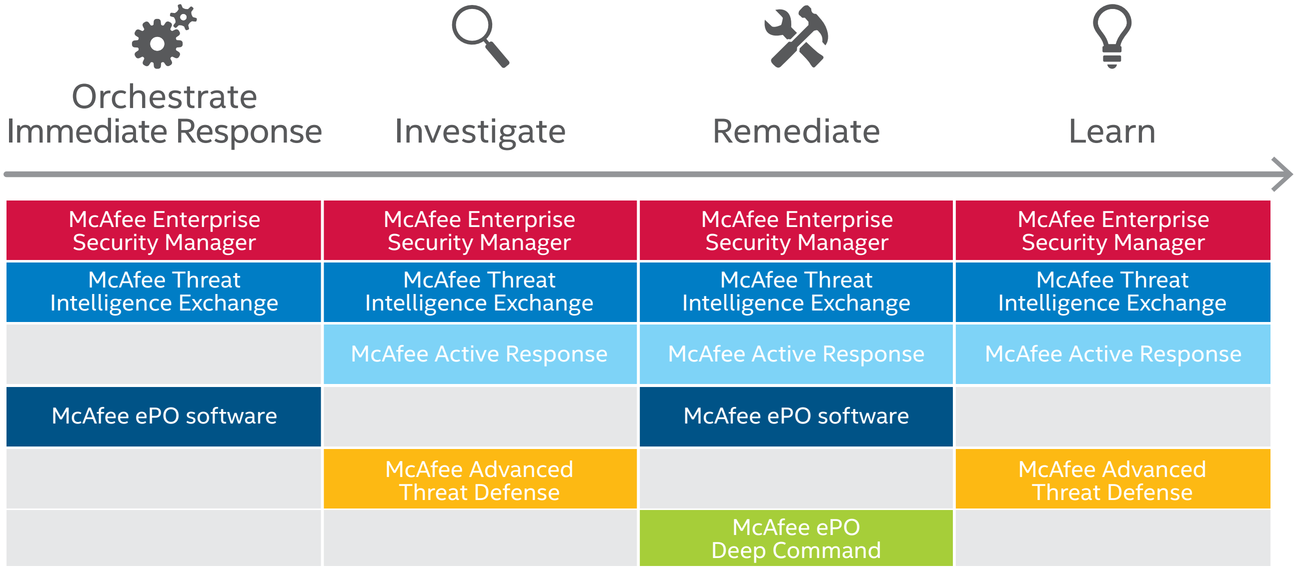
Decision Elements

These factors could influence your architecture:

- What kind of events do you currently collect from your security and other products?
- Do you have a dedicated incident response team in-house or specific staff who perform malware and attack forensics?
- Are the teams responsible for each distinct security solution in different functional silos?

Technologies Used in Our Solution

Intel Security solutions provide the technology that allows you to address each step of the recommended incident response process. These include the McAfee® Enterprise Security Manager, the McAfee Threat Intelligence Exchange, McAfee Active Response, McAfee ePolicy Orchestrator® (McAfee ePO™) software, McAfee ePO Deep Command, and McAfee Advanced Threat Defense. Most of these solutions connect processes and tools, will help at multiple stages (including the Protect and Detect stages of Disrupting Targeted Attacks), and can be used for a wide array of tasks. A few solutions are intended to fulfill a very specific requirement, such as McAfee ePO Deep Command, which is designed to reimage compromised systems deemed beyond repair.



Orchestrate Immediate Response	Investigate	Remediate	Learn
McAfee Enterprise Security Manager	McAfee Enterprise Security Manager	McAfee Enterprise Security Manager	McAfee Enterprise Security Manager
McAfee Threat Intelligence Exchange	McAfee Threat Intelligence Exchange	McAfee Threat Intelligence Exchange	McAfee Threat Intelligence Exchange
	McAfee Active Response	McAfee Active Response	McAfee Active Response
McAfee ePO software		McAfee ePO software	
	McAfee Advanced Threat Defense		McAfee Advanced Threat Defense
		McAfee ePO Deep Command	

Figure 2. Here's how Intel Security solutions fit in the recommended incident-handling workflow.

