When Failure Is Not an Option:

Risk & National Security

23 June 2015

Brad Pietras
Vice President, Engineering and Technology

Overview

- What's at Risk
- Protecting the Enterprise
- Reactive vs Proactive Defense
- Cyber Kill Chain
- Incident Response Transformation
- Organizing for Success

Reliance On a Robust and Secure Cyber Space

- **Personal information**
- **Organizational information**
- **Social and professional relationships**
- **Trade secrets and other intellectual property**
- **Infrastructure**
  - **Energy**
    - **Supervisory control and data acquisition systems (SCADA)**
  - **Financial**
  - **Transportation**
  - **Telecommunications**
  - **Healthcare**
  - **Defense and Security**
- **Confidence in information systems and services**
- **$375-$500B in annual cost to global economy[1]**

National Security Depends on Cyber Security Across Public and Private Sectors

[1]Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. Center for Strategic and International Studies. June 2014

China Blamed for Massive Breach of US Government Data

On Friday, it was revealed that all of the data on Standard Form 86— filled out by millions of current and former military and intelligence workers— is now believed to be in the hands of Chinese hackers.

This not only means that the hackers may have troves of personal data about Americans with highly sensitive jobs, but also that contacts or family members of American intelligence employees living abroad could potentially be targeted for coercion. At its worst, this cyberbreach also provides a basic roster of every American with a security clearance.

- *The Guardian, 13 June 2015*

Protecting the Lockheed Martin Enterprise

Aeronautics

Information Systems & Global Solutions

Missiles & Fire Control

Missions Systems & Training

Space Systems

- 118,000 Employees
- 70,000 Scientists, Engineers and IT Professionals
- Global Operations: 1000 Facilities in over 75 Countries
- 2x OC-48 Internet pipes (2.4 Gbit/s)
- ~200TB full packet capture storage
- 300 million web requests/day
- 1.2 million Web Proxy Connections per day blocked
- 3.3 million IP addresses
- 145,000 managed desktops
- 1.75 billion sensor events/day
- 30 million emails/day
- 800,000 Active Directory Objects

Largest Defence Contractor, Highly Targeted by Adversaries

Cyber Tradecraft Development

Intelligence Driven Defense® Key to Protecting the Network

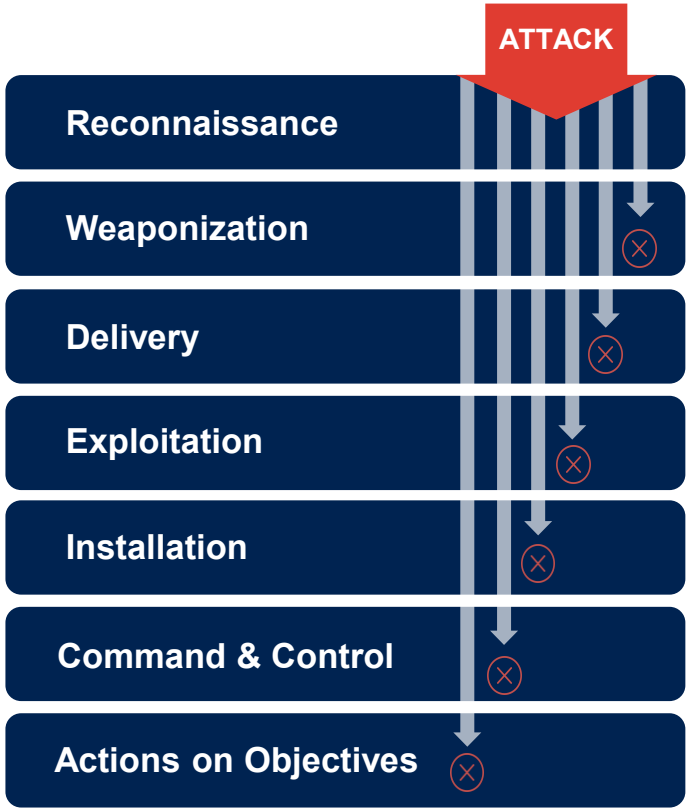
Trending Towards Advanced Visibility and Predictability
Cyber Kill Chain®

REACTIVE

- SOC Model
- Sample Sample Sample
- Event Driven
- Lack TTP knowledge
- PCNP / NDIS through COTS tools

