Active Defense
Overview and Solutions

To understand how Active Defense can help improve security program effectiveness, we need an analogy. Many organizations think of the ideal enterprise network as a castle or fortress: this mental model includes thick stone walls, guard towers and maybe even a moat.

Castles may keep real- world invaders at bay, but we have learned time and again that determined attackers nearly always succeed in penetrating even the most secure networks via targeted attacks.

Security professionals can't rely on the integrity of the network's perimeter and must operate under the assumption that undetected malicious activity is present nearly all the time.

A more appropriate analogy might be the enterprise network as a contemporary city. This analogy works on several levels. Consider the evolving w ay s that we access data. Users have multiple routes into and out of the network through company workstations, personally owned mobile devices, cloud storage and more. This means that legitimate users and intruders both have numerous opportunities to engage in unseen activities.

Just as any city of sufficient size experiences near-constant unpoliced criminal activity, expanding network size and complexity have confounded defenders' ability to monitor in near real-time as well. Indeed, respondents to EY's 2015 GISS that reported experiencing significant incidents revealed that only 4 5 % of detected incidents were discovered by the Security Operations Center (SOC). To maintain order, the castle guards of old evolved into the modern police, and security operations professionals must evolve as w ell.

What does Active Defense add to the existing security operations program?

Let's carry our analogy into the SOC. The security operations team comprises the enterprise's network police force. Security monitoring with network and endpoint tools is akin to sending officers out to enforce speed limits and watch for crime. In the real world, patrol officers are effective at deterring and defeating the criminals that they can actually see. However, they aren't effective at defeating the sophisticated crime that

occurs behind closed doors and in areas that aren't patrolled. For this, the city needs detectives. Rather than patrolling and monitoring, detectives cultivate informants, investigate leads, analyze evidence and actively hunt suspects.

How does Active Defense fit into a holistic cyber security program?

Most security operations teams lack the "detective" capability, and this is w here Active Defense can enhance organizational effectiveness. By employing a deliberate operational cycle to plan, execute, and review intelligence-driven activities to help implement targeted countermeasures, fortify defenses and hunt intruders, Active Defense practitioners provide the organization with the capability to identify and help eradicate latent attackers that circumvent traditional security monitoring and target your intellectual property and business systems.

Active Defense is a deliberately planned and continuously executed campaign to identify and help eradicate hidden attackers and defeat likely threat scenarios targeting your most critical assets

PREPARING AN ACTIVE DEFENSE

What are the prerequisites to establishing an Active Defense Program?

Active Defense results from the fusion of timely threat intelligence with deliberately planned and executed proactive measures that help combat specific threat scenarios. Active Defense does not replace traditional security operations. Instead, it organizes and enhances the existing security operations program. Conducting an Active Defense requires some preparation in order to achieve maximum effectiveness.

What must I understand about my organization to enable Active Defense?

Next, defenders must develop an understanding of what "normal" means f or the network. Typically, this is referred to as a "baseline" in the context of security. However, much of this baseline lives in the minds of the IT staff rather than in security monitoring tools.

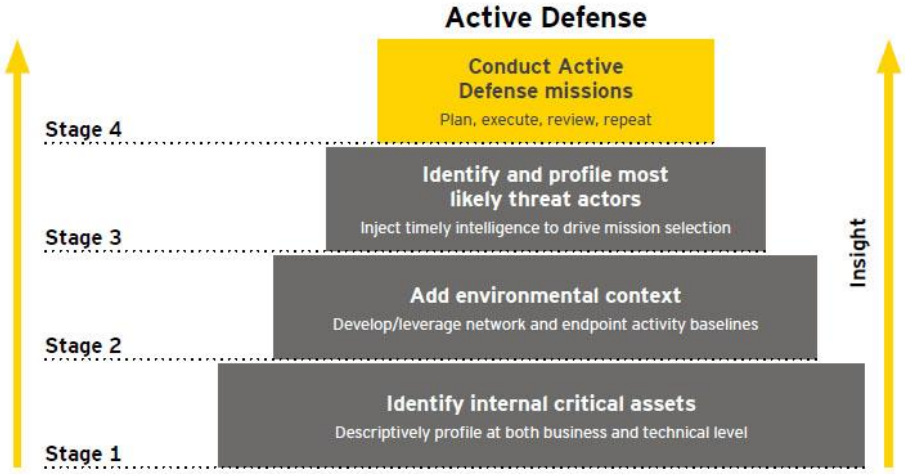
This understanding is important for enhancing the security operations function, because Active Defense includes strong anomaly analysis and hunting components.
Many activities executed by intruders avoid triggering automated security monitoring tools because they don't fit the typical procedures, inputs or models of known attack signatures. Instead, they use compromised credentials or illicit accounts and b lend with regular user behavior.

However, alert and experienced security analysts may recognize malicious activity when they see it, provided they have a model f or normal behavior on the network.

What must I understand about my adversaries for an Active Defense to succeed?

