THE EVOLUTION OF **CYBER SECURITY**

MIKE GORDON

DIRECTOR INTELLIGENCE AND OPERATIONS

LOCKHEED MARTIN CORPORATION

LOCKHEED MARTIN

MIKE **GORDON**

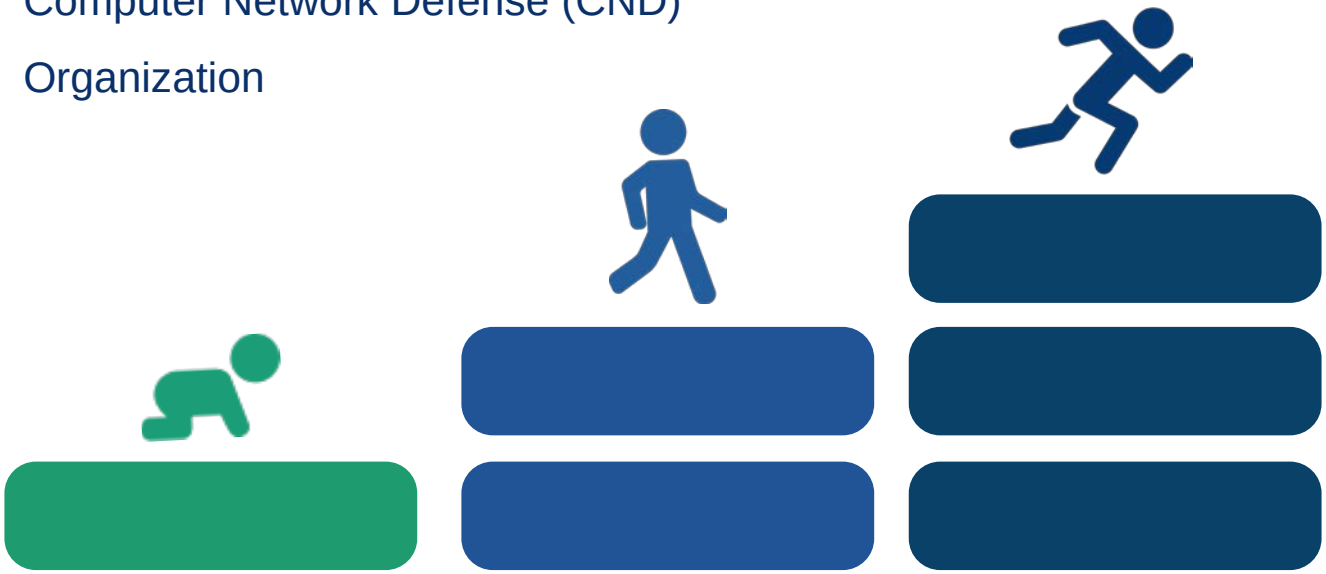
Director of Intelligence and Operations, Lockheed Martin

Responsible for the Overall Computer Network Defense for Lockheed Martin. Affiliated with: Network Security Information Exchange, Defense Security Information Exchange, and DC3 DoD/DIB Collaborative Information Sharing Environment.

CRAWL, WALK, **RUN**

The Evolution of People, Framework and Technology

Lockheed Martin's Transition into a Proactive Computer Network Defense (CND) Organization



THE EVOLUTION OF **CYBER TALENT**

Thought Leaders Drive Innovation

Innovation requires Analytical, Strategic and Leadership Mindset

CONSUMERS

- Computer Analysts
- Ingest Data
- Stove-piped Skills
- Scattered Population

ANALYSTS

- Intel Analysts
- Interpret Information
- Interdisciplinary Skills
- Mission Focused

