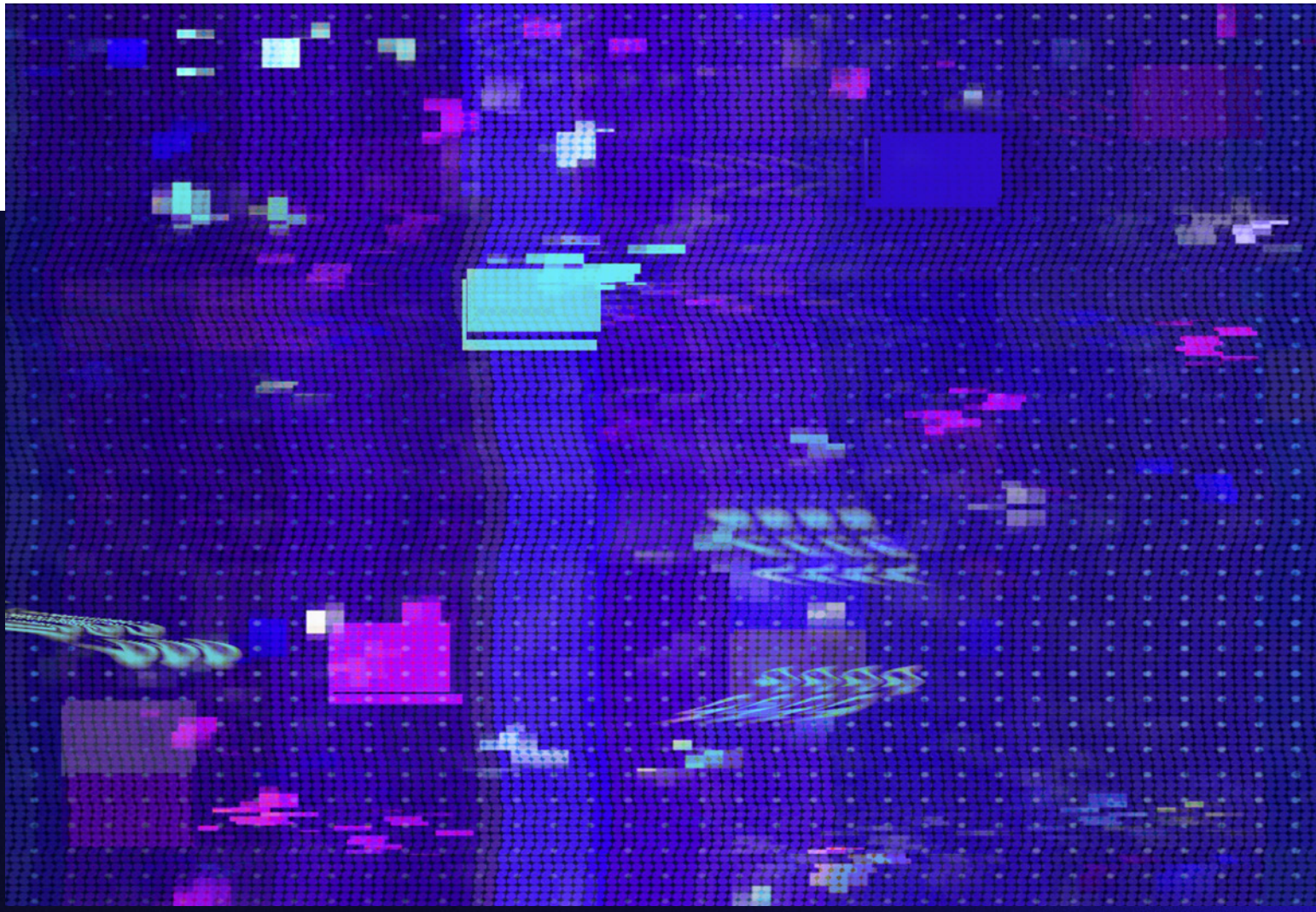
Secureworks®

WHITE PAPER

Find the Weakest Link: 7 Steps of a Cyberattack and Keys to Breaking the Kill Chain

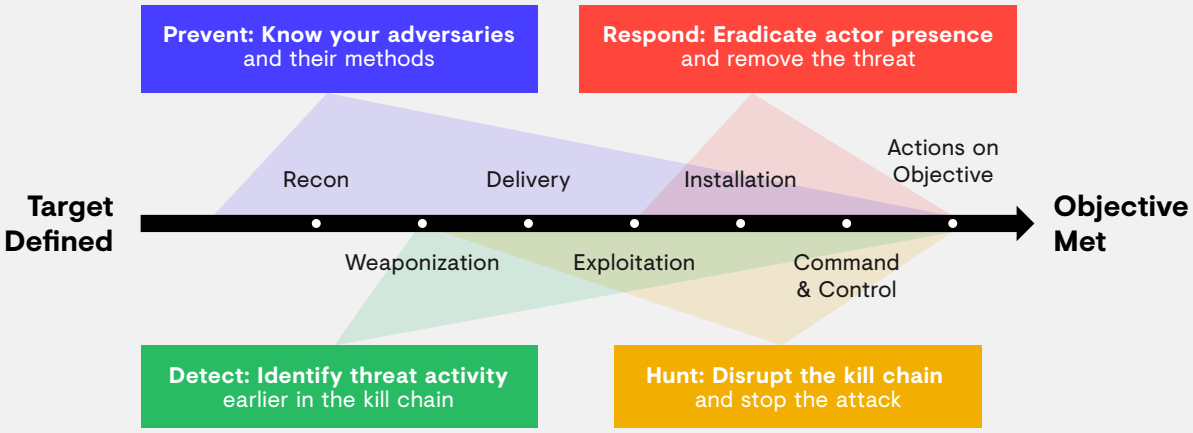
Preventing, Detecting, Hunting,
and Responding to the Advanced Threat



The Kill Chain[1] is the high-level framework or workflow that threat actors employ in their efforts to compromise the target. Disrupting any part of the chain means that the attacker's efforts are thwarted.