PROACTIVE

- Intelligence Driven
- Understand Adversary
- Object Recursion and Meta Data Analysis through Layer 7 Visibility
- Protocol Logging through Layer 3 Visibility



PREDICTIVE

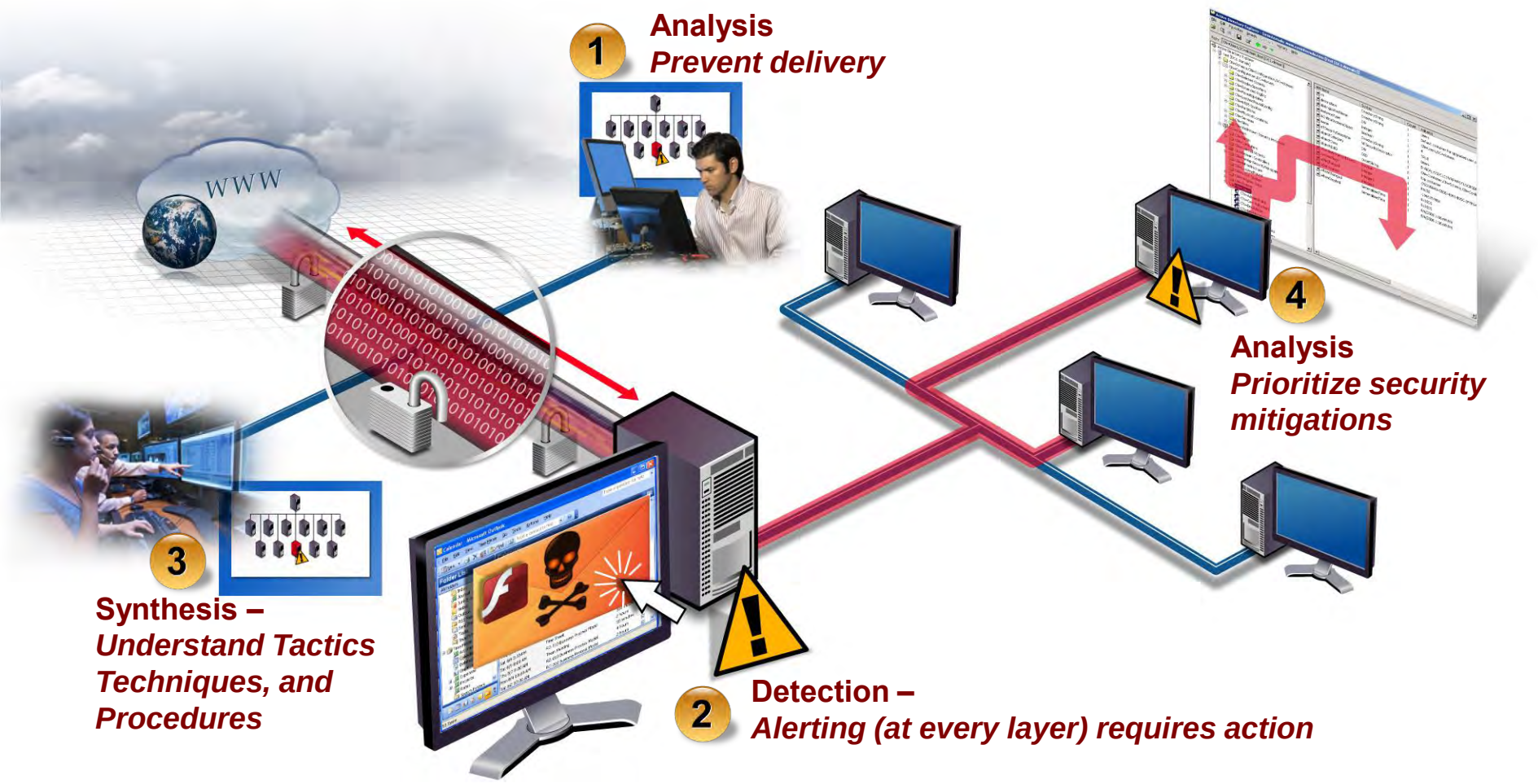
- Predict Attack Trends
- Anticipate Actions through analytics
- Big Data Analytics through Fused PCAP/Log/Meta
- Ability to Decode Brute Force through Layer 3 Detection

