THE EVOLUTION OF CYBER SECURITY

MIKE GORDON
DIRECTOR INTELLIGENCE AND OPERATIONS
LOCKHEED MARTIN CORPORATION
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
BUILDING TOP TIER CYBER TALENT

Focus on Building Talent with Multidisciplinary Skillsets

- Capability Developer
- Engineer Architect
- Cyber Intel Analyst
- Traditional Intel Analyst
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

© 2015 LOCKHEED MARTIN CORPORATION
LOCKHEED MARTIN CYBER KILL CHAIN®

Allows for Proactive Remediation and Mitigation of Advanced Threats

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives

Effectiveness
Prioritize
ROI
Analysis
Measurement
Investment
Escalation
Resiliency
Dialogue
Culture

ROI Prioritize
Analysis Measurement
Investment

© 2015 LOCKHEED MARTIN CORPORATION
Additional Levels of Maturity Strengthens Network Security

- **MISSION INTEGRATED**
  - "Influencer"
  - Fully Matured CND Defense Model

- **MISSION PARTNER**
  - "Transformer"
  - 24x7 Alerting and Mitigations

- **PRODUCER**
  - "Adaptive"
  - Intelligence Driven Defense®

- **CONSUMER**
  - "Proactive"
  - CND Framework

- **SPECTATOR**
  - "Reactive"
  - Vendor Driven Capabilities

- **AD-HOC**
  - "Monitored"
  - No Formal Security Capabilities

- **SET IT AND FORGET IT**
  - No Formal Security Capabilities

- **INFLUENCE & REVOLUTIONIZE**
  - Fully Matured CND Defense Model

- **TRANSFORM & EVOLVE**
  - 24x7 Alerting and Mitigations

- **ACTIONABLE INTEL CREATORS**
  - Intelligence Driven Defense®

- **ACTIVE DEFENDERS**
  - CND Framework

- **AT THE TABLE**
  - Vendor Driven Capabilities

- **MISSION INTEGRATED**
  - "Influencer"
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

© 2015 LOCKHEED MARTIN CORPORATION
THE EVOLVING CYBER MATURITY

Trending Towards Advanced Visibility and Predictability

CRAWL
- Firewall
- Antivirus

WALK
- PCAP / NIDS through COTS tools
- Intel Subscriptions
- Memberships

RUN
- Object Recursion and Meta Data Analysis through Layer 7 Visibility
- Protocol Logging through Layer 3 Visibility

FLY
- Big Data Analytics through Fused PCAP/Log/Meta
- Ability to Decode Brute Force Through Layer 3 Detection

© 2015 LOCKHEED MARTIN CORPORATION
INTEGRATED DEFENSE PLATFORM

Developing Custom Technology to Increase Visibility

Threats
- Passive Emails
- Active Emails
- Passive Web Extracts

Offline Analysis

Lockheed Martin Platform

Defense Scanner
- Machine Learner
- Dynamic Analyzer

CNI Email with Attachment
- Unwraps Content
- "Benign Attachment"
- Unwraps Content
- Multiple Embedded Objects
- Unwraps Content
- Obfuscated Malicious Content

Specimen Memorial

Metadata Database

Open Source is Coming Soon
LAIKA BOSS OPEN SOURCED

Our Custom Technology, Available to the Masses

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

For Details Visit:

MANAGING KNOWLEDGE
Managing Gained Intelligence to Create Actionable Tasks

CND Knowledge Toolbox

- Indicator Management
- Campaign Profiles
- Malware Profiles
- Analyst Notebook
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
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