Cybersecurity

Integrating threat sharing into cyber defense

David Senty
Director, Cyber Operations

2 December 2013

MITRE

30 Years of Information Assurance
Different Areas of Focus, Same Model

Reduce the Attack Surface

1980s

Focus on protecting operating systems

DoD 5200.28-STD

- Trusted computer base
- Least privilege

1990s

Focus on firewall technology

- Consolidate internet presence
- Proxy internet traffic
- Minimize ports & protocols

2000s

SATAN

Focus on vulnerability assessments

- Know your network
- Find your vulnerabilities
- Patch management

Today

Focus on mitigation and compliance

- FISMA → Continuous Monitoring
- Consensus Audit Guidelines 'CAG 20'

MITRE

What We've Learned

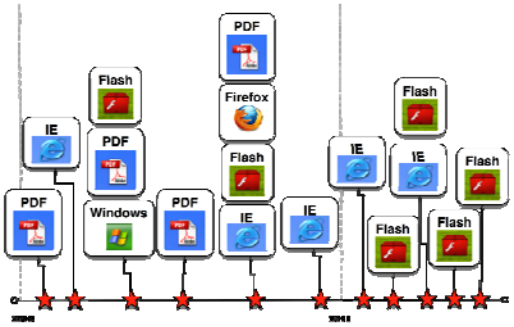
Reducing attack surface really hard – maybe impossible

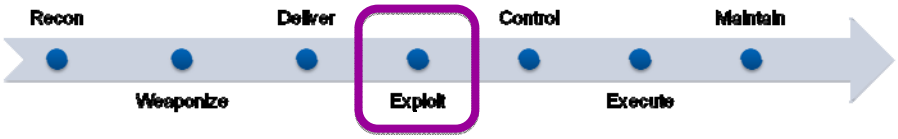
- Networks too large and complex
- Zero vulnerabilities for all assets on network?
  - Assumes you know all assets
  - Assumes you can know all vulnerabilities

Approved for Public Release; Distribution Unlimited. 13-1511

Scanning and Patching Isn't Enough

- **0-day Exploits**
  - Ave. patch time: 30 days
  - Ave. 0-days per year: 8
  - Exposure: 240 days per year
- **Best-practice patching**
  - 90% patched within 72 hours
  - Exposure : > 65% of the year





Cyber Attack Lifecycle

New Approach

A traditional information assurance approach based solely on regulation, which resulted in an approach based on mitigation and compliance around static defenses

To a threat based cyber defense that balances Mitigation with Detection and Response

- Defenders become demanding consumers of intelligence
- Producers of intelligence

MITRE

Characteristics of the Threat

1. **We won't always see the initial attack**
2. **We can't keep the adversary out**
3. **Advanced Persistent Threat is not a "hacker"**

Approved for Public Release; Distribution Unlimited. 13-1511

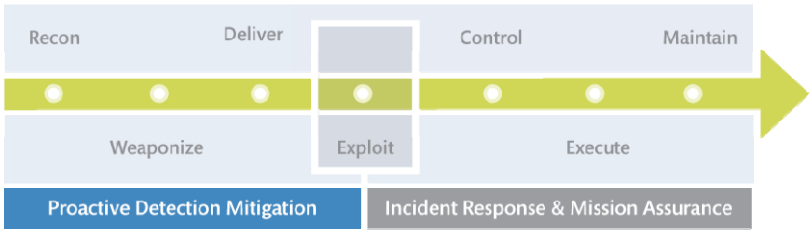
MITRE

Key Elements of Threat-Based Approach

1. **Understanding of Threat Building Blocks**
2. **Effective Threat Sharing Model**
3. **Agile defensive posture aligned with threat**

Approved for Public Release; Distribution Unlimited. 13-1511
MITRE

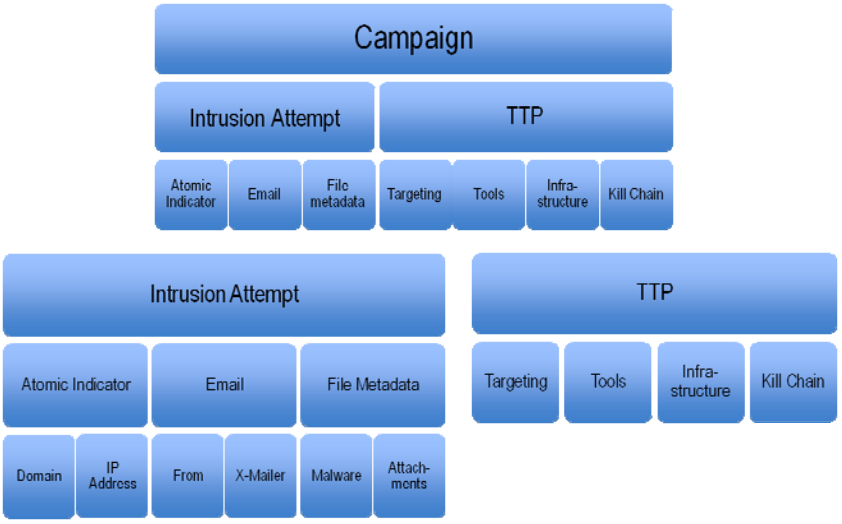
Cyber Attack Lifecycle
A Model to Understand Cyber Threat Actions



