Fighting the APT: Intelligence, Analysis, and User Awareness

Albert Lewis, CISSP, CISM
InfoSec Policy & Compliance Lead
The MITRE Corporation

ajlewis@MITRE.org

Approved for Public Release; Distribution Unlimited. 13-1513

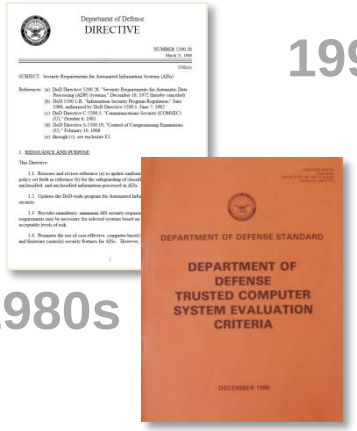
MITRE

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

Reduce the Attack Surface

Reduce the Attack Surface

1980s

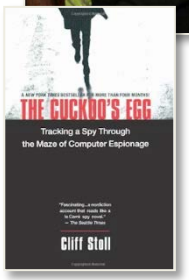


Focus on protecting operating systems

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

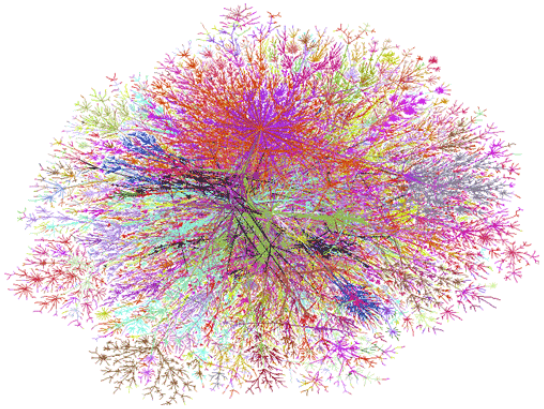
- FISMA → Continuous Monitoring
- Consensus Audit Guidelines 'CAG 20'

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**



MITRE

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

Characteristics of the Threat

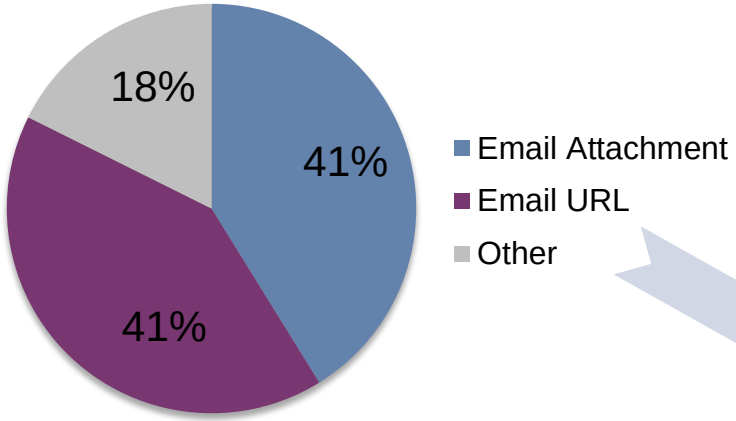
1. **We won't always see the initial attack**
2. **We can't keep the adversary out**
3. **Advanced Persistent Threat is not a "hacker"**

Attributes of a Top-Notch Cyber Program Today

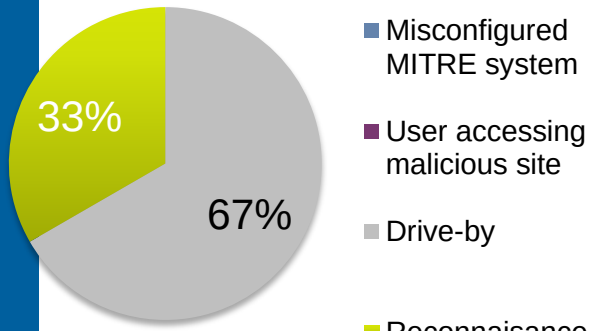
1. **Cyber Intelligence Program**
   - Rich set of sources
   - Disciplined Indication and Warning process
   - Good understanding of threat actors in your sector
2. **Quality Malware Analysis Program**
   - Large repository of samples which extracts unique signatures
   - Works with larger malware community
3. **Development team working side-by-side with operators (DevOps)**
4. **Incidence response “baked into” defensive posture**
5. **Workforce culture of “cyber aware”**

Advanced Persistent Threat (APT)
How do they attack?