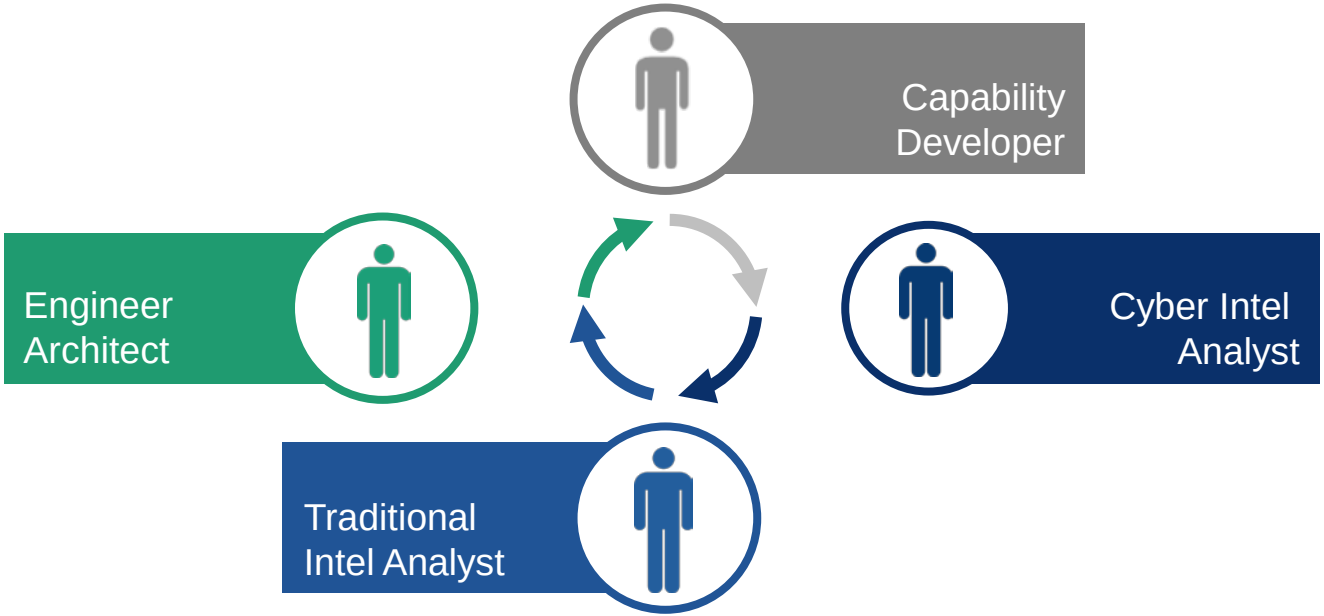
LEADERS

- Thought Leaders
- Teach Domain
- Empowered Workforce
- Part of Corporate Mission

LOCKHEED MARTIN

BUILDING TOP TIER **CYBER TALENT**

Focus on Building Talent with Multidisciplinary Skillsets



THE EVOLUTION OF **CYBER FRAMEWORK**

Intelligence Driven Defense® Key to Protecting the Network

Cyber Kill Chain® Puts The Advantage into the Hands of the Defender

REACTIVE

- One-off Events
- Ignore Motives
- Internalized Information
- Ad-hoc Monitored

PROACTIVE

- Conceptualize Trends
- Interpret Motives
- Promote Sharing
- Adaptive Producer

PREDICTIVE

- Predict Attacks
- Anticipate Actions
- Collaborate Industry-wide
- Mission Integrated