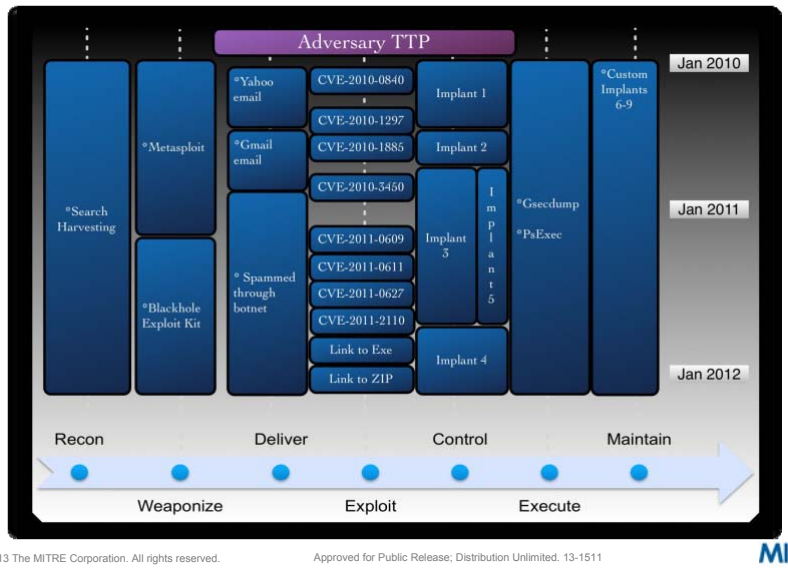
Recon	•Obtain information to conduct the attack
Weaponize	•Place payload into delivery vehicle
Deliver	•Send the attack to the potential victim
Exploit	•The point of no return
Control	•Direct the victim system to take actions
Execute	•Fulfill mission requirements
Maintain	•Insure future access

Approved for Public Release; Distribution Unlimited. 13-1511
MITRE

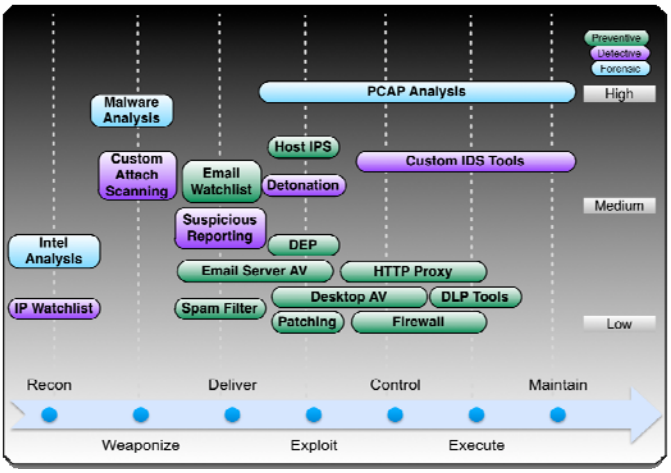
Threat Building Blocks



Example:
Adversary TTPs throughout the Attack Lifecycle



Putting it Together : Layering Your Defense



Approved for Public Release; Distribution Unlimited. 13-1511
MITRE

Share Indicators and Tools, Not Outcomes

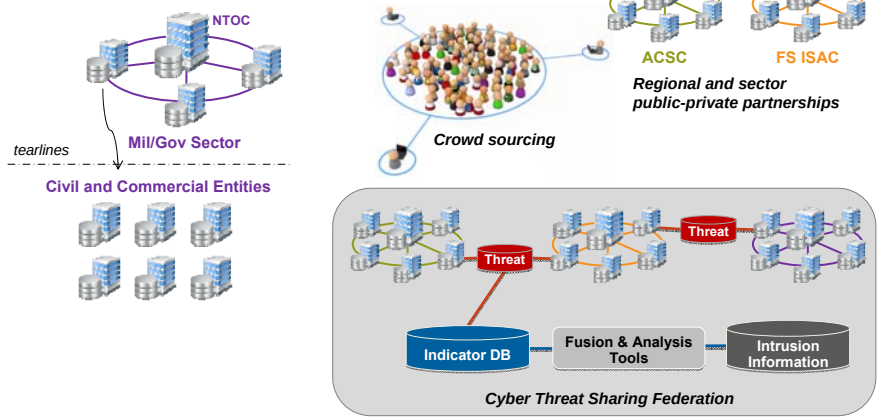
- **Early attempts focused on vulnerabilities, intrusions, and attribution**
- **Organizations resisted sharing**
  - Fear of embarrassment and liability
  - Classification constraints
- **Attribution is overvalued**
  - Not that important to response and mitigation
  - Can be relevant to understanding adversary TTPs