1. **Orchestrate immediate response.** First, Intel Security solutions have been designed to minimize the impact of an attack without requiring direct human involvement. Our security framework, called Security Connected, helps you automate initial containment. With the Security Connected framework, we can automatically take obvious containment actions, such as quarantining an infected system or blacklisting newly discovered malicious domains, IPs, or URLs. Our Security Connected framework also allows you to respond automatically to zero-day malware. The two main products enabling those capabilities are the McAfee Enterprise Security Manager, our security information and event management (SIEM) platform, and the McAfee Threat Intelligence Exchange.

- **McAfee Enterprise Security Manager delivers centralized automated incident response.** The McAfee Enterprise Security Manager provides actionable integration with other security products such as McAfee ePO software, McAfee Network Security Platform (the McAfee Intrusion Prevention System), and McAfee Threat Intelligence Exchange. The McAfee Enterprise Security Manager collects data from multiple sources, including IoCs from McAfee Advanced Threat Defense, and is able to instruct other products to take corrective actions based on the analysis of the data it receives.

  For example, if Enterprise Security Manager detects an incident where a compromised endpoint is sending malicious traffic on the network, it can tell McAfee ePO software to apply a McAfee Host Intrusion Prevention policy that will quarantine that endpoint. And the policy can be granular enough to allow the endpoint to only communicate with the McAfee ePO server, so you can maintain remote control of the system while ensuring that the endpoint does not cause more damage.

  Another scenario involves the Enterprise Security Manager telling the Intrusion Prevention System to block communication to a specific IP address if it detects that that IP address is malicious and that systems on your network are communicating with it.

  While the McAfee Enterprise Security Manager comes with pre-built connectivity to many Intel Security and third-party technologies and data sources, it also provides an open interface to allow orchestrating action with other technologies from third parties. McAfee Enterprise Security Manager can be configured to execute custom scripts in response to triggers. You can write scripts in any scripting language that is supported on the Scripting Host, and then run scripts on a designated Scripting Host or launch them via SSH.

- **McAfee Threat Intelligence Exchange proactively immunize against emerging threats.** If you are the victim of an advanced targeted attack, chances are good that the attacker will try to use zero-day malware to compromise your systems. McAfee Threat Intelligence Exchange offers an automated response against zero-day threats. If a new malicious file is detected in your environment, that file's reputation can be set to malicious, a reputation change that can block the file's ability to execute on and compromise other hosts, and drive blocking by network and content controls from Intel Security and partners. The malicious file can also be cleaned from the initial victim.

  These interventions can happen automatically thanks to the McAfee Threat Intelligence Exchange integration with McAfee Endpoint Protection, McAfee Advanced Threat Defense, and other Intel Security and partner products. If you prefer, you can manually apply a reputation to that file. To fine-tune what is allowed or blocked in your environment and to match your risk sensitivity, you can override default reputation settings for specific files and certificates. McAfee Threat Intelligence Exchange will then propagate that information through the Data Exchange Layer (DXL) to all of the Threat Intelligence Exchange-enabled countermeasures in the environment, including gateways. The entire process can take place in less than a second. That automatic feedback loop for newly discovered threats allows all of your Threat Intelligence Exchange-enabled security products to instantly respond to new threats.

2. **Investigate quickly.** Now that you have performed the necessary first response to disrupt the attack, you need to investigate the incident in-depth to gain full understanding of the extent, the scope, and the impact of the potential breach. McAfee Enterprise Security Manager accelerates the investigation time by automating part of the analysis for you. McAfee Active Response allows you to search your environment for traces of compromise and McAfee Threat Intelligence Exchange provides you with unique and powerful information to retrace the breach.

- **McAfee Enterprise Security Manager accelerates the analytics and investigation process.** By automating part of the analysis process and by providing the information you need at your fingertips, the McAfee Enterprise Security Manager accelerates the time required to investigate incidents. Its ability to drill-down on incidents, get details of events, pivot the data, and perform historical analysis allows you to quickly access the relevant events that make up and surround an incident. You'll reconstruct the chain of events in a couple of clicks. In addition, McAfee Enterprise Security Manager can add contextual data, such as the geolocation or the criticality of the systems or users involved in an incident. That additional context gives the investigator an edge in understanding the extent and scope of the attack.