Reactive Computer Network Defence

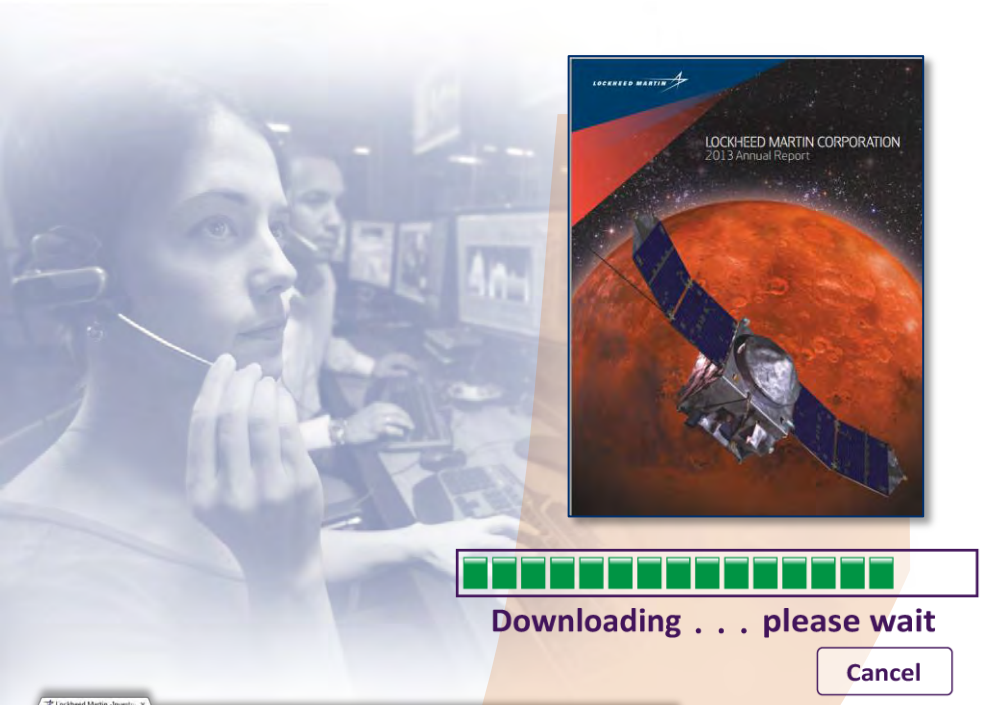
Highly Reactive to each new threat

Proactive Computer Network Defence

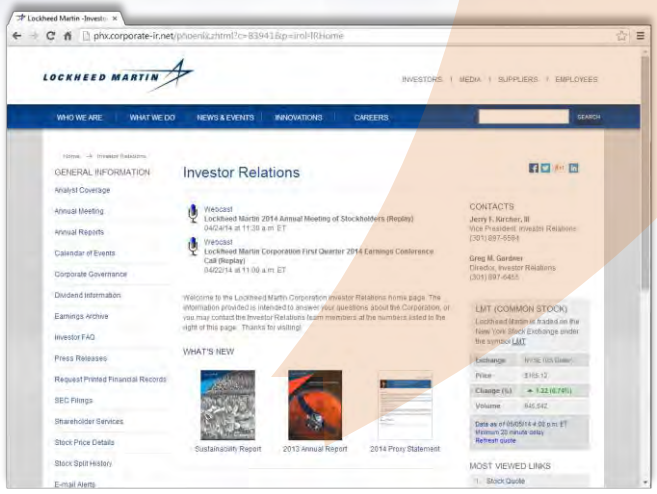
Intelligence Driven



1. Reconnaissance



Cancel



Adversary

- Browse www.lockheedmartin.com website
- Download 2013 Annual Report
- Identify contact information for LM employees, suppliers, customers

Analyst

- Externally facing websites visible to analysts
- Inbound requests logged and archived
- Query parameters, web referrers, and user-agents logged and archived
- Analyst use indicators to refine adversary profile
  - Targets & topics of interest
  - Browser type
  - Language settings
  - Search Terms