Approved for Public Release; Distribution Unlimited. 13-1511
MITRE

Evolve the Information Sharing Landscape Everyone Can Contribute

From government-led, top-down distribution

To new constructs

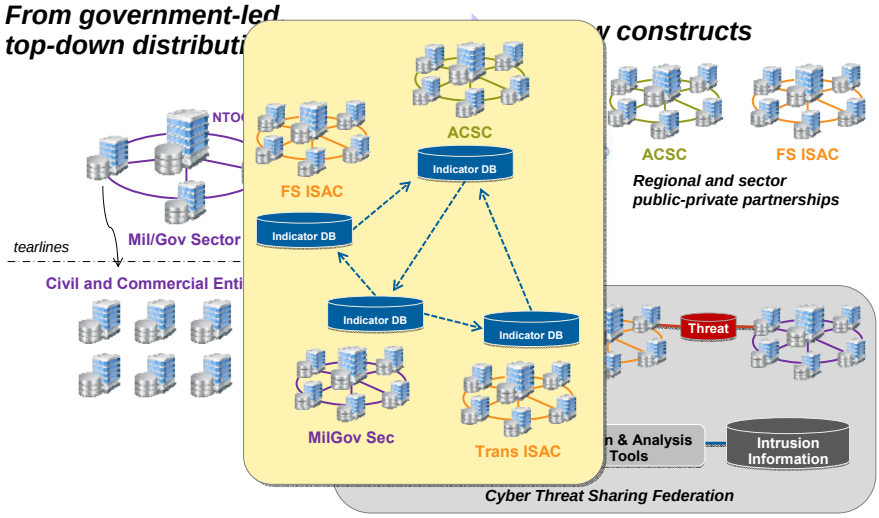


MITRE

Evolve the Information Sharing Landscape Everyone Can Contribute

From government-led
top-down distributi

y constructs



MITRE

Supported By Standards-Based Infrastructure

External Feeds of Threat Information

- OSINT
- DSIE/ACSC
- AV vendors
- ISPs, MSSs

Internal Feeds of Operational & Analyst Threat Information

MITRE CRITS: Structured Threat DB

Sharing Partners

- Indicators
- Observables
- Incidents
- TTPs
- Campaigns
- Threat Actors
- Targets
- COAs

Approved for Public Release; Distribution Unlimited. 13-1511
MITRE

Sharing knowledge of our opponents and watching the plays develop, we can make the saves that protect our **net**works.

Approved for Public Release; Distribution Unlimited. 13-1511

BACK UP

MITRE

Cyber Security Technical Capabilities

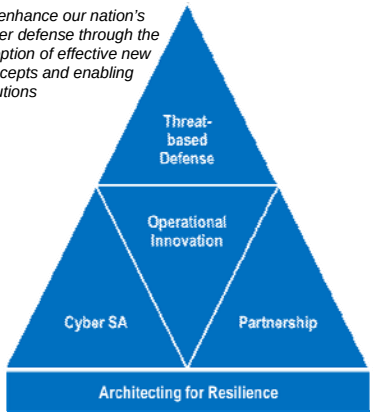
Technical Capability Areas

- Cloud Security
- Mobile Security
- Identity & Access Management
- Threat-Based Cyber Operations
- Multilevel Security
- System Assurance
- Privacy
- Security Programs & Governance
- Architecture, Engineering & Policy
- Specialty and Emerging

Focus Areas for Transformation

Corporate Cyber Initiatives

To enhance our nation's cyber defense through the adoption of effective new concepts and enabling solutions



MITRE

Cyber Security Capability Areas – One Level Deeper

Cloud Security
- Cloud Computing
- Distributed Systems
- Virtualization

Identity & Access Management
- Authentication & Access Control
- Federation
- Administration

Mobile Security
- Devices
- Communications
- Applications
- Enterprise Mgmt.

Multilevel Security
- Cross Domain Solutions
- Multilevel Data

Threat-Based Cyber Operations
- Defensive Cyber Operations
- Cyber Threat Analysis
- Insider Threat
- Situational Awareness
- Cyber Automation Standards
- Partnerships

System Assurance
- Continuous Monitoring
- Software & Hardware Assurance
- Vulnerability Assessment & Security Testing
- Trustworthy Computing
- Anti-Tamper

Privacy

Security Programs & Governance

Architecture, Engineering & Policy
- System Security & Mission Assurance Engineering
- Cyber Resiliency
- Security Architecture
- Security Policy & Risk Management

MITRE