Finally, defenders need an understanding of the threat actors that are likely to target their organization. Many security teams simply assume that they are targeted by the big-three nation state adversaries, organized crime groups and hacktivists. Although this may be true, additional insight is required in order to craft an Active Defense.

Within each group, motivations and capabilities vary widely. Defenders should work closely with threat intelligence providers to paint an accurate portrait of the threat landscape with as much detail as possible. If possible, specific threat actors should be named and analyzed to gain insight that will be leveraged in defensive activities.



Conducting an Active Defense

Active Defense consists of deliberately planned and executed defensive actions called “missions.” Each mission is followed by activities designed to capture lessons learned and enhance organizational learning.

Missions include one or more specific objectives and a defined end-state, and they may last between one day and several weeks. Mission objectives typically include the implementation of one or more targeted Countermeasures to defeat specific threat scenarios or deliberately planned activities to identify hidden intruders (hunting).

Although individual missions may take the form of projects, an Active Defense program is conducted as an iterative operational cycle. Each cycle focuses on defending a specific asset or group of assets from a specific threat actor and may include one or more missions. The operational cycle includes phases for planning, mission execution (of one or more missions) and cycle review. Each mission within the operational cycle also includes analogous phases for planning, execution and review.

What are the components of an Active Defense?

Cyber threat intelligence (CTI) helps lay the groundwork for Active Defense and provides context and guidance during operations. Once likely adversaries have been identified, defenders work with their threat intelligence provider to identify specific tactics via cyber kill chain analysis. Kill chain analysis is the division of the steps taken by an adversary as part of an attack into individual “buckets” that correspond to the links of the kill chain.

Besides known tactics, additional data collected and mapped f or relevant threat actors includes:

- Attacker source IP ranges
- Malware metadata
- Typical hardware or software leveraged by the attacker
- Typical hardware or software targeted by the attacker
- Typical times of attacker operations

For each defended asset, defenders also gather:

- Hardware or software used to access the sensitive data and business processes
- Patch level and patching schedule for identified hardware and software
- Previous attack information
- Detailed identity and access information associated with the resource

This information is supplemented with intelligence about current events in the organization's industry to determine who is attacking peers and for what purpose. Industry peers are a great source to develop first-hand insight about the latest tools, tactics and procedures used by attackers.

What is an Active Defense mission?

A key facet of Active Defense is the enhanced operational focus and effectiveness realized through the deliberate planning of Active Defense missions. Security teams typically harden their defenses on an ad hoc basis, implementing industry best practices when they have time or in reaction to high-profile vulnerability announcements. By contrast, Active Defense missions are planned and executed to proactively defeat specific threat scenarios and uncover hidden intruders in the network. This means that defenders' time is spent deterring and defeating the enterprise's most likely attackers rather than an undefined or nonspecific adversary.

What types of mission can I conduct with Active Defense?

The use of the term "mission" conveys the fact that the operational process proceeds with a significant amount of analytical rigor and discipline in order to achieve maximum effectiveness in accomplishing the organization's security goals. Missions are planned in response to specific threat intelligence in the unique context of the defended organization; and by focusing on the threat to the business from real-world threat scenarios, Active Defense practitioners can maximize their defensive capabilities for their security budget.

Although Active Defense is inherently adversary focused, it is also tailored for specific defended assets — typically the organization's most valuable proprietary data and business systems. An Active Defense mission can include any activities that meet this description. However, we find that a few general categories of activities tend to generate the greatest returns.

Active Defense mission categories

Fortification	Hunting
Network reconnaissance Manual identification and validation of complex vulnerabilities and threat scenarios and development of network situational awareness for decision makers	**Anomaly analysis** Focused investigation for anomalous and malicious activity that cannot be detected by automated security monitoring tools
Targeted countermeasures Leverage insight from the intelligence process to design and implement counter-measures that defeat specific threat scenarios	**Trapping and coercion** Alter network and endpoint conditions to provoke a hidden attacker into engaging in malicious activity liable to be detected by targeted intensive monitoring

FORTIFICATION

The first category of Active Defense mission includes those activities that help improve the enterprise's defenses against specific tactics that may be used by specific attackers.

Network Reconnaissance

Network reconnaissance missions develop the organization's understanding about its own level of risk to specific threat actors or threat scenarios. Missions of this type are generally more complex than straight forward vulnerability scanning and may include mock attacks or red team exercises. An example of an information gathering mission would b e a multi- day experiment to determine whether existing security monitoring tools are able to identify the u se of a particular piece of malware on the network.

Tailored Countermeasures

Tailored countermeasures are most often focused on network and endpoint fortification and attempt to deter, degrade or defeat specific adversary tactics. Active Defense fortification activities differ from hardening activities executed by traditional security operations teams in that they are executed deliberately in response to timely threat intelligence about a threat actor or threat scenario rather than as " industry best practices" on an ad hoc basis.

HUNTING

Hunting missions attempt to discover latent (but active) attackers on the network, or previously unknown evidence of past attacks.

