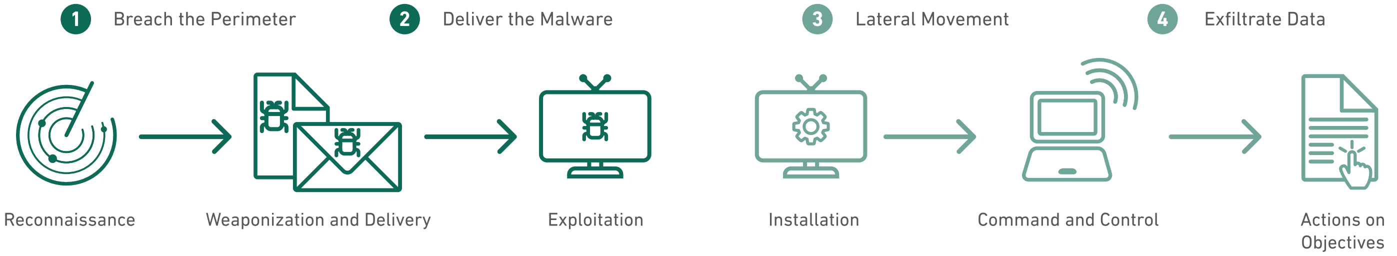
FORTRA

DATASHEET *(Cybersecurity)*

Clearswift and Cyber Kill Chain

The Cyber Kill Chain is a framework developed by Lockheed Martin1 for the identification and prevention of cyberattack activity. The model identifies what adversaries must complete in order to achieve their objective. Interrupt the chain, defeat the attack.


1 Breach the Perimeter
2 Deliver the Malware
3 Lateral Movement
4 Exfiltrate Data
Reconnaissance → Weaponization and Delivery → Exploitation
Installation → Command and Control → Actions on Objectives

Unauthorized Access

Reconnaissance

Research, identification and selection of targets, looking for publically available information on the Internet and specific technologies, with the objective to identify vulnerabilities that can be exploited.

Weaponization

The attacker uses an exploit and creates a malicious payload. Executable files and client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents can serve as the weaponized deliverables.

Delivery

The attacker delivers the malicious payload to the victim by e-mail, web, USB sticks, QR-Code, or other means. It can be the actual file, or a link which the user then clicks on.

Exploitation

Once delivered, the malicious payload is triggered either through a stealth install or through social engineering techniques and interaction with the victim. Exploits, if used, target vulnerable applications or systems within the victim's network.

Unauthorized Access

Installation

Once executed, the payload installs a backdoor on the victim's system allowing persistent access to the attacker. Depending on the profile of the attack, the exfiltration of information (or encryption) can take from days to months so as not to arouse suspicion.

Command and Control

The attacker creates a command and control backdoor communication channel. This ensures the victim's servers' can communicate with the attackers, enabling a persistent "hands on keyboard access" to the target network and assets.

Actions on Objectives

The attacker takes action to achieve their goals, such as data exfiltration, data destruction, and encryption for ransom or infection of another target system or user.

Breaking the Cyber Kill Chain with Clearswift

Breaking the cyber kill chain at any point will defeat the attack. Multi-layer defense should be in place to do this. For most organizations this is from the delivery stage onwards. Clearswift Secure Gateways do just this.

Clearswift Secure Email Gateway (SEG) / Clearswift Secure Exchange Gateway (SXG) / Clearswift ARgon for Email

- Block **Delivery** phase using Advanced Threat Protection features, sanitization of active content and dual anti-malware engines
- Block **data evasion** through email traffic as the result of **Actions on Objectives** phase using Deep Content Inspection features

Clearswift Secure Web Gateway (SWG) / Clearswift Secure ICAP Gateway (SIG)

- Block **Delivery** phase using Advanced Threat Protection features, sanitization of active content and dual anti-malware engines
- Block data evasion through HTTP/HTTPS traffic as the result of **Actions on Objectives** phase using Deep Content Inspection features

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.