  In addition, the BackTrace feature of McAfee Enterprise Security Manager allows you to look back up to 60 days to hunt for IoCs that may have happened in the past. For example, it can reveal internal systems that previously communicated with newly identified malware sources to help you reconstruct an attack. This is a very useful feature when you receive new IoCs, either from third parties or from your integration with McAfee Advanced Threat Defense. BackTrace can ingest those IoCs and let you know if it finds any traces of those attacks in the past.

- **McAfee Active Response investigates in real time.** McAfee Active Response allows you to look in real time for specific attributes on all of your endpoints including indicators of compromise. Such attributes include files dropped on a system, registry keys, and processes running in memory. After running an Active Response scan you can be sure that no attack component is lying dormant. A dormant component is one that has been downloaded, but has not been executed yet, making it virtually undetectable before it's run. Because McAfee Active Response is able to find such components, you can be confident that no artifacts of compromise within the system are left undetected.

- **McAfee Threat Intelligence Exchange identifies impacted systems and 'patient zero.'** McAfee Threat Intelligence Exchange will tell you where and when an unknown or malicious file has run in your environment for the very first time, giving you invaluable information about how the compromise happened in the first place. McAfee Threat Intelligence Exchange can also answer valuable investigation questions such as: Where else has the file run, and when? Has anyone else in the world seen that file before, or was it specifically crafted to attack my environment?

3. **Remediate compromised systems.** Now that you have gained a full understanding of the attack, you can start the remediation process. McAfee ePO software unifies policy and endpoint management to make this process easy. From the McAfee ePO console, you can start an organization-wide clean up.
    - **McAfee ePO software centralizes endpoint remediation.** McAfee ePO software is the centralized policy and management platform used by our endpoint security products as well as many Intel Security partner solutions. In incident response, the software allows the administrators and security team to centrally and remotely act on endpoints. Those actions can be manual or automated, and they can be coupled with other security countermeasures, such as McAfee Enterprise Security Manager, antivirus software, or McAfee Host Intrusion Prevention System, for an even greater range of automated actions. In addition to providing a central point of control, McAfee ePO software provides forensic data to McAfee Enterprise Security Manager by collecting context about the endpoint, such as which user was logged in during the attack, which can be invaluable information during an investigation.
    - **McAfee Threat Intelligence Exchange performs organization-wide cleanup in seconds.** Once you have identified a malicious file, or a file that is too suspicious for your risk level, you can use McAfee Threat Intelligence Exchange to perform an organization-wide cleanup of that file. McAfee Threat Intelligence Exchange enables you to kill a malicious process from memory and delete it from your system the second you've decided that a file should be eradicated. It is as easy as changing the reputation of that file with only one click. As you discover zero-day malware during your investigation, all you need to do is flag the file as known malicious in McAfee Threat Intelligence Exchange and all endpoints will be cleaned.
    - **McAfee ePO Deep Command remotely reimages systems.** In some instances, the security team might recommend reimaging a system, especially if it is easier than attempting to clean the system up or if the system is rendered non-operational after a compromise, for example, if its Master Boot Record has been damaged. It might be the case that the system is remote without physical access to IT support so it would be difficult to physically reimage the machine. But by taking advantage of the Intel® vPro™ Active Management Technology (Intel AMT), McAfee ePO Deep Command allows you to communicate with endpoints at a level beyond the operating system and enable secure remote access to systems that can't even boot, making it possible for you to reimage remote compromised clients.
    - **McAfee Active Response takes action when IoCs are found.** In addition to the real-time endpoint searching used to investigate, McAfee Active Response allows you to take manual or automatic action, such as kill a process or delete a file when it detects an indicator that it is looking for or monitoring. McAfee Active Response allows you to import custom scripts, so you can customize your response to the discovery of IoCs in your environment.
    - **McAfee Enterprise Security Manager takes action across siloed products.** As we've seen, the McAfee Enterprise Security Manager provides actionable integration with other security products. It can orchestrate corrective action when and to the degree you need it to, as your investigation gives you more confidence about the more drastic remediation measures that you need to take. This allows you to take this appropriate action without having to switch consoles.

