Intelligence Driven Defense using the

LOCKHEED MARTIN CYBER KILL CHAIN™

"The Cyber Kill Chain™ suite of services enables users to better understand how an adversary moves from target observation to a final objective"

- **Recon** – Research, identification, and selection of targets.
- **Weaponize** – Creation of weaponized payload.
- **Delivery** – Transmission of weapon into targeted environment.
- **Exploit** – Upon delivery, exploitation triggers attackers' code on targeted system.
- **Install** – Often a persistent backdoor or other remote access tool is installed.
- **C2** – Targeted and exploited host beacons to attackers for "hands-on-keyboard" access.
- **Actions on Objectives** – Attackers begin collecting, encrypting, and exfiltrating data.

Learn how to apply Lockheed Martin Cyber Kill Chain™ strategies with advanced Cyber Threat Identification courses at the Lockheed Martin Center for Security Analysis (LMCSA)

Every cyber security attack from Recon to Action is a chance to understand more about our adversaries. The Lockheed Martin Cyber Kill Chain™ project enables customers to defend their networks against intruders along each link along the chain of attack.

Intelligence Driven Defense using the LOCKHEED MARTIN CYBER KILL CHAIN™

Cyber Kill Chain™ Service Overview

- The Cyber Kill Chain suite of services was developed to address and defend against the Advanced Persistent Threat (APT).
- The indicator is the key element that enables enterprise defense through each stage of attack. The indicator is essentially a fingerprint left by an adversary or threat somewhere during the process of attack.
- APT actions and indicators are continually evaluated against the chain of attack which propels an intelligence driven defense.
- At each step along the intrusion chain, known indicators and discovered indicators are used to create mitigation strategies.
- These mitigations follow the DoD Information Operations (IO) model of detect, deny, disrupt, degrade, and deceive.
- Use continually gathered and shared intelligence to attribute specific campaigns or threats, each with its own mitigation strategies.

To register for LMCSA courses, email LMIT.TrainingTeam@imc2.ems.lmco.com or call 703-339-6201 x 317.

09/13