LOCKHEED MARTIN

LOCKHEED MARTIN **CYBER KILL CHAIN®**

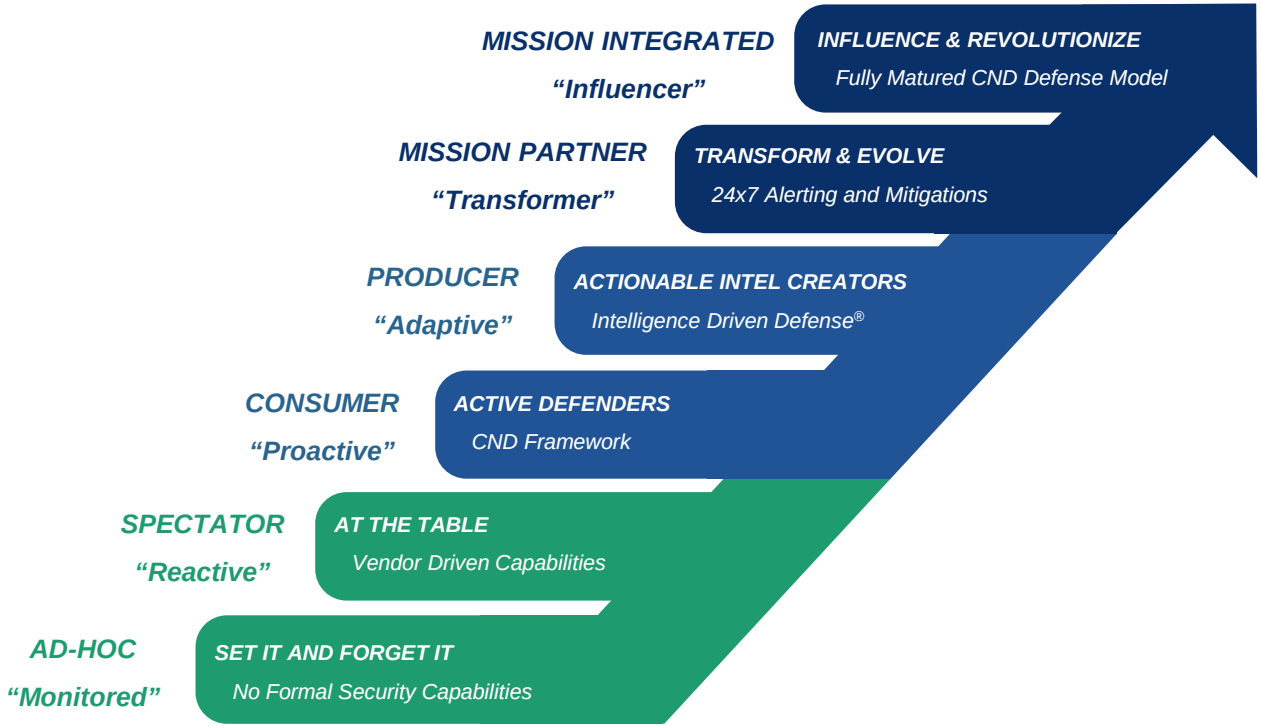
Allows for Proactive Remediation and Mitigation of Advanced Threats

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

LOCKHEED MARTIN

CYBER **MATURITY MODEL**

Additional Levels of Maturity Strengthens Network Security



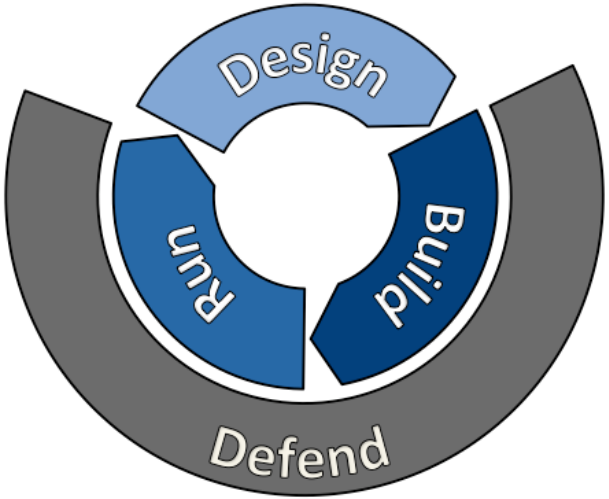
LOCKHEED MARTIN

DESIGNING A SECURE **LIFECYCLE**

Never Conforming to the Norm, Always Driving Innovation

Defendable Architectures

Explicitly designing, implementing, and maintaining systems to support Intelligence Driven Defense®



