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.

LOCKHEED MARTIN

CRAWL, WALK, **RUN**

The Evolution of People, Framework and Technology

Lockheed Martin's Transition into a Proactive

Computer Network Defense (CND)

Organization
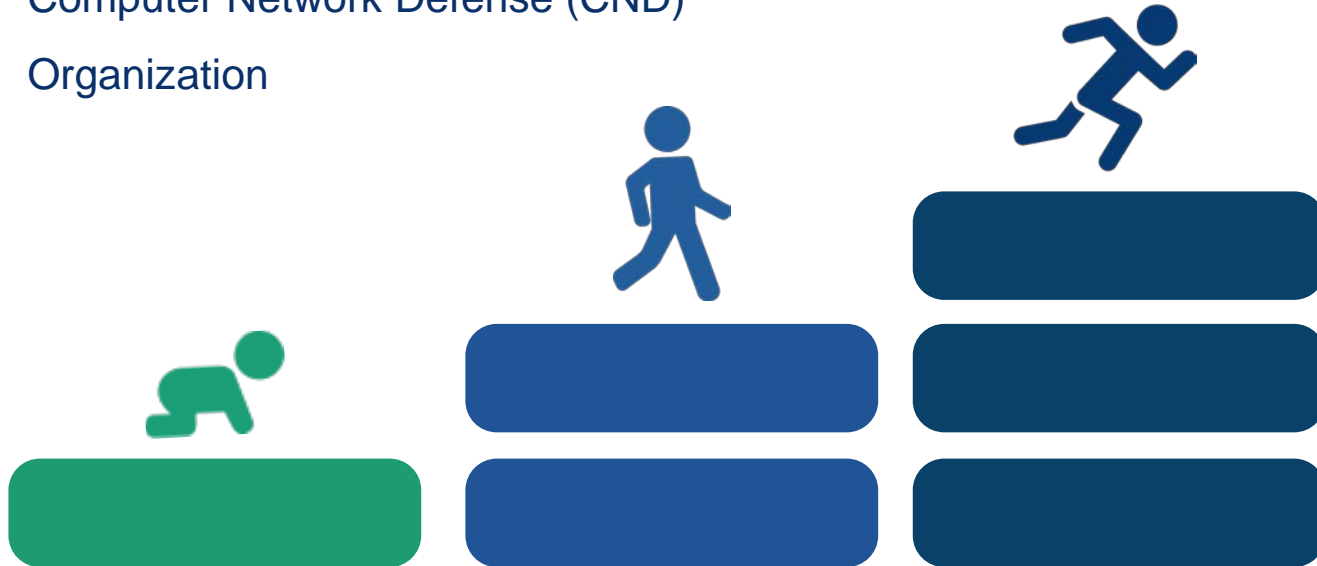
THE EVOLUTION OF **CYBER TALENT**

Thought Leaders Drive Innovation

Innovation requires Analytical, Strategic and Leadership Mindset

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

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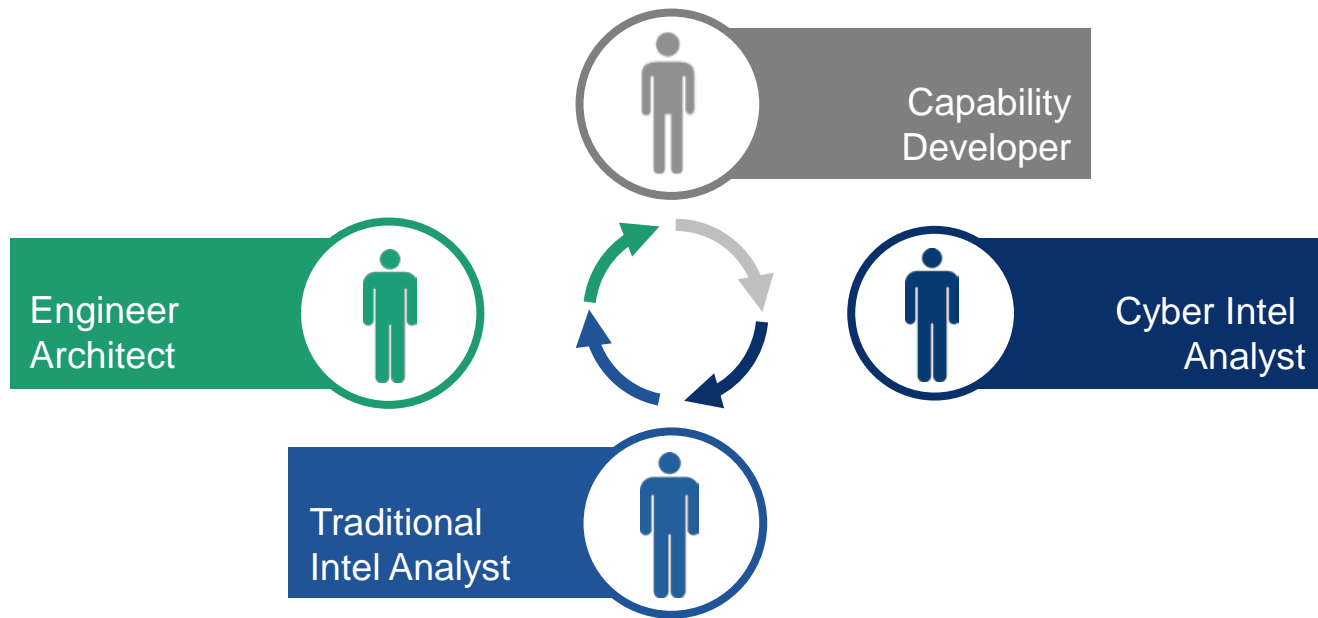- Interpret Information
- Interdisciplinary Skills
- Mission Focused

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

LOCKHEED MARTIN **CYBER KILL CHAIN®**

Allows for Proactive Remediation and Mitigation of Advanced Threats

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

Analysis	ROI	Prioritize
Measurement	Resiliency	Escalation
Investment	Dialogue	Culture

Effectiveness

Priority

CYBER **MATURITY MODEL**

Additional Levels of Maturity Strengthens Network Security

MISSION INTEGRATED
"Influencer"

INFLUENCE & REVOLUTIONIZE
Fully Matured CND Defense Model

MISSION PARTNER
"Transformer"

TRANSFORM & EVOLVE
24x7 Alerting and Mitigations

PRODUCER
"Adaptive"

ACTIONABLE INTEL CREATORS
Intelligence Driven Defense®

CONSUMER
"Proactive"

ACTIVE DEFENDERS
CND Framework

SPECTATOR
"Reactive"

AT THE TABLE
Vendor Driven Capabilities

AD-HOC
"Monitored"

SET IT AND FORGET IT
No Formal Security Capabilities
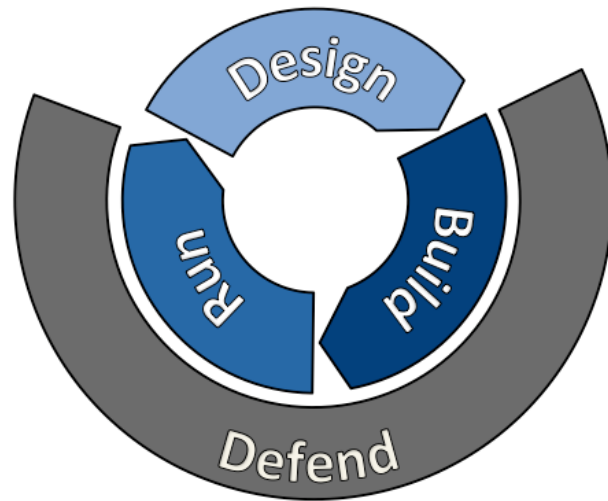
LOCKHEED MARTIN

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®

LOCKHEED MARTIN

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
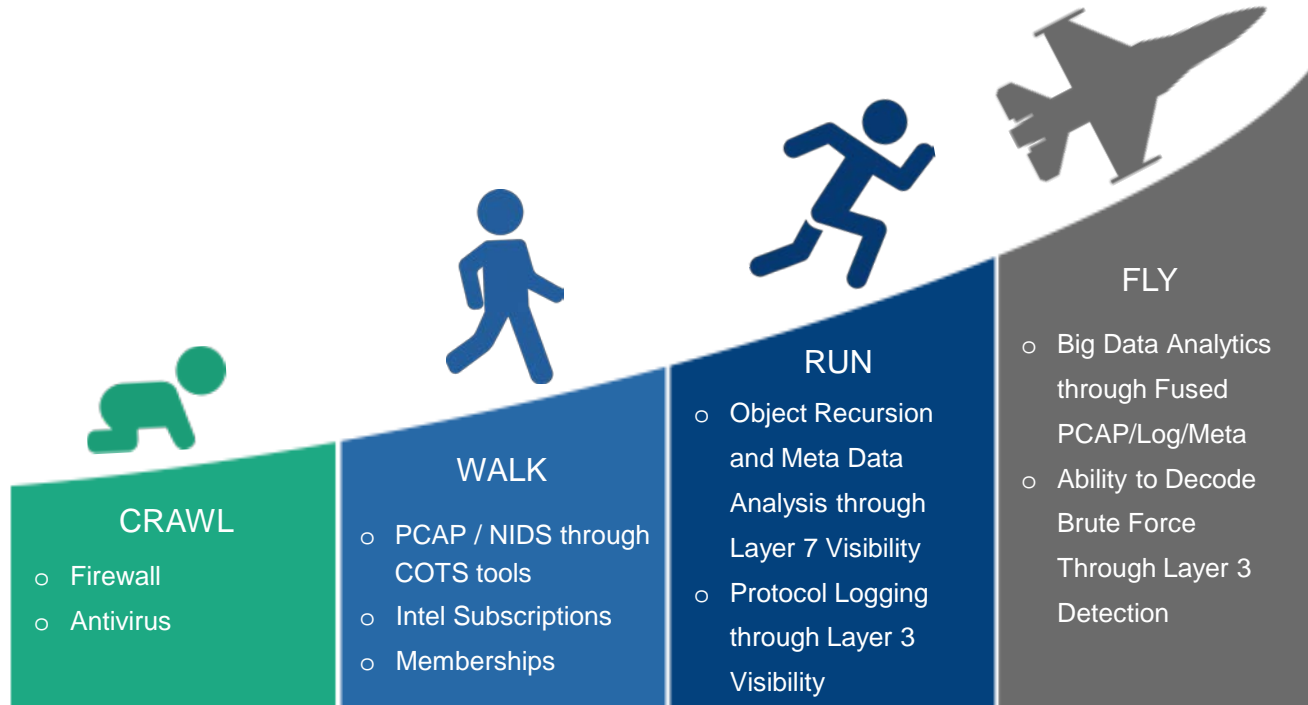- Analyst Enabled Platform
- Unified System

AGILE

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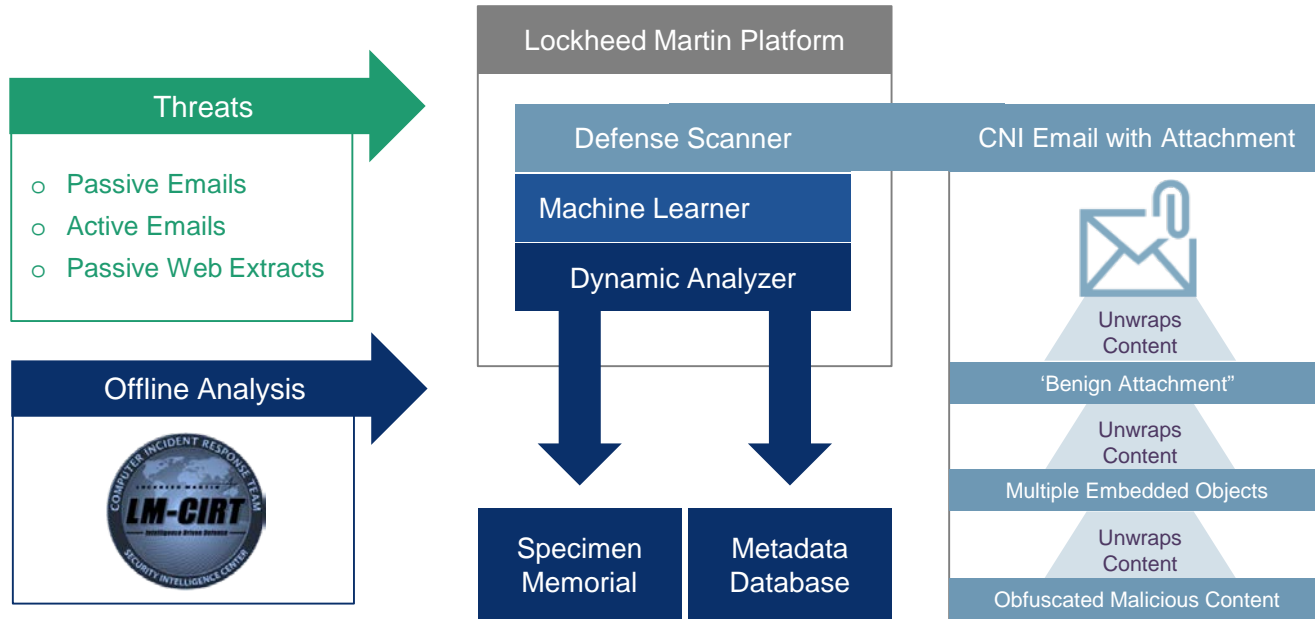- Fully Integrated PCAP/Log/Meta

THE EVOLVING **CYBER MATURITY**

Trending Towards Advanced Visibility and Predictability

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

INTEGRATED **DEFENSE PLATFORM**

Developing Custom Technology to Increase Visibility

Lockheed Martin Platform

Threats
- Passive Emails
- Active Emails
- Passive Web Extracts

Offline Analysis

Defense Scanner

CNI Email with Attachment

Machine Learner

Dynamic Analyzer

Specimen Memorial

Metadata Database

Unwraps Content

'Benign Attachment"

Unwraps Content

Multiple Embedded Objects

Unwraps Content

Obfuscated Malicious Content

MANAGING **KNOWLEDGE**

Managing Gained Intelligence to Create Actionable Tasks
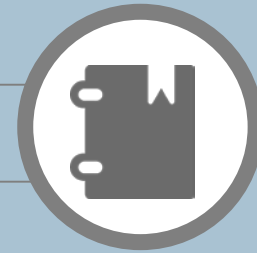
MEASURING **VISIBILITY**

The Level of Visibility Determines How You See the Problem

Nearsighted

Views Campaigns First-Hand. Closest to the Explosion.

Mid-Range
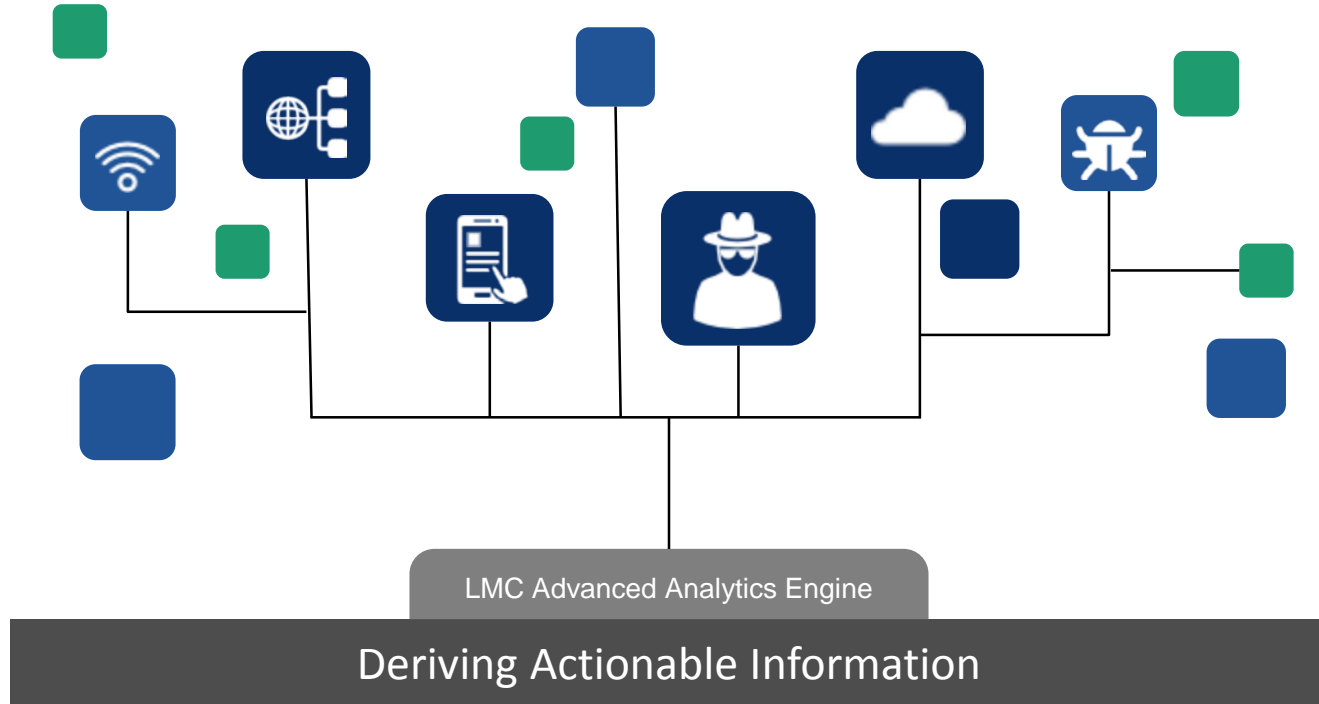
View Campaigns in Motion. Insight into Internet Surface.

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

LMC Advanced Analytics Engine

Deriving Actionable Information

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

LOCKHEED MARTIN