2-3. Weaponization & Delivery

Adversary

- Create weaponized PDF from 2013 LM Annual Report via 0-day exploit
- Email: lockheed.user@lmco.com with malicious PDF attachment “LM Annual Report”

Analyst

- Complete recursive analysis
- Email and PDF blocked by custom sensor
- Files and metadata stored for analysis
- Analyst alerted to blocked email
- Analysis of email provides
  - Evidence of targeted attack
  - Malware details
  - Adversary intelligence
- Information sharing of intelligence gained

4-5. Exploitation & Installation

Adversary*

- Human click on PDF attached in email
- Malicious PDF contains 0-day exploit
- Malware is installed
- Remote Shell Executable establishes command and control

Analyst

- Employee training and email testing
- Intelligence sharing with external partners leads to additional signature development
- Shell execution blocked by custom rules on endpoints
- Analyst alerted to shell execution
- Analysis of logs provides
  - Method of delivery
  - Method of exploration

Assuming email delivery successful

6. Command & Control

Adversary*

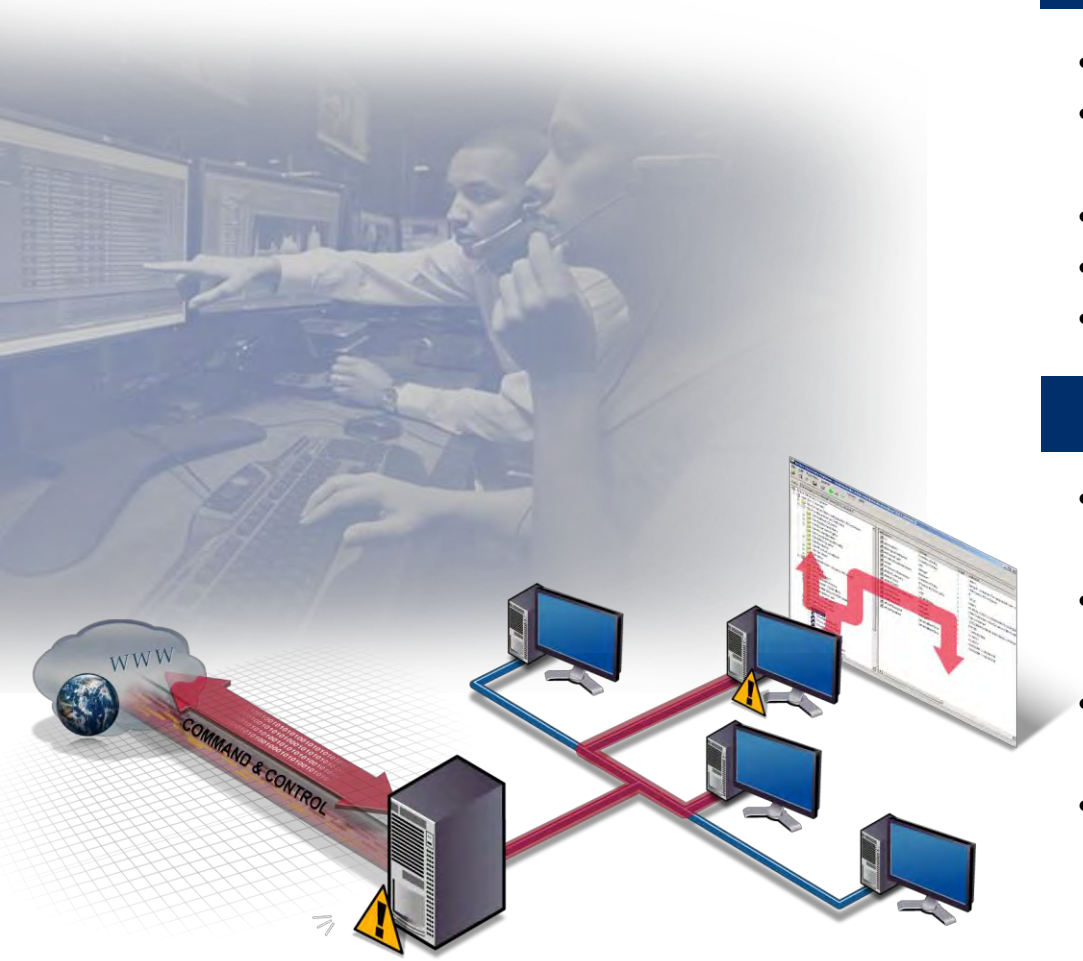
- Establish persistent session to a categorized, but known malicious domain

Analyst

- Connection blocked based upon malicious domain
- Analyst alerted to blocked connection
- Analysis of packets for blocked connection
- Custom brute force coding
- DNS blackholes

Assuming email delivery, exploitation & installation successful

7. Action on Objectives



Adversary*

- Dump user credentials
- Move laterally as an authenticated user. . .
- Package and exfiltrate data
- Destroy system
- Modify data

Analyst

- Analyst alerted based upon vendor tool and custom detections
- Immediate analyst response to alert
- Analysis of host system logs to confirm incident
- Incident response plan activated

Assuming email delivery, exploitation, installation, and command & control successful

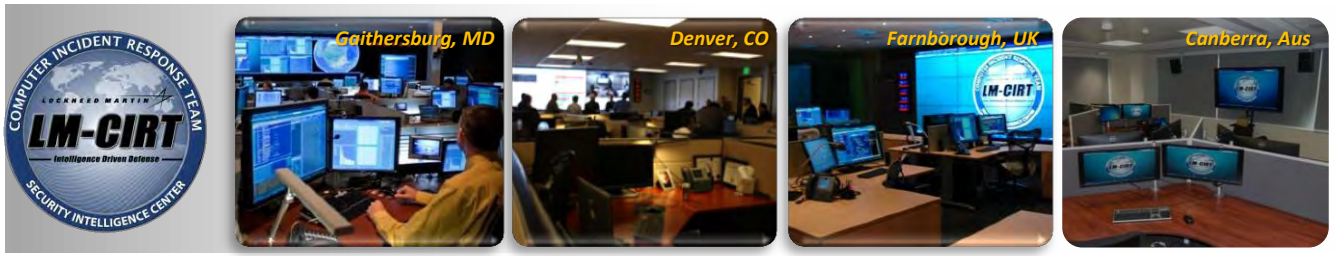
Moving Beyond Incident Response

Incident Response Team Transformation

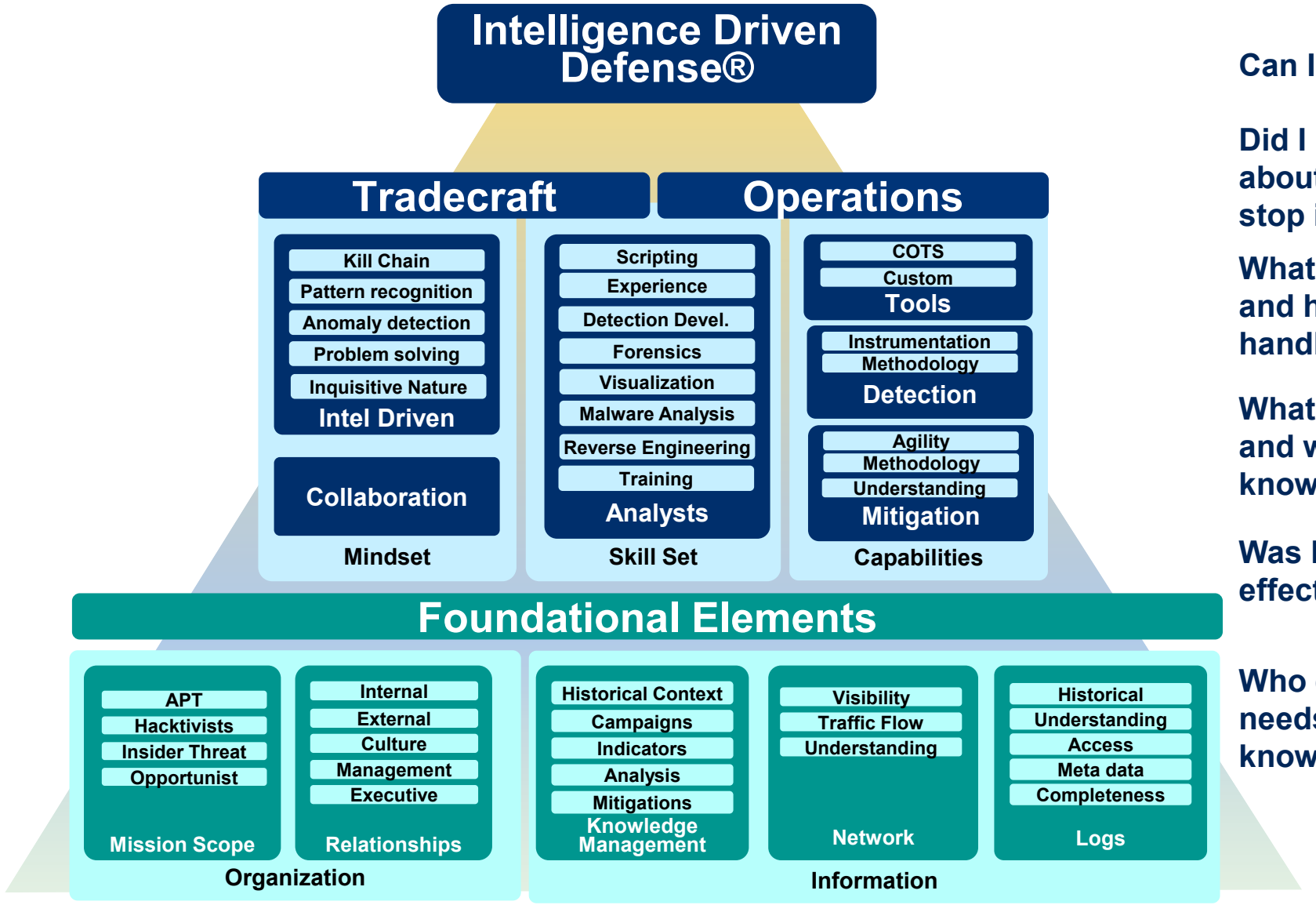
Tradecraft
Intel Driven Mindset & Collaboration