THE EVOLUTION OF **CYBER CAPABILITIES**

Analytics and Development Skills Blend to Build Mission Focused Technology

Putting Technology to work for Analyst and Analysts to work for Tools

COTS

- Vendor Driven
- Set and Forget
- Externally Reliant Feeds
- Disparate Systems

CUSTOM

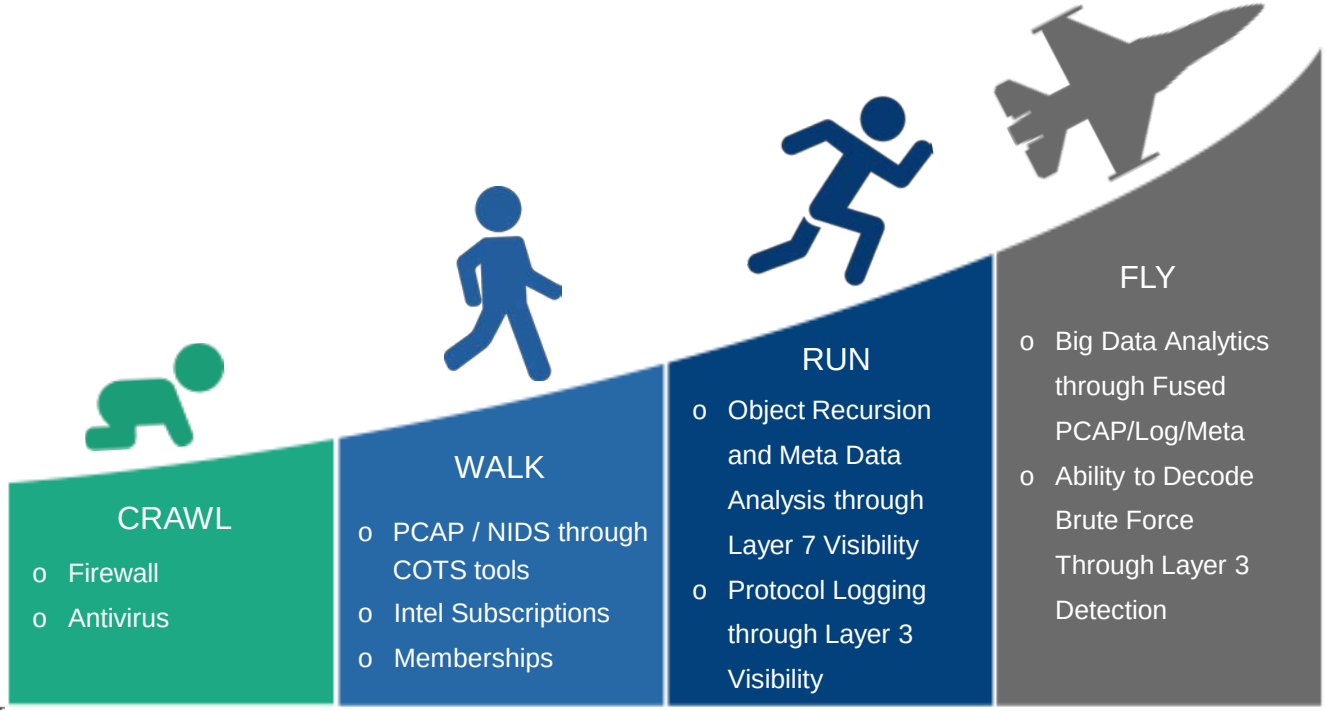
- LM StarVision
- Intel Driven
- Analyst Enabled Platform
- Unified System

AGILE

- Future Analytics
- Rapid Correlation / Mining
- System of Systems
- Fully Integrated PCAP/Log/Meta