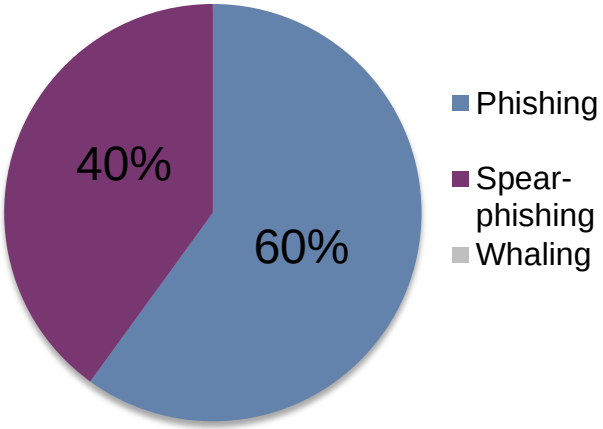
Attack Vectors



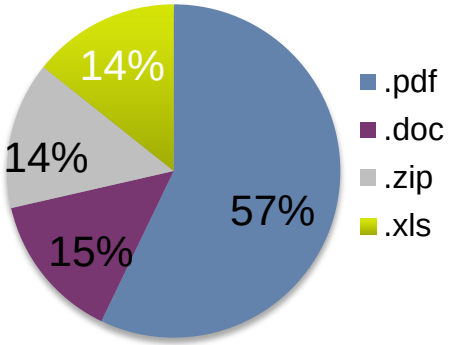
Other



Social Engineering Technique



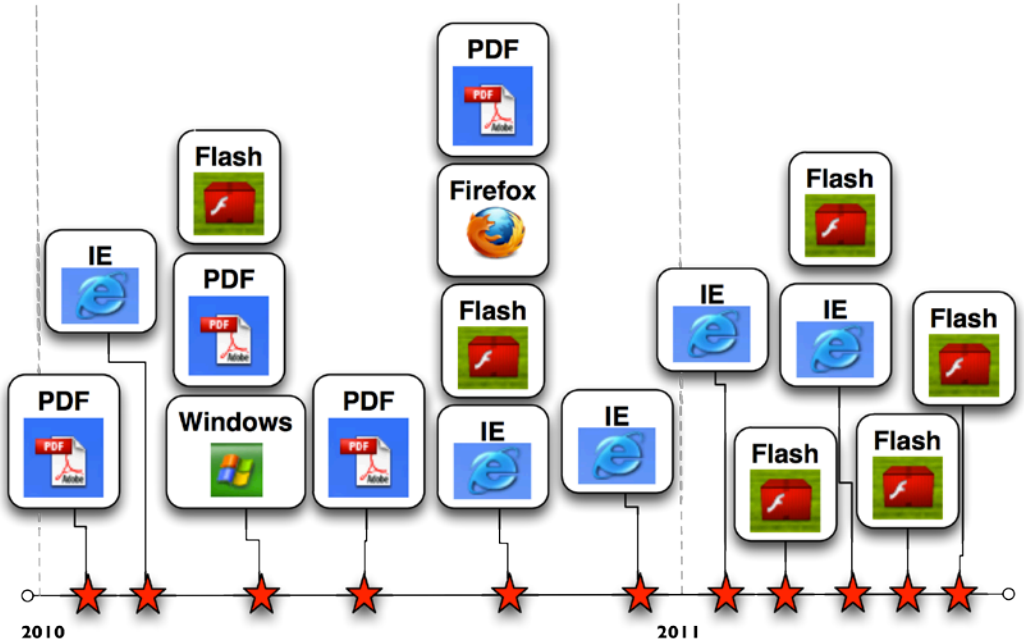
Attachment Payload

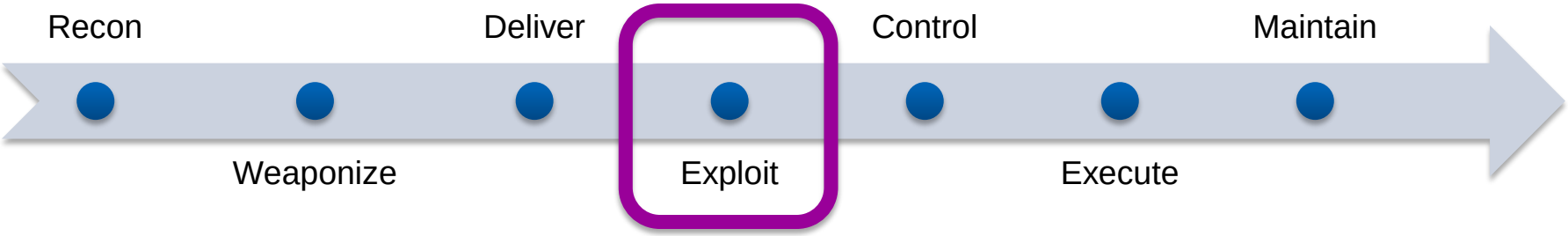


MITRE

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

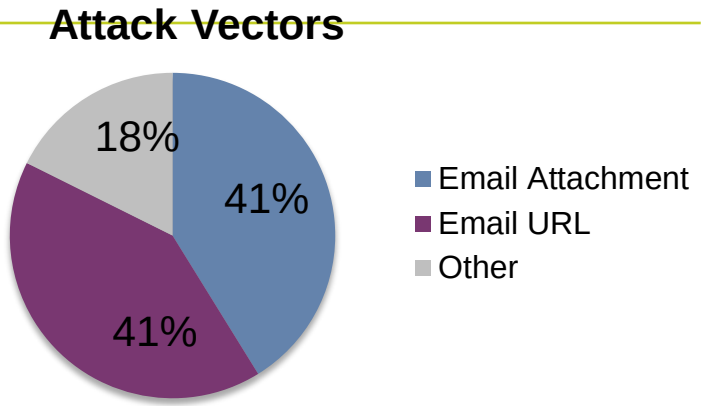
MITRE

Tools and Sensors

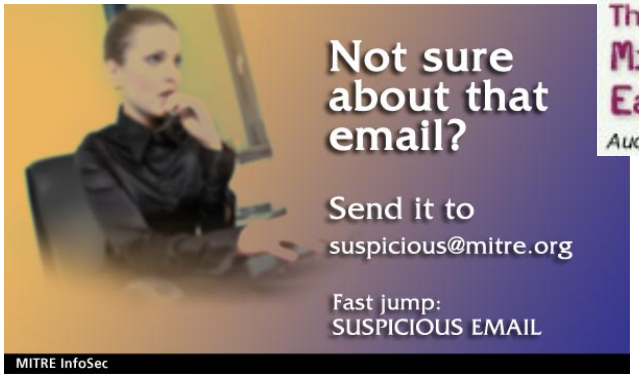
- **Centralized Log Manager**
  - Web proxy, Mail, DNS, etc. logs
- **Security Information and Event Management**
  - NetFlow analysis
- **Packet Capture and Analysis**
  - Malware extraction
  - Traffic analysis
- **Snort – Network Intrusion Detection System**
  - Intelligence derived signatures
- **RT - Trouble ticketing system**
  - Incident Response work flow and documentation
- **Desktop anti-virus**
- **Email gateway anti-virus**