4. **Learn from the encounter.** Now that you have remediated the incident, it is time to take advantage of the knowledge you've acquired to proactively protect your environment and detect similar types of attacks in the future. McAfee Advanced Threat Defense, McAfee Enterprise Security Manager, and McAfee Active Response can help you use that new knowledge to your advantage.
    - **McAfee Advanced Threat Defense generates local threat intelligence.** Thanks to its ability to perform both a dynamic code analysis (sandboxing) and static code analysis, McAfee Advanced Threat Defense is uniquely able to generate a complete list of IoCs associated with malware that it analyzes. The information includes the name, hash (MD5 or SHA-1), and severity of the convicted file, the system that first detected it, the message that carried it, the source and destination systems, and the source URL if applicable. This gives you precious information for your investigation and offers a unique chance to learn from the attack. Other security solutions such as McAfee Enterprise Security Manager and McAfee Threat Intelligence Exchange can learn from the information generated by McAfee Advanced Threat Defense to increase their knowledge of the attack during response, and it can also be used to refine policies and enforcement to improve each countermeasure's ability to block similar attacks in the future. This is a crucial ability, especially if that malware was specifically created to target your organization with no one else getting a chance to analyze it for you.

- **McAfee Enterprise Security Manager keeps watch for future attacks.** The ability that allows McAfee Enterprise Security Manager to consume IoCs to detect whether an attack has taken place in the past can also be used to ask McAfee Enterprise Security Manager to watch for those indicators in the future. McAfee Enterprise Security Manager can automatically build correlation rules based on those IoCs so that it can alert you or take action, should an attack matching those IoCs take place in the future.

  In addition, McAfee Enterprise Security Manager uses watchlists, which allow it to closely monitor specific groups of users, IP addresses, or other assets that might have been involved in attacks previously. If a new event matches the watch list, the system can either take action automatically, or elevate the event for immediate visibility and response by administrators.

- **McAfee Active Response continuously watches for future attacks.** McAfee Active Response allows security teams to constantly monitor activities that are taking place on the endpoint, such as creation of new files, processes that are running in memory, the creation or modification of registry keys, what drivers are loaded, and much more. The use of triggers and collectors gives McAfee Active Response the unique ability to alert you on any of the parameters it monitors as soon as a system exhibits a behavior, such as attack activities, that you've been watching. For example, if you know that an attack modifies a registry key, or creates a specific file on the targeted system, McAfee Active Response alerts you immediately as soon as that registry key is modified or that file is dropped on another system. McAfee Active Response triggers enable you to continuously monitor critical events or state changes both now and in the future.

- **McAfee Threat Intelligence Exchange shares what you've learned in real time.** The McAfee Threat Intelligence Exchange provides a transport mechanism for sharing what you've learned with your other security products via a communication layer called the Data Exchange Layer (DXL). You can share information such as file and certificate reputations and malware information. McAfee Threat Intelligence Exchange, McAfee Web Gateway, McAfee Intrusion Prevention System, McAfee Advanced Threat Defense, and McAfee Endpoint Protection are all connected through the DXL, and integrated partner products are becoming available. The DXL uses an open communication standard, making it available to any security product that wants to take advantage of the information shared on the DXL.

Optional Integrations

- **McAfee Network Security Platform blocks malicious traffic.** The McAfee Intrusion Prevention System can help accelerate the response time by offering countermeasures on-the-fly when an attack is detected. McAfee Enterprise Security Manager can, for example, instruct the Intrusion Prevention System to block an IP address when it discovers that other infected systems are communicating with that address. McAfee Enterprise Security Manager can also tell the Intrusion Prevention System to enable blocking on certain Intrusion Prevention System signatures that you were only monitoring before the attack was detected.

- **McAfee Host Intrusion Prevention System quarantines an infected endpoint, blocking malicious traffic to and from the endpoint.** The McAfee Host Intrusion Prevention System can help respond immediately to an attack by offering countermeasures on-the-fly when an attack is detected. As with a network Intrusion Prevention System, McAfee Enterprise Security Manager can tell the Host Intrusion Prevention System to drop or block communication with other infected endpoints on the network, or to quarantine the host if it is infected itself.