Actors behind threats have a toolbox of exploit techniques at their disposal. They often combine several intrusion tools and techniques in order to compromise and maintain access to their target. The key to disrupting the kill chain is breaking it.

The further along the chain that a threat actor gets, the more difficult and expensive it is to defeat them. The key to breaking the kill chain is to hit it as early as possible, because costs begin to rise at an increasing rate as soon as the actor expands beyond the endpoint and into the environment.



Actors behind threats have a toolbox of exploit techniques at their disposal, and often combine several intrusion tools and techniques in order to compromise and maintain access to their target.

Reconnaissance

Reconnaissance defines how the threat group gathers information before and during the computer network operations they engage in. This may be through open source research, scanning the web, the theft of intellectual property, or human sources.

Weaponization

Weaponization describes the "coupling of a remote access Trojan with an exploit into a deliverable payload."[2] This is often done via an automated tool commonly called a "weaponizer," but sometimes referred to as a "builder." These "weaponizer" frameworks are often detectable by artifacts left within the files.

Delivery

This step describes the transmission of the tools into the victim organization. The most common forms of delivery take the forms of scan & exploit, credential-access, spearphish, web-delivery, or physical delivery.

Exploitation

Exploitation describes the methods used to execute the malicious code. This step details whether the adversary uses new 0-days, appears to acquire 0-days and exploits second-hand, or relies upon social engineering to trick users.

Installation

Installation describes the methods and artifacts left behind by the actor while implanting malicious code on compromised systems. These artifacts can include notable aspects of the installation, and unique installation tools.

Command & Control

Command and Control describes the methods used to interact with compromised resources left within the organization. This activity extends beyond communicating with implants to include hosts used to login with collected credentials, as exfiltration end points, and to interact with web shells. Additionally, hands-on-keyboard activity is often performed from different endpoints than the IP addresses used as call back addresses in Remote Administration Tools (RATs). Specific ports, domain names and IP addresses, traffic patterns, and custom protocols used in the interaction with those RATs are all indicators that are descriptive of this stage of the kill chain.

Actions on Objective

After gaining access to the compromised systems, the activity performed by the threat group after a successful intrusion is known as the Actions on Objective stage. The threat group pursues actions to reach their objective, first by collecting information regarding implant, host, account and access status. The group may also collect NTLM hash credentials, payment card information (PCI), stage files to be exfiltrated, delete files or modify physical controls.

Security teams must have full visibility into the operations and security of their systems, networks, and assets.

Keys to Breaking the Kill Chain

Prevent: Know Your Adversaries

Organizations should look to deploy forward intelligence capabilities that provide actionable information on threat actors and their operations.

- Who are they and how do they operate?
- What are their tactics, techniques, and procedures?
- What tradecraft do they use?
- What indicators signal their attack, and at what stage?
- How do you resist them effectively?
- Determine your readiness to resist them.

Detect: Identify Threat Activity Earlier

Security teams must have full visibility into the operations and security of their systems, networks, and assets. Organizations must evaluate their current security architecture and consider recalibrating security policies to ensure that the right information is being collected and correlated to give security professionals a view of the “big picture” across their entire IT ecosystem.

- Are they already here?
- Are we instrumented to detect advanced tradecraft?
- Does telemetry extend across a full attack surface?
- Can we see indicators at all phases of the kill chain?
- How quickly can we determine if it is targeted?

Hunt: Disrupt the Kill Chain

Security leaders must evaluate the capabilities of operations and personnel. Leaders must answer whether their operations are efficient and effective and if not, how they can be improved. This includes assessing the expertise and constraints on that expertise to monitor and address threats in real time.

- Can we detect and block advanced tradecraft?
- Can we limit lateral movement?
- How easily can we adapt internal controls?
- Can we anticipate the adversary's next moves?
- Do we know enough to engage the adversary?
- How quickly can we marshal response forces?

Respond: Eradicate and Remove the Threat

Because there is no "silver bullet," organizations must evaluate their capability to respond effectively to an incident. Security professionals should take an introspective look at their organization to determine if they are adequately prepared to respond to a breach. It is critical your organization has a Cyber Incident Response Plan (CIRP).

- What is the full scope of attacker presence?
- What tradecraft should we sweep for?
- How will the adversary respond?
- Is the CIRP plan tuned for targeted attacks?
- Can we close all the doors at once?
- Are we prepared to prevent re-entry?

Conclusion

To ensure threat actors don't wreak havoc on your systems, you want to break the kill chain as early as possible. A successful break requires knowledge of the adversary, early detection of their activity, hunting that disrupts their movement and access, and full eradication of the threat. To successfully check those boxes you will need full visibility into your IT ecosystem and operations. You must consider current efficiencies and effectiveness, and then determine if you're prepared to respond to any breaches that may occur.

Sources:

[1-2] Lockheed Martin, The Cyber Kill Chain, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States

1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Europe & Middle East

France

8 avenue du Stade de France 93218
Saint Denis Cedex

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom

One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates

Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086

Japan

Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp