Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention

All attacks follow certain stages. By observing those stages during an attack progression and then creating immediate protections to block those attack methods, organizations can achieve a level of closed-loop intelligence that can block and protect across this attack kill chain.
Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention

A SANS Analyst Whitepaper

Written by Tony Sager

July 2014

Sponsored by
Palo Alto Networks
Introduction

When it comes to the prevention of advanced threats, what you don’t know can harm you the most. Most security departments have the means to capture known attacks, although a few of these can still occur. What has been historically difficult is stopping unknown attacks—those attacks specifically tailored to get around the latest protections by changing signatures, targets and/or patterns of behavior.

However, all attacks follow certain stages, starting with reconnaissance of the target, delivery of weapons to the target, installation, establishing a command and control (C&C) channel, and accomplishing the mission—which is often the process of exfiltrating data. Each of these stages leaves a trail for intelligent sensors to follow and detect.

By observing the many stages during an attack progression and then creating immediate protections to block those attack methods, organizations can achieve a level of closed-loop intelligence that can block and protect across this attack “kill chain.” The key is to integrate all the stages into a high-speed response platform that can then detect and block such attacks as early as possible in the kill chain.

This paper explains the many steps in the kill chain, along with how to detect unknown attacks by integrating intelligence into sensors and management consoles.
Although adversaries can be very clever and well equipped, they do not perform magic. Like their victims, adversaries are information creators, and that information leaves a trail of evidence that can be used against the adversary—just as adversaries use information collection against their victims.

**Stages of Attack**

A better understanding of adversaries and their tradecraft can allow for the more effective design of defenses, including creating multiple opportunities to identify attackers, disrupt them and increase their risk and uncertainty.

For example, to carry out their misdeeds, adversaries must always follow six basic steps:

1. **Reconnaissance:** Gather information on the target. Initial information gathering can be conducted by studying targets through their public websites, following their employees on social media and using other public information. It also includes technical tactics such as scanning ports for vulnerabilities, services and applications to exploit.

2. **Weaponize the information.** In this second stage, adversaries analyze the data collected on their targets to determine what attack methods to use. Attackers may target specific operating systems, firewalls and other technologies. In addition, they may target specific people within the organization for their phishing and drive-by download attacks onto the endpoints.

3. **Deliver the weapon.** Endpoints, in particular, are the primary means of delivery, whether through drive-by download from a website, a targeted phishing attack or infection through an employee-owned device through a secure VPN. Delivery of the weapon can also occur through a vulnerable application, particularly a web application that can be manipulated through cross-site scripting, form fields tampering and other means.

4. **Install, spread and hide.** It always starts with one infected system, either a DNS server or an infected endpoint. Once a single system is infected, the malicious activity has the potential to spread rapidly. Likely scenarios include privilege escalation, internal scans to find specific applications and servers to steal data from or park data and toolkits on, traffic capture and other means. Once installed, infections hide their existence from security devices through a variety of methods, including tampering with security processes.

5. **Establish a command and control channel.** To communicate and pass data back and forth, attackers set up command and control channels to operate between infected devices and themselves. These channels increasingly use encryption to hide their tracks.

6. **Accomplish the task.** Once in a system, attackers will find unprotected servers on which to park sensitive data and from there send it out of the organization to what is usually another compromised server operating as a “bot” (remotely controlled computer) outside of the organization’s control.
Each of these steps leaves a trail, starting with the initial infection. For example, after the initial infection of a DNS server, attackers use the server to hide command and control traffic and data exfiltration from the network security team. To and from traffic, along with connecting devices and applications, provide a myriad of intelligence on actions that should be blocked. For example, the DNS server should not be communicating with a production server inside the organization. Even if the traffic is encrypted, it should be detected, pulled from the network, deeply inspected (possibly decrypted) and blocked based on the specific machine connections being made or attempted.

The Cyber Kill Chain

As attacks have become more advanced, the notion of a “Cyber Kill Chain®” has become common in security discussions. This approach is based on the premise that attacks have an operational life cycle to gather the information (see Figure 1).

![The Intrusion Kill Chain Model](image)

The better security professionals understand the kill chain life cycle, the more opportunities they have to interrupt, manipulate and even prevent the attack from succeeding.

---

1 Cyber Kill Chain is a registered trademark of Lockheed Martin.


At an “intelligence” level, understanding the attacker’s intentions, targets, capabilities and overall tradecraft should lead to better defenses and defeat advanced threats—preferably by putting in place the defenses to prevent entire classes of problems such as those listed in each stage of the kill chain. The idea is to detect and block the behaviors before they are executed. In reality, sometimes intelligence is gathered by seeing the malware executing, which is usually conducted in a safe sandbox either on premises or in the cloud with a third-party intelligence services provider.

### Table 1. Kill Stages of an Advanced Attack

<table>
<thead>
<tr>
<th>Attack Stage</th>
<th>Malicious Action</th>
<th>Kill Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance and Weaponization</strong></td>
<td>After some initial public information lookups, the attacker scans the network and finds a vulnerable DNS server. The attacker modifies his toolkit to exploit the vulnerability and load botware onto the DNS server, use the DNS traffic to hide its command and control activity and be able to move bots around to other DNS servers as needed.</td>
<td>This is a difficult point at which to create a kill action; however, preventive actions here could go a long way. Inventory of applications and versions, patching and awareness of the patch level would protect against discovery of exploitable vulnerabilities.</td>
</tr>
<tr>
<td><strong>Delivery</strong></td>
<td>The attacker uses a vulnerable UDP port to load the malware, then establishes the communication channel with the master controller.</td>
<td>Intelligence applied with DNS monitoring at this layer would watch for unusual UDP/TCP traffic, along with URL filtering and comparison to known command and control signatures.</td>
</tr>
<tr>
<td><strong>Install and Spread</strong></td>
<td>The DNS server is set up as a launching point for finding hosts that can be infected inside the organization.</td>
<td>Unusual traffic between servers that usually don’t talk to one another is another behavior that intelligent sensors should be able to detect, examine and block.</td>
</tr>
<tr>
<td><strong>Establish Command and Control</strong></td>
<td>Once established, inbound commands are sent to the exploited DNS server, which returns outbound traffic and/or begins identifying other vulnerable devices within the organization to exploit.</td>
<td>All of these actions create changes to the system that show up in logs and traffic reports. Intelligent tools should pick up and report on unusual connections between servers and devices, to-from locations, types of traffic and the ports used. If connections are suspect, tools should capture traffic between the servers for further examination, including decrypting packets and examining contents, when required. Watching for patterns of repeated downloads, uploads or lateral movement of files is one way to detect and kill the attack before sensitive data gets out.</td>
</tr>
<tr>
<td><strong>Task Accomplished: Data Exfiltration</strong></td>
<td>The attacker has control of the target systems and is sending data outside the organization.</td>
<td>Outbound traffic monitoring can catch this last stage of attack. However, criminals have learned to send their data from unsuspecting servers and use low and slow bursts to try and thwart outbound protections. Advanced tools should make determinations on outbound traffic based on traffic type, to-from pathways and other patterns to detect sensitive outbound data in egress traffic.</td>
</tr>
</tbody>
</table>
Security experts can use the “trail” of attack information left by perpetrators for analyzing techniques, targets and other threat activity to intelligently prevent, detect, block or disrupt exploits or attempted attacks. In this challenge, speed or “velocity” of response is paramount. The goal is to design the defensive enterprise to make the loop as tight as possible, so that new security information can be used to quickly tune defenses (preferably automatically) to prevent incidents or contain damage.

The key is integrating new, applicable threat information across the various devices that may be involved in threat detection and prevention—including the IDS/IPS and next-generation firewall on the edge of the network and at strategic network segments, along with endpoint security, SIEM/log management, sandboxing and URL filtering, and other security information aggregation systems.

How security teams achieve this integration varies considerably, according to the 2013 SANS Security Analytics Survey published in October 2013. In it, more than 600 respondents indicated that they use all of these technologies and more to analyze attack data (see Figure 2).

