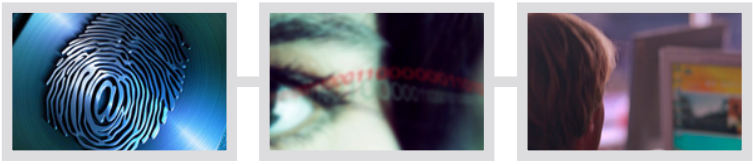


A New Cyber Defense Playbook

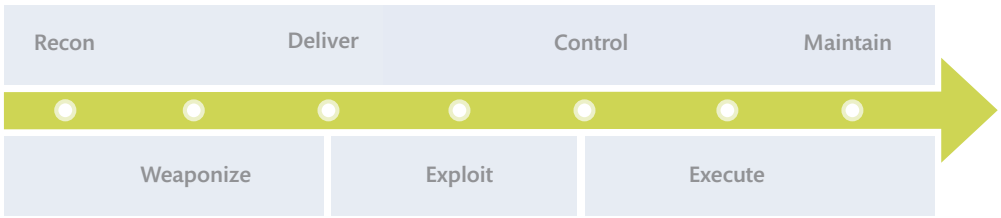
Introduction

The time has come to help unite scattered cyber defenders using a new, improved playbook. Defenders today are isolated, focused on their own narrow defensive zones. The opponent is organized, persistent, and successful, resulting in huge losses in National intellectual property. However, special teams of defenders are working together to share tools, indicators, and experiences that have significantly improved their defenses. A few teams have gone a step further and are getting dramatic results using active defense strategies. Central to all of this is analysis; the purpose is to leverage what we can see from the adversary to predict and detect their next moves.

Introduced in the sections below are tools and practices critical to the progress made so far. The National interest demands that these practices be widely franchised and federated into an enterprise of "extreme collaboration."

Advanced Analysis using the Kill-Chain

The advanced persistent threat (APT) employs a strategy we can divide into stages called the "kill-chain[1]". Defenders can leverage the kill-chain as if it were "game film" to break down and analyze events, but there is a problem; we can only see the second half. However, what has been demonstrated is that careful analysis of that second half can give clues about how the adversary played the first half. Armed with this perspective for the next engagement, defenders have opportunities to anticipate and proactively sidestep threats before a foothold is established.



Analyzing the full attack using the kill-chain framework, defenders have developed new and more effective signatures for malware, anticipated ebbs and flows in attack activity, and identified where seemingly disparate activities actually add up to a coordinated APT campaign.

[1] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Powerful Analytic Techniques and Tools: CRITs

Leveraging the kill-chain analysis requires powerful tools that capture, correlate, and exchange detailed cyber threat information. A prototype of one such tool—CRITs (Collaborative Research Into Threats)—is demonstrating success and being adopted by several cyber threat information exchange communities.

