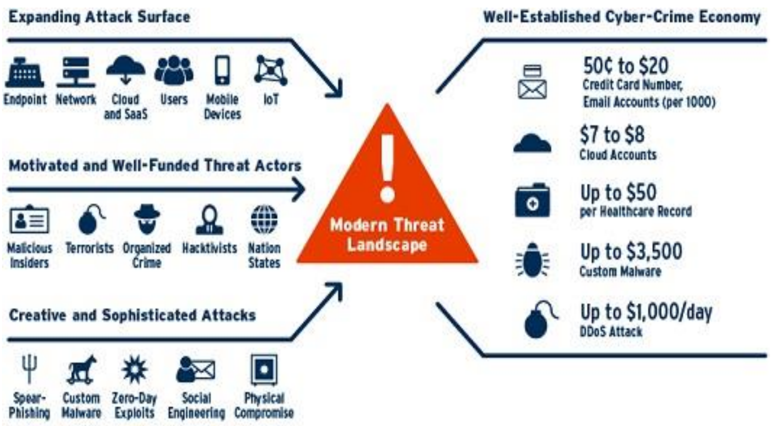
THE SAGE GROUP

Mentoring Solutions for Law Enforcement

“Solutions that Empower your Workforce”

Threat Lifecycle Management Overview and Solutions



The perimeter is gone and your attack surface is rapidly growing thanks to cloud-based applications, mobile technologies, and the Internet of Things (IoT).

In addition, today’s advanced threat actors are circumventing traditional defenses. It’s never been more important to detect and kill threats early in the cyber-attack lifecycle to avoid downstream consequences and costs.

The Cyber Attack Lifecycle

Reconnaissance

The threat actors assess your defenses, and determine how to perform the initial compromise. Whether through spear phishing, zero-day exploit, physical compromise or bribing an employee, they will find a way in.

Initial Compromise

The threat actors bypass your perimeter defenses and gain entry to your network through a compromised system or user account. They can now authenticate within the internal network.

Command & Control

The threat actors put back doors and remote access tools (RATs) in place. They can now stealthily return at any time to continue their mission.

Lateral Movement

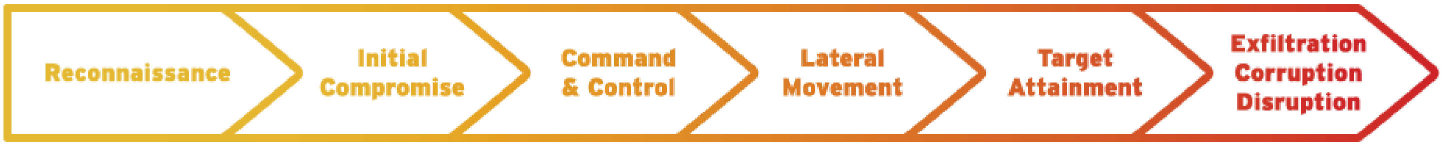
The threat actors scan your internal network, identifying additional targets. They compromise more systems and user accounts. Their access into your environment is now widespread.

Target Attainment

At this stage, the threat actors identify and finally gain access to the systems of interest. They now have all the access they need to realize their objective.

Exfiltration, Corruption and Disruption

This is where cost to your business rises exponentially if the attack is not defeated. The threat actors realize their mission. They might steal intellectual property or other sensitive data, corrupt mission-critical systems, or disrupt the operations of your business. In any case, they have done real damage.



Cyber Attack Lifecycle

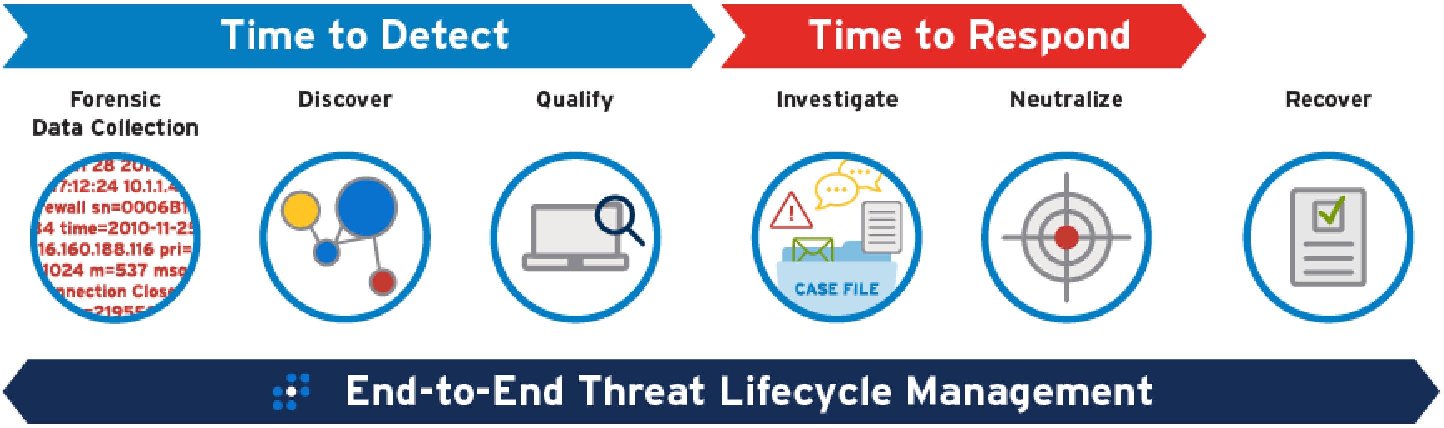
Dramatically Reduce Detection and Response Times

To protect your company from large-scale impact, you need to detect and respond to threats quickly. This requires efficiency of operations and a well-enabled team.

Threat Lifecycle Management

The effectiveness of your security monitoring and response program is largely determined by the efficiency of your workflows. How much visibility does your team have into your environment? How many alarms can they qualify every day? How quickly can they respond to incidents?

Threat Lifecycle Management (TLM) is the key to answering these questions and maximizing your team's security effectiveness. TLM is a series of aligned security operations capabilities. It begins with the ability to "see" across your IT environment and ends with the ability to quickly mitigate and recover from security incidents. The result? Faster detection and response, while keeping staffing levels flat.



Collect

You can’t detect what you can’t see. Create or implement a tool that collects log and machine data from across the enterprise and augments this machine data with critical context. Network and Endpoint Forensic sensors will also provide further visibility across the extended IT environment.

Discover

Plan for and implement a big data analytics approach to ensure no threat goes unnoticed. Setting up Machine analytics to automatically analyze all collected data, detect both routine and advanced threats is also essential. Last, but not least, a powerful search capabilities that enable your team to efficiently hunt for threats and reduce your mean time to detection should be heavily considered.

Qualify

An efficient qualification process allows you to analyze a greater number of alarms with less staff. Implement a risk-based priority score so your team knows where to spend their time. Setting up alarms can also provide immediate access to rich forensic detail displayed in user-friendly analysis tools.

Investigate

It is critical to ensure that qualified threats are fully investigated. Enable collaborative investigations by using an embedded incident response capable tool to automate your routine investigatory task actions. Create Dashboards and live activity feeds to provide real-time visibility into active investigations and incidents.

Neutralize

When an incident is qualified, you must implement mitigations to reduce and eventually eliminate risk to the business. For some threats, such as ransomware or compromised privileged users, every second counts. Use easily accessible and updated incident response processes, coupled with a third party tool, to maximally reduce MTTR.

Recover

Collateral damage often exists after an incident. Threats may lurk in the system or return through a backdoor. Collaborative workflows are needed to bring teams together for rapid recovery. Have an Incident Response tool that provides central access to all required information.