![Figure 2. How Security Teams Analyze Security Data (from 2013 SANS Security Analytics Survey)](image)

---

Figure 2. How Security Teams Analyze Security Data (from 2013 SANS Security Analytics Survey)

---

Those organizations that apply this type of intelligence to their detection and prevention plans use a variety of outside service providers and in-house tools, as shown in Figure 3.

![Pie chart showing automation levels](chart.png)

**Figure 3. Limited Use of Automation (from 2013 SANS Security Analytics Survey)**

When aggregated across all tools and services used, just under 7 percent felt they have “fully” or “highly” automated these functions, while 36 percent said they have no automated processes for applying intelligence to their enterprise response plans and 34 percent have “fairly” automated systems.
Combining Tactical and Strategic Intelligence

The role of cyberdefense must always be considered at two levels in parallel: tactical and strategic.

The tactical view is about immediate action and is usually reactive to an event in the wild or at the doorstep. This tactical information is delivered in the form of bulletins, advisories and threats in progress. Increasingly, tactical information is being collected to detect and stop new threats. Reaction occurs in near real time, either through internal collection and analysis or a third-party intelligence provider. As details of the adversary’s operation are revealed, they must be quickly translated into specific steps to tune defenses and detect, prevent or disrupt the adversary. Managing that security information, along with our asset and vulnerability information to apply patches, is critical for long-term safety of an enterprise’s networks.

The second view is more strategic and usually more focused on protection and improvements in risk posture. Based on an understanding of many incidents and attackers, what can organizations do to redesign and minimize the attack surface of vulnerabilities, so attacks have no way to execute in the first place and attacks of a similar nature cannot execute either? This is where IT security teams must work in conjunction with the vulnerability management team for follow-up and remediation, including workflow.

Tactical and strategic information need to be used together to make systemic improvements in prevention, response and overall risk posture. Once a new threat is detected, the most critical points of knowledge required for response include:

- The threat’s applicability to the existing environment
- Those vulnerabilities within the environment that the threat can target and exploit
- The ability to correlate the attacker’s actions against the threat target and prevent attacker action along the attack chain
- Combining this information with intelligence from the enterprise’s own security collection systems—as well as from third-party resources—to prevent events anywhere along the attack kill chain
Consider the Targets

Viewing the attacker as a participant at various locations on the enterprise's system provides insight into a wide variety of information to better understand and detect the attacker's actions. These locations include:

- **At the endpoint.** This is usually the first stage of infection, particularly individual user endpoints that are hit by drive-by downloads from infected websites, phished credentials and so on. Stopping attacks here makes the most sense. If the phish can be detected and the user action blocked, for example, little or no cost is associated with the attack. However, many of these exploits pass through undetected until the endpoint is impacted in a larger attack.

- **On the network.** Command and control traffic, as well as exfiltrated data, can be traveling in packets that attempt to beat monitoring systems by traveling low and slow or using common encryption. Detecting and observing a command and control channel would be helpful in blocking the attack from finishing up its commands, as well as for observing the attackers' behavior to discover their targets, methods and point of origin. This intelligence is useful for preventing future attacks, for example.

- **Target-rich applications.** To spread malware quickly and pick up sensitive information, attackers and malware look for rich applications. Of particular interest are:
  - DNS servers, which are a common starting point for attackers looking to quickly spread malware
  - Databases, which store sensitive information
  - Email servers, which can be exploited to target phishing emails

- **Operational infrastructure.** Many of the common operational subsystems in the enterprise (trouble ticketing and software license tracking, for example) can also contain information that can be correlated with adversary action.

Traditionally, each of these potential sources appears in a separate information “silo,” separated by tool, function, user and format, with security teams trying to sift through this information on a silo-by-silo basis. Automated processes need to be able to integrate across these systems to detect and accept new intelligence for actionable response.
Information to Close the Loop

In military terms, the Observe, Orient, Decide, Act (OODA) loop is a well-known and classic way of framing the action–reaction challenge in a military context. The classic cyberdefense OODA loop is the vulnerability discovery–patch distribution–patch installation loop, which is a key factor in prevention. In this specific information-action loop, the attacker unfortunately has the natural advantages of both speed and focus (see Figure 4).

Figure 4. OODA loop with attacker’s activities inside (shown in lighter green) and the defender’s activities outside (shown in darker green)

---

5 https://en.wikipedia.org/wiki/OODA_loop
In today’s world of advanced attacks, simply noting a threat and creating a patch is time-consuming and leaves systems at risk until a patch can be created and tested. So in addition to vulnerability remediation, today’s “detect, protect and response” loop must begin and end with a means to translate newly gathered intelligence into useful, actionable information. That means this loop should also include:

- **Applicability analysis.** Is the identified anomaly a threat, or is it aimed at a system that is not even in operation at the location of the attack?

- **Prevention of attacks in progress.** Patching is a slow process, and when new attacks are aimed at unpatched vulnerabilities, blocking the attack attempt is the only other preventive measure security teams can take.

- **Prevention of future iterations.** The blocking action created should apply to future iterations of the same type of exploit patterns detected in the initial attempt.

- **Information sharing.** Once new attack methodology is detected and observed, it is critical to share the information so others can also block the attacks with the updated information.

To close this loop, the enterprise must extend its information reach, normally by using vendors and information-sharing partners in order to observe anomalies and orient defense earlier in time and by learning from attacks others have experienced. With the intelligence gathered by the enterprise’s systems during attempted events, along with third-party information from vendor partners and other sources, defenders can now develop this adversary model to combat the chain-of-attack steps holistically rather than in silos.
Prevent, Detect Threats Faster

To successfully turn these information loops to the defender’s advantage, security intelligence must extend beyond the physical and logical boundaries of the defender’s enterprise. Think of this as learning about the adversary from farther in space (by seeing exploits happening to others) and earlier in time (by seeing exploits before they happen, perhaps during development, testing or reconnaissance).

Typically, security teams do this in two ways: (1) through using vendor products and services and (2) by creating and using information-sharing partnerships. The first option is mostly implicit through the use of products and services from vendors who have a natural broad view through support of their user base. When some new form of threat code attempts actions on an enterprise, the product or service vendor monitors the customer network and sandboxes the activity until it determines what is occurring and whether or not it is a new malicious sample. This allows the enterprise defender to benefit from a vastly greater information reach than it can develop on its own, and it also draws resources and expertise that IT groups may not be able to access.

A second approach—creating and using information-sharing partnerships to quickly learn from others—is now coalescing with the first approach in which products and services vendors support the sharing of information. These partnerships can be driven by sectors of industry, geographic location, or vertical and business relationships. The partnerships can range from very informal to structured and government-sponsored approaches, and can encompass commercial models that provide these intelligence services to clients in the cloud. These activities tend to start from a human-centric approach, emphasizing the creation of a trusted community of enterprises with a common interest.

Any new intelligence applied to prevention models must be derived from an understanding of the adversary. The goal is to cost-effectively design systems for the optimal mix of prevention, detection and response. Understanding and modeling the life cycle of the adversary allows the identification of the types of actions the adversary takes and the information she needs to be successful, while tuning the enterprise’s systems to block that sequence of actions in the future.
The Integration Challenge

The real challenge for most security teams will be that of integration. Even if they get the information design right and have access to this wide variety of content—delivered in a highly automated fashion, with appropriate defensive controls ready to take action—they will still be saddled with the complex problems of massive data sets, analysis, correlation, integration and finding the right needle in the haystack. For the foreseeable future, no amount of automation (while necessary) can replace the good judgment of skilled and well-trained humans to sift through the fog and make sense of what really matters. Bringing that data to the skilled individual will help organizations stretch their resources, prevent incidents in real time and/or contain them faster.

The Essential Role of Automation

The need for much greater automation of cyberdefenses has been a topic for several years. In many enterprises, humans still act as the primary engines for gathering and integrating information from across many sources of data. As a tenet of the Critical Security Controls, automation is key for the collection, sharing, correlation, usability and applicability of intelligence information. However, designing the total workflow of such a system comes with some unique challenges:

- There is a constant churn of new information, both internally and externally generated, that can actually get in the way of true intelligence. Malicious movements can hide among all the "noise."
- Threat intelligence comes with varying levels of "trust" in the source (which can determine how quickly security personnel are willing to act on the information).
- Intelligence must be applicable to the enterprise and its existing applications and vulnerabilities.
- An automated security system must be able to work with and across existing security and operational infrastructure rather than in silos. It must be tied directly to parts of the system that can take action (for example, search, block, delete and reconfigure).

Rapid action requires a high degree of automation and standardization built into security and response systems in order for them to work together intelligently with the right analysis to stop malicious actions before they cause damage.

---

7 www.counciloncybersecurity.org/critical-controls
To achieve the kind of speed and scale required to improve cyberdefense against advanced threats and attacks, security professionals need a greater emphasis on automation to detect unknown attack methods and stop them from taking hold in their organizations. Given the scarcity of analytic talent, most enterprises count on the security vendor community to help them process threat information through secure sandboxing techniques, bring threat and intelligence information together into a human-usable form (for example, in some sort of display or dashboard) and create prevention technologies based on new intelligence on the fly.

These services allow enterprises to focus their in-house resources on understanding their risk environment and key analytic tasks. The use of commercial, commodity solutions will help them gain scale and leverage their operational and risk investments more efficiently.

Enterprises should, of course, be wary of depending on any single vendor to achieve an intelligently connected security program. This need requires that solutions play well together, contribute their information to a holistic view of risk and allow for tuning and customization.

A few enterprises take “a build-your-own approach” due to their unique environments or the sensitivity of their domains. However, the cost of this build-your-own approach is not sustainable without continually updating specialized inputs or analytics and skills.

Either approach requires a market-driven threat intelligence environment that is, to the greatest extent possible, frictionless and as automated as possible.
Tony Sager is the chief technologist and a founding member of the Council on CyberSecurity—an independent, international, nonprofit organization whose mission is to identify, validate and sustain best practices in cybersecurity by people in the application of technology and the use of policy. He leads the development of the Critical Security Controls, a worldwide volunteer consensus activity to find and support technical practices that stop the vast majority of attacks seen today. Tony also serves as the director of the SANS Innovation Center, a subsidiary of The SANS Institute.

Mr. Sager retired from the National Security Agency in June 2012 after 34 years as an information assurance professional. His last job was chief operating officer of the Information Assurance Directorate. Before that he created and led the Vulnerability Analysis and Operations (VAO) Group, which was responsible for some of the National Security Agency’s most important advances in cyberdefense.

SANS would like to thank this paper’s sponsor:

Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Dates</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS San Francisco Winter 2017</td>
<td>San Francisco, CAUS</td>
<td>Nov 27, 2017 - Dec 02, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SIEM &amp; Tactical Analytics Summit &amp; Training</td>
<td>Scottsdale, AZUS</td>
<td>Nov 28, 2017 - Dec 05, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Khobar 2017</td>
<td>Khobar, SA</td>
<td>Dec 02, 2017 - Dec 07, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich December 2017</td>
<td>Munich, DE</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2017</td>
<td>Austin, TXUS</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore 2017</td>
<td>Bangalore, IN</td>
<td>Dec 11, 2017 - Dec 16, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2018</td>
<td>New Orleans, LAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta</td>
<td>San Diego, CAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2018</td>
<td>Amsterdam, NL</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Northern VA Winter - Reston 2018</td>
<td>Reston, VAUS</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai 2018</td>
<td>Dubai, AE</td>
<td>Jan 27, 2018 - Feb 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2018</td>
<td>Las Vegas, NVUS</td>
<td>Jan 28, 2018 - Feb 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2018</td>
<td>Bethesda, MDUS</td>
<td>Jan 29, 2018 - Feb 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2018</td>
<td>Miami, FLUS</td>
<td>Jan 29, 2018 - Feb 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London February 2018</td>
<td>London, GB</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2018</td>
<td>Scottsdale, AZUS</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2018</td>
<td>Bangalore, IN</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Southern California- Anaheim 2018</td>
<td>Anaheim, CAUS</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>San Diego, CAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London November 2017</td>
<td>OnlineGB</td>
<td>Nov 27, 2017 - Dec 02, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>