By actively examining seemingly benign activity or artifacts in the context of know n tactics and techniques of particular threat actors or in the context of specific threat scenarios, Active Defense practitioners take the initiative against attackers and reduce the time that attackers can expect to operate inside the network before being identified and eradicated. Hunting missions fall generally into two categories.

Anomaly Analysis

These missions examine artifacts located on particular hosts along with patterns of network traffic to identify malicious activity that automated security monitoring tools miss. Although the organization may have a sophisticated and comprehensive deployment of sensors to conduct security monitoring for network segments and endpoints, there are many forms of malicious activity that thwart automated detection but are plainly obvious to human analysts.

Trapping and Coercion

These missions attempt to compel latent attackers to perform activities that will cause them to be discovered. Once an attacker gains access to the network, escalated privileges and established persistence, they are unlikely to engage in additional overt malicious activity. This is because they likely have gained access to legitimate account credentials or have had the opportunity to install malicious software to mask, clean or hide their activities. By altering conditions on the network, defenders can impose a dilemma on hidden attackers.

They must either work to maintain their access and subject themselves to the scrutiny of alert Active Defense practitioners, or they will lose access. Here are examples of this type of mission:

- **Malware starvation**
  Many types of malware emit a regular " beacon" or " heartbeat" to a command and control (C&C) server as long as they are active. This serves two purposes. First, it acts as a remote notification to an attacker that his access to the network is still available. Second, it provides automated control systems with an opportunity to deliver orders to fielded malware instances (implants).

- **DNS Manipulation**
  Malware authors typically use hostnames to configure malware C&C servers rather than IP addresses. This improves resiliency for the malware, since defenders typically block outgoing traffic to specific IP addresses (routers and switches don't know about hostnames). Using a hostname allows the malware's C&C server to be located at any IP address. The attacker just needs to register it, and DNS servers around the world will carry the news to his deployed malware. Defenders who have tried to squash a malware infection have probably seen this behavior before: they block outgoing traffic from beaconing malware only to see it shift to new destination addresses every few hours.

Is Active Defense right for me?

The Sage Group considers the ability to mount an effective Active Defense as a strategic end-state for the enterprise security program, and the journey to establishing an effective Active Defense varies for every organization. According to several surveys, 47% of respondents reported that their organization does not currently have an SOC; of those that do, 26% outsource real-time security monitoring, and only 12% reported being able to fulfill all functions in-house.

Is my organization ready to implement an Active Defense?

The Sage Group's cybersecurity offerings help develop the security program with an eye toward establishing an Active Defense. However, if any of the following statements reflect your organization, then Active Defense may be right for you:

- ☐ We have an SOC, but we still aren't finding evidence of advanced attackers.
- ☐ We have an SOC, but we still had a major breach.
- ☐ We have had an SOC for a few years, but we need to evolve beyond static monitoring.
- ☐ We have strong business pressures to defend intellectual property or confidential business information (R&D, M&A, ICS/SCADA, etc.).
- ☐ We have an outsourced SOC, but we don't believe that our most valuable data and systems are truly secure.

How can The Sage Group help me prepare to conduct an Active Defense in the future?

Many organizations can benefit from the enhanced operational discipline and adversary focus inherent to Active Defense. However, effectiveness from an Active Defense program requires appropriate maturity levels in a range of security competencies, including security operations, security monitoring, asset identification and classification, IT operations, threat intelligence, security architecture and others.

By focusing on an Active Defense capability as a strategic goal, decision-makers and security practitioners can engage in meaningful discussion about the steps for organizational improvement that will help realize the benefits described herein.

When this occurs, the benefits of an Active Defense can be:

- For the security operations team, Active Defense helps provide a defined set of improvement activities rationalized by threat intelligence and security analytics; and then connected to achievable objectives. The team builds countermeasures, hunts hidden intruders and bolsters defenses on the basis of real reporting about the behavior of real attackers.
- For decision-makers, Active Defense helps connect resource deployment directly to measures of cyber security program effectiveness. Instead of focusing on performance measures like "Number of patches applied" and "Number of tickets closed," effectiveness can be demonstrated via, for example a decrease in successful targeted attacks or a decrease in the time required to discover and eradicate the attacks that were successful.

What are the Benefits of an Active Defense?

- An agile operational cycle designed to help achieve rapid results and accelerate learning.
- Cyber Threat Intelligence analysis that helps yield new insights about adversaries or the enterprise and generates recommendations.
- Active Defense missions focused on hunting or fortification.
- Active Defense helps enhance but does not replace Security Monitoring and Incident Response.

In Conclusion

An organization's intellectual property and critical business systems have substantial monetary value, and organization leaders expect their security programs to keep the data secure and the attackers out. To this end, the effectiveness of the organization's security operations can be significantly enhanced by an Active Defense guided by deliberate planning, a defined strategic end-state and an adversary focus. By organizing and integrating the organization's existing security operations, Active Defense can help reduce the number of successful targeted attacks and decrease the amount of time that intruders can operate before being ejected from the network.