User Awareness Practices

- **Motivation: Users are the biggest target**



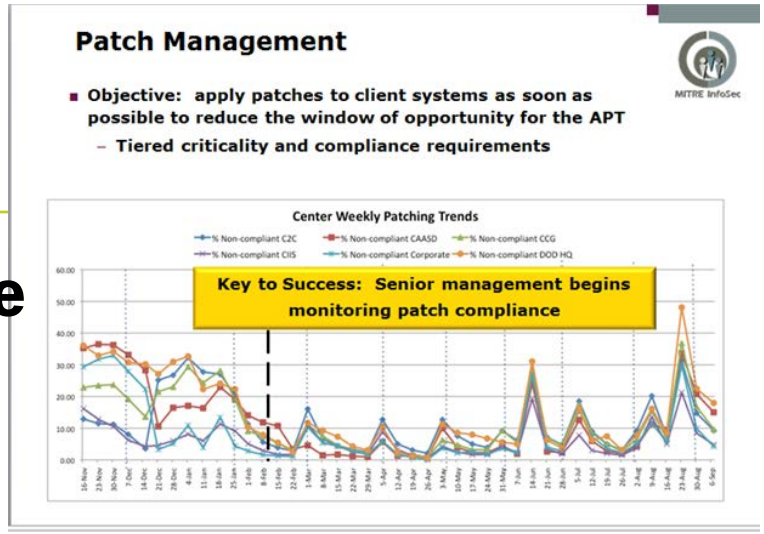
- **Best Practices:**
  - **Repeated Targeted messaging; building a "Don't click" culture**
  - **Easy reporting: suspicious@mitre.org**
  - ***Personal Engagement* – 1-1 follow-up from suspicious email, proactively briefing frequently targeted users, follow-up on incidents, …**