THE EVOLVING **CYBER MATURITY**

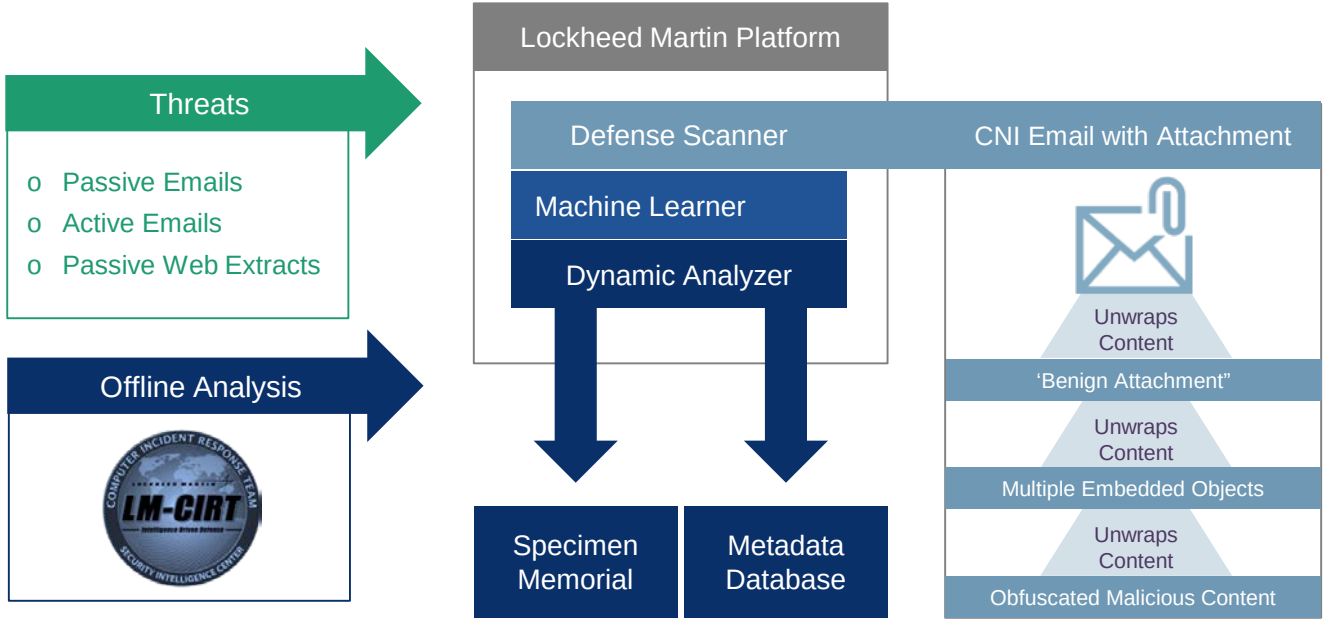
Trending Towards Advanced Visibility and Predictability



LOCKHEED MARTIN

INTEGRATED **DEFENSE PLATFORM**

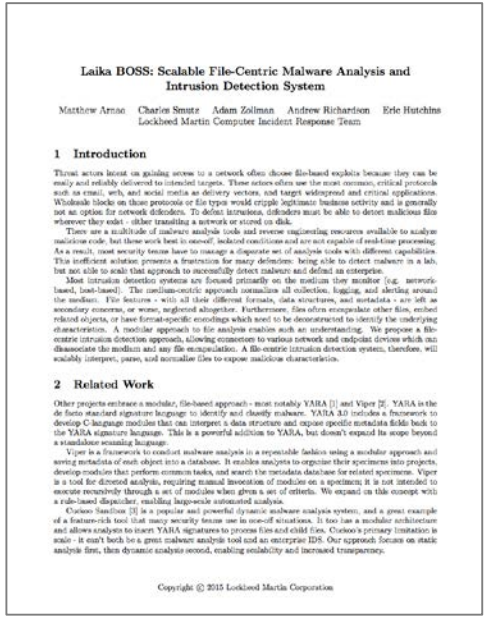
Developing Custom Technology to Increase Visibility



Open Source is Coming Soon

LAIKA BOSS **OPEN SOURCED**

Our Custom Technology, Available to the Masses



Laika BOSS: Scalable File-Centric Malware Analysis and Intrusion Detection System

Matthew Arnao Charles Smutz Adam Zollman Andrew Richardson Eric Hutchins
Lockheed Martin Computer Incident Response Team

1 Introduction

Threat actors intent on gaining access to a network often choose file-based exploits because they can be easily and reliably delivered to intended targets. These actors often use the most common, critical protocols such as email, web, and social media as delivery vectors, and target widespread and critical applications. Wholesale blocks on those protocols or file types would cripple legitimate business activity and is generally not an option for network defenders. To defeat intrusions, defenders must be able to detect malicious files wherever they exist - either transiting a network or stored on disk.

There are a multitude of malware analysis tools and reverse engineering resources available to analyze malicious code, but these work best in oneoff, isolated conditions and are not capable of real-time processing. As a result, most security teams have to manage a disparate set of analysis tools with different capabilities. This inefficient solution presents a frustration for many defenders: being able to detect malware in a lab, but not able to scale that approach to successfully detect malware and defend an enterprise.

Most intrusion detection systems are focused primarily on the medium they monitor (e.g. network-based, host-based). The medium-centric approach normalizes all collection, logging, and alerting around the medium. File features - with all their different formats, data structures, and metadata - are left as secondary concerns, or worse, neglected altogether. Furthermore, files often encapsulate other files, embed related objects, or have format-specific encodings which need to be deconstructed to identify the underlying characteristics. A modular approach to file analysis enables such an understanding. We propose a file-centric intrusion detection approach, allowing connectors to various network and endpoint devices which can disassociate the medium and any file encapsulation. A file-centric intrusion detection system, therefore, will scalably interpret, parse, and normalize files to expose malicious characteristics.

2 Related Work

Other projects embrace a modular, file-based approach - most notably YARA [1] and Viper [2]. YARA is the de facto standard signature language to identify and classify malware. YARA 3.0 includes a framework to develop C-language modules that can interpret a data structure and expose specific metadata fields back to the YARA signature language. This is a powerful addition to YARA, but doesn't expand its scope beyond a standalone scanning language.

Viper is a framework to conduct malware analysis in a repeatable fashion using a modular approach and saving metadata of each object into a database. It enables analysts to organize their specimens into projects, develop modules that perform common tasks, and search the metadata database for related specimens. Viper is a tool for directed analysis, requiring manual invocation of modules on a specimen; it is not intended to execute recursively through a set of modules when given a set of criteria. We expand on this concept with a rule-based dispatcher, enabling large-scale automated analysis.

Cuckoo Sandbox [3] is a popular and powerful dynamic malware analysis system, and a great example of a feature-rich tool that many security teams use in one-off situations. It too has a modular architecture and allows analysts to insert YARA signatures to process files and child files. Cuckoo's primary limitation is scale - it can't both be a great malware analysis tool and an enterprise IDS. Our approach focuses on static analysis first, then dynamic analysis second, enabling scalability and increased transparency.

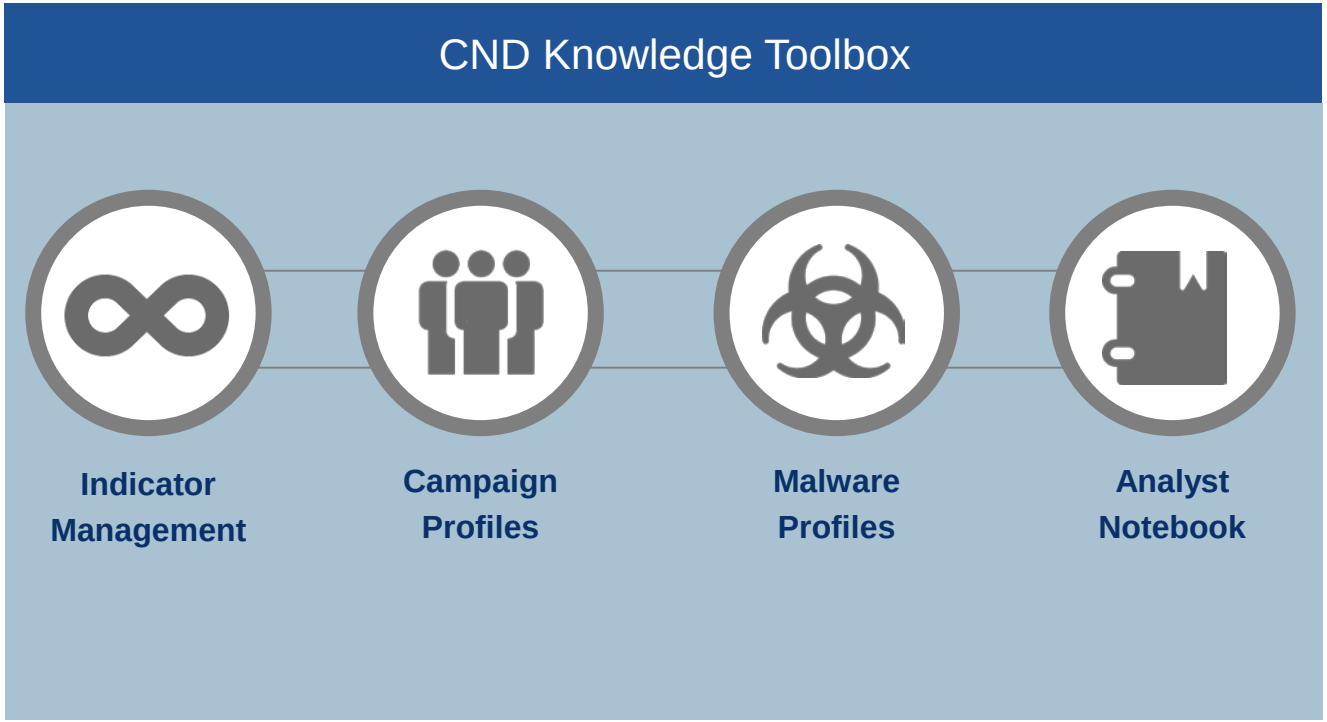
Scalable File-Centric Malware Analysis and Intrusion Detection System to be Open-Sourced Soon.

For Details Visit:

http://lockheedmartin.com/us/what-we-do/information-technology/cyber-security/laika-boss.html

MANAGING **KNOWLEDGE**

Managing Gained Intelligence to Create Actionable Tasks



MEASURING **VISIBILITY**

The Level of Visibility Determines How You See the Problem

Nearsighted

Views Campaigns First-Hand. Closest to the Explosion.

Mid-Range

View Campaigns in Motion. Insight into Internet Surface.