Operations
Skills, Tools & Processes

Foundational Elements
Organisation Structure and Support & Actionable Data



Characteristics of a Successful Organisation



Can I see it?...

Did I know about it and stop it?...

What happened and how do I handle it?...

What did I do and what do I know?...

Was I effective?...

Who else needs to know?...

Cyber Security Risk Management Operating Model

Board of Directors	Board of Directors Cyber Security Metric Periodic Board of Director Committee Briefings Annual White Paper – Cyber Security Update
LMC Executive Staff	Quarterly Executive Reviews (QERs) Periodic Business Area EVP & Staff Threat and Status Briefings Annual Executive Management Council Strategy Review
Independent Reviews	LM Corporate Internal Audit Outside Program Reviews
Risk & Sustainability Councils	Quarterly Enterprise Risk Management Updates
Enterprise Business Services	EBS Quarterly Operating Reviews IT Strategic Governance Board
Corporate Information Security	CIS Monthly Operating Reviews Quarterly CIS & Business Area Risk and Strategy Reviews / Updates

Summary: Executing Integrated Risk Management

Board of Directors

- Aware of Cyber Threats
- Ensures Controls and Adequate Resources Exist
- Understands Risk Exposure

Executive Management

- Alignment of Resources to Risk
- Measures Success of Cyber Defenses
- Ensures Return on Security Investment

Cyber Intel Analysts

- Understands the Adversary
- Derives Intelligence from Internal & External Sources
- Integrates Cyber Intelligence into Security Operations

National Security Depends on Collaboration in the Private and Public Sectors

When Failure Is Not an Option:

Risk & National Security

23 June 2015

Brad Pietras
Vice President, Engineering and Technology

Backup

Security Operations vs. Security Intelligence

Security Operations Centre

- Vendor Driven Defence
- Focus on tools
- Event by event analysis
- Analysis without context of threat
- 24x7 onsite staff coverage
- Tools initiate action (“alert”)

Security Intelligence Centre

- Intelligence Driven hostile activity analytics
- Attack Analysis, Intelligence Fusion, Digital Forensics and custom code development
- Focus on people and collaboration
- Deep understanding of threat, intent, capabilities, collection requirements and our programs
- 24x7 not necessarily required
- Skilled analysts configure tools for high fidelity detection
- People initiate action