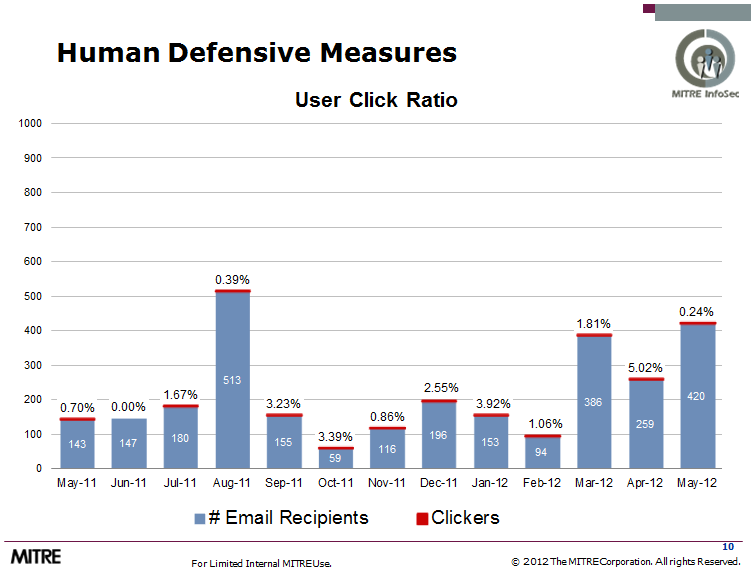


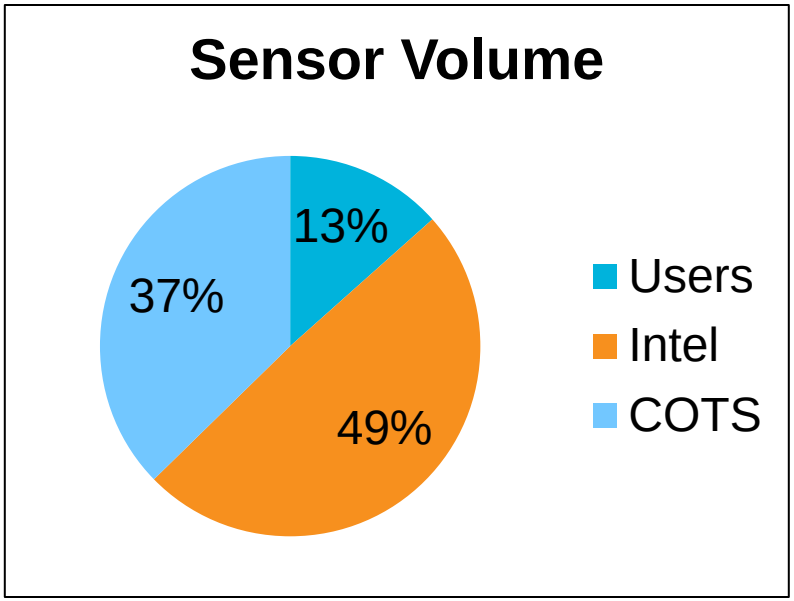
MITRE

User Awareness Results

- Great patch response time
- Click rate
- Users as sensors



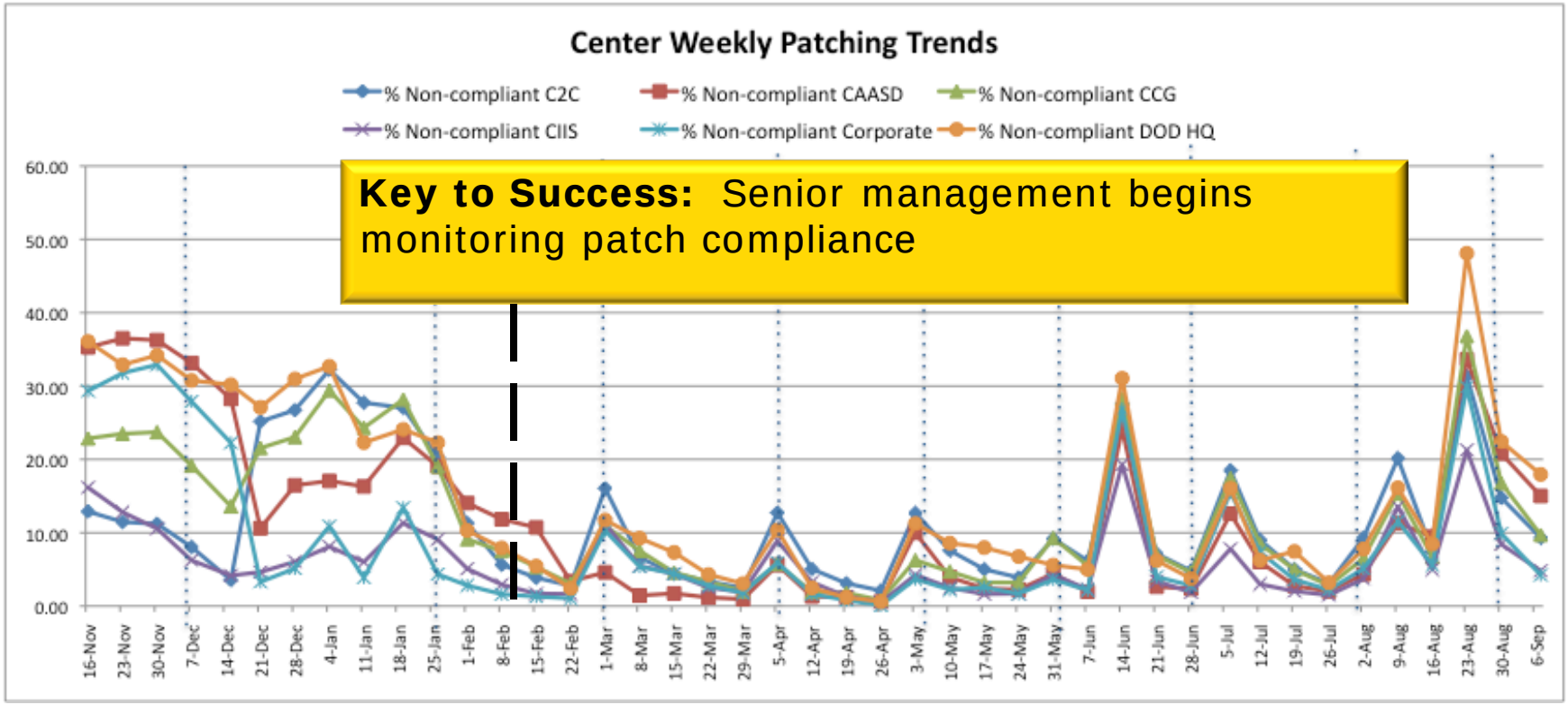




MITRE

Patch Management

- **Objective: apply patches to client systems as soon as possible to reduce the window of opportunity for the APT**
  - Tiered criticality and compliance requirements