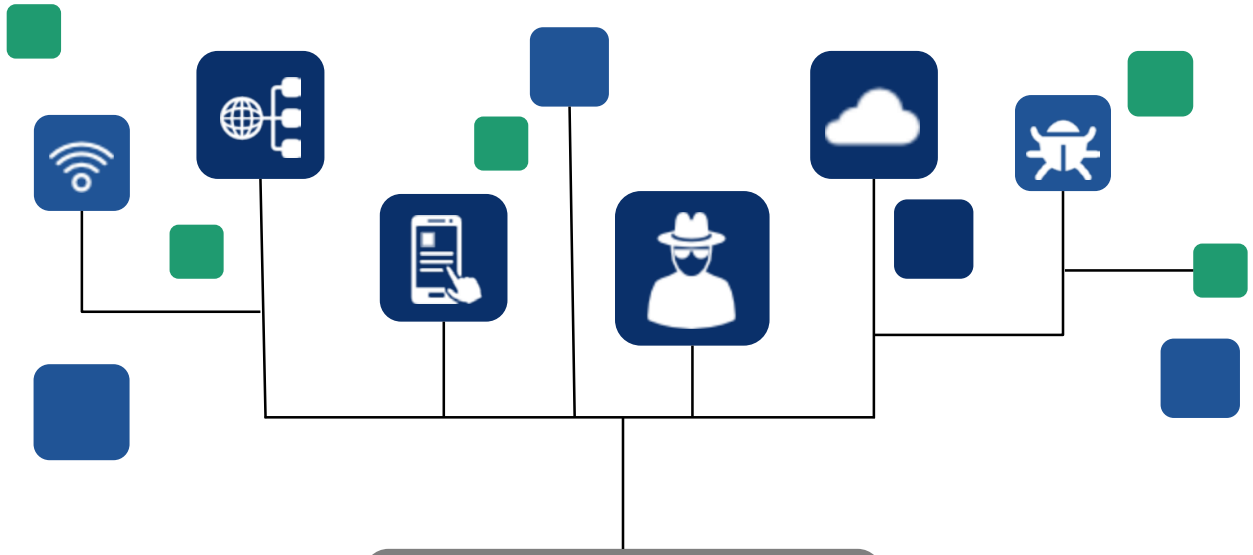
Farsighted

Views Campaigns in Action. Sweep of Internet to Gain Intel.

Perception is a Function of Your Vantage Point

SOLVING THE PUZZLE: **BIG DATA**

Turning Petabytes of Analysis into Discrete Intelligence



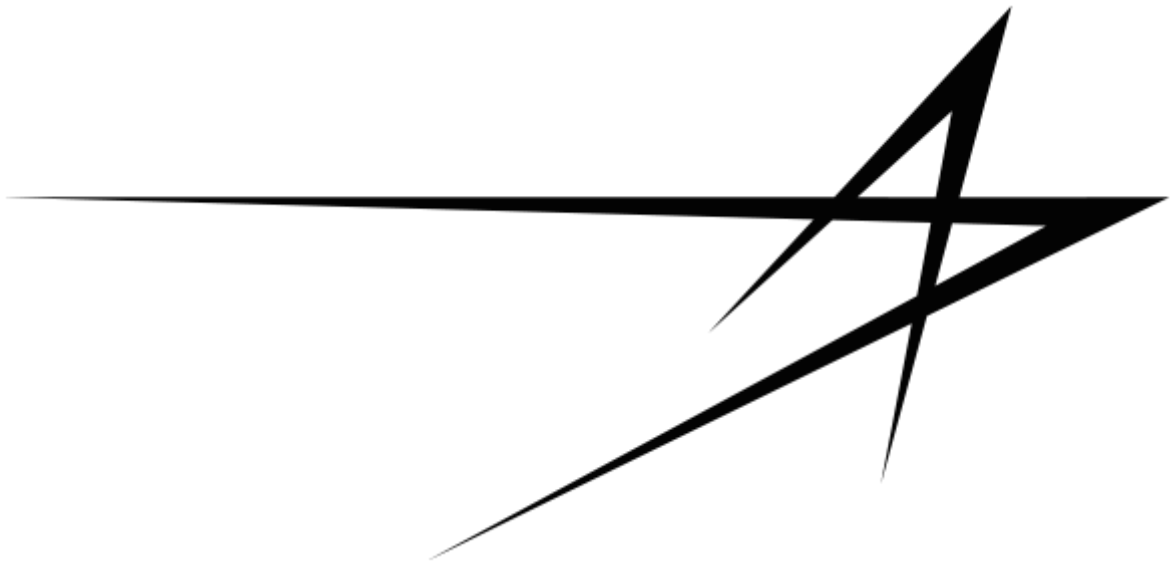
QUESTIONS AND **CLOSING**

People, Framework, and Technology is Key

Building an Empowered, Integrated, and Analytical Workforce to Compliment Intelligent Tools, Capabilities and Countermeasures, Provides Greatest Resilient Posture to Proactively Thwart Adversaries.

Contact: Mike Gordon

Mike.Gordon@lmco.com



Links **CLOSING**

People, Framework, and Technology is Key

Building an Empowered, Integrated, and Analytical Workforce to Compliment Intelligent Tools, Capabilities and Countermeasures, Provides Greatest Resilient Posture to Proactively Thwart Adversaries.

Contact: Mike Gordon

Mike.Gordon@lmco.com