Impact of the Solution

Every second counts after a breach has been detected. The longer it takes to respond, the more harm is done. Our solution compresses the incident response time to a minimum. It is able to automatically take action, providing crucial first-response abilities within seconds of the detection and allowing you to stop any damage as early as possible. The solution then closes the gap between detection and complete remediation by first enabling the security response team to quickly and accurately understand not only the technical aspect of the breach, but also its scope and extent. This is the most time-consuming activity for incident responders, according to Intel Security research.[2]

Once the investigation is complete, the Intel Security solution includes the tools necessary to fully remediate with efficiency and confidence, driving the remediation time down from weeks to hours. The solution takes it a step further by learning from the encounter, consequently bolstering your defenses, and allowing you to prevent and react even faster to attacks in the future. This integrated and optimized system allows you to gain a substantial advantage against advanced targeted attacks.

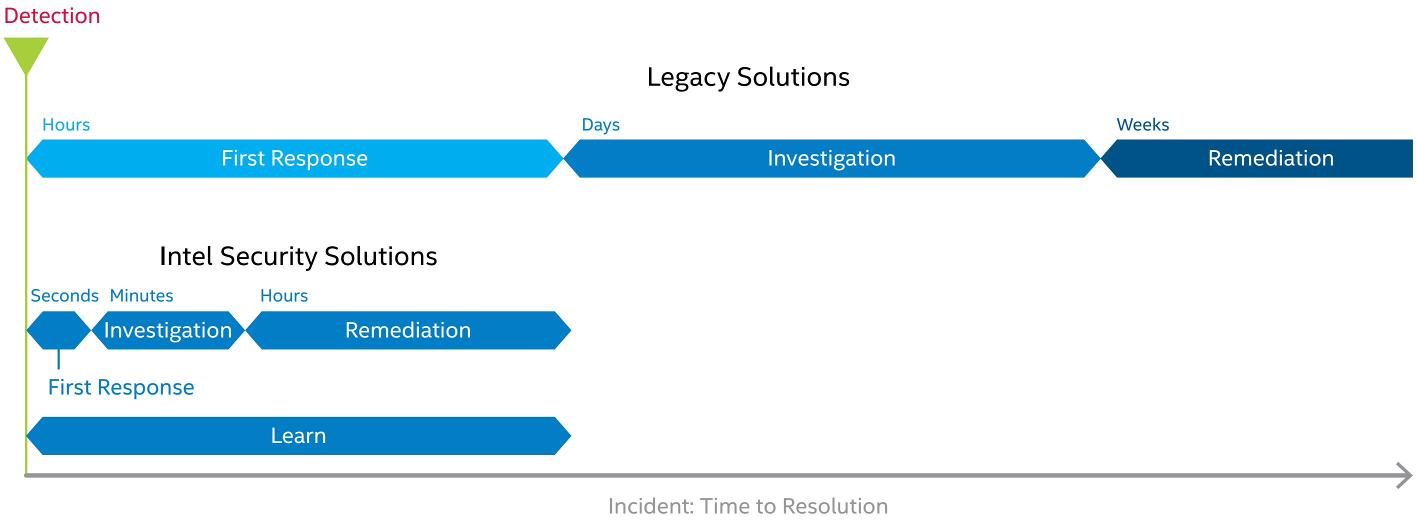


Figure 3. Security Incidents Time To Resolution.

Q&A

I already have forensic tools, why do I need the Intel Security solution?
The Intel Security 'correct' solution does not intend to replace forensic tools. It is meant to shorten the elapsed time between detection and remediation. Investigation of the attack is a part of the entire process and our solution can speed your forensics by quickly letting you know which systems you should get a dump from, for deeper investigation, and to follow appropriate court-ready procedures.

In my organization, the endpoint team does not interact very much with the network team. And neither really talks with security operations. So, they won't share data if it is made available to them.
This is precisely why you need the Security Connected platform. The integration of the technologies together, through McAfee Threat Intelligence Exchange and DXL, will ensure the communication and collaboration between all products that play a part in security, regardless of where that product falls in your environment and the collaboration tools available to the administrators

I don't want to be locked down to a closed and proprietary architecture.
Intel Security products are integrated with products from more than 130 third parties, and we support a range of open standards including STIX/TAXII, IoCs, and RESTful APIs. Our products support open standards wherever reasonable. The DXL framework, for instance, uses an open communication standard.

[1] 2014 Global Report on the Cost of Cyber Crime, Ponemon Institute, October 2014
[2] Research and Analysis by Intel Security and ESG, April 2015, "Tackling Attack Detection and Incident Response"

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com