Key to Success: Senior management begins monitoring patch compliance

MITRE

Cyber Intelligence Business Case

- **Zero days exploits provide a window of opportunity for the APT**
- **COTS security technology is only partially effective against detecting APT attacks**
- **User reporting is not 100%**
  - The APT needs only one user to click

Other means of detecting and defending against the APT are needed
…
the mission of cyber intelligence is to bridge this gap

Key Elements of Threat-Based Approach

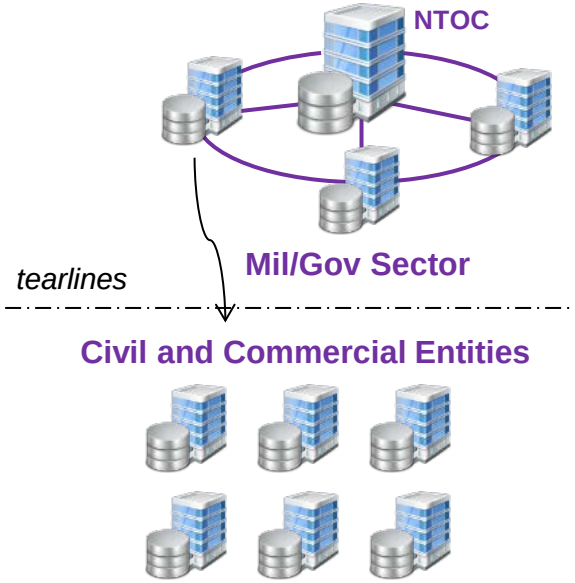
1. **Understanding of Threat Building Blocks**
2. **Effective Threat Sharing Model**
3. **Agile defensive posture aligned with threat**

Share Indicators and Tools, Not Outcomes

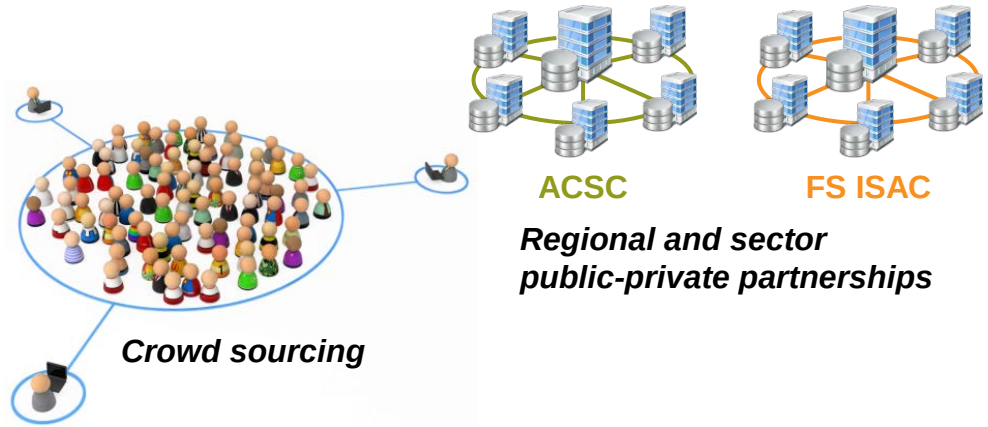
- **Early attempts focused on vulnerabilities, intrusions, and attribution**
- **Organizations resisted sharing**
  - Fear of embarrassment and liability
  - Classification constraints
- **Attribution is overvalued**
  - Not that important to response and mitigation
  - Can be relevant to understanding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