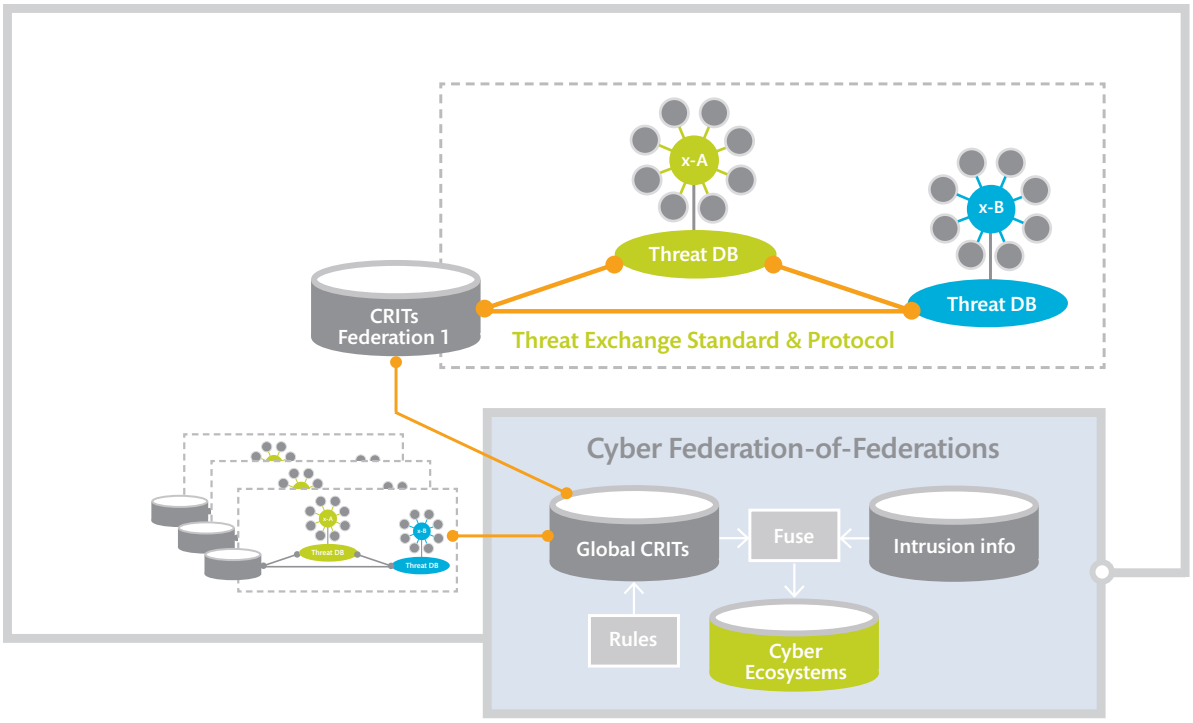
CRITs combines an analytic engine with a cyber threat database that not only serves as the main repository for attack data and malware, but also provides analysts with a powerful platform for conducting malware analyses and correlating malware and for targeting data. These analyses and correlations can also be saved and exploited in CRITS. CRITs employs a simple but very useful hierarchy to structure cyber threat information. At the highest level, a campaign represents a construct that packages together all of the related information about a particular kill-chain-based intrusion into a set of activities. Campaigns consist of intrusion attempts combined with Tactics, Techniques and Procedures (TTPs). An intrusion attempt consists of discrete atomic indicators, email, and file metadata an adversary uses in an attempt to compromise an endpoint. TTPs consist of the targeting, tools, techniques, infrastructure, and kill-chain activities that the adversary uses to conduct a series of related intrusion attempts.

The combined cyber threat information and groupings are designed to act as input to risk models and allow an organization to prioritize defensive actions. To facilitate the trustworthy sharing of cyber threat information among other communities, CRITs enforces fined-grained sharing rules and embeds sharing permissions within the structured threat information it stores and exchanges.

Standards-Based Information Sharing

The ability to share data between organizations is crucial, and to accomplish that broadly requires robust data standards. CRITs is built on existing cyber security standards and protocols (e.g., CVE, CPE, CyBoX, and MAEC[2]) for the secure exchange of cyber threat information. But more is needed. The goal is to operate on and exchange both structured and free-form threat information from multiple sources, using both machine-readable and human-readable formats. Today the standards are not sufficient to share fully; additional work is required to refine existing standards to include new data, data structures, and analytic artifacts so that they can be shared widely and independently of a specific implementation like CRITs.

[2] http://makingsecuritymeasurable.mitre.org



Extreme Collaboration: Cyber Federation

The most promising way forward is an "extreme collaboration," organized, peer-oriented information sharing between entities, at levels of technical detail not yet common today. Combined with the innovations described above, extreme collaboration could provide the Nation with a game changing *cyber defense play book*. We need to supplement the current sharing models. Today's "clearinghouse" style exchanges generally focus on higher level data than proposed here and use a "hub and spoke" style sharing network. Frequently the spokes share detailed data, but the hub filters and abstracts information before dissemination. The envisioned collaboration will require making detailed technical data more directly accessible to all participants.

A Cyber Federation would have a standards-based sharing architecture to exchange techniques, tactics, and tools. Each federation component would consist of an organization (either individual or another federation) that shares cyber threat information.

The Cyber Federation would serve as the trusted intermediary to broker interactions and cyber threat information. Beginning with the tools described, the federation would provide "blueprints" and reference implementations to get sharing underway immediately.

The Cyber Federation would evolve into a national platform of extreme collaboration, where cyber threat information would be exchanged and fused with intrusion information to provide a cyber defense game-changer for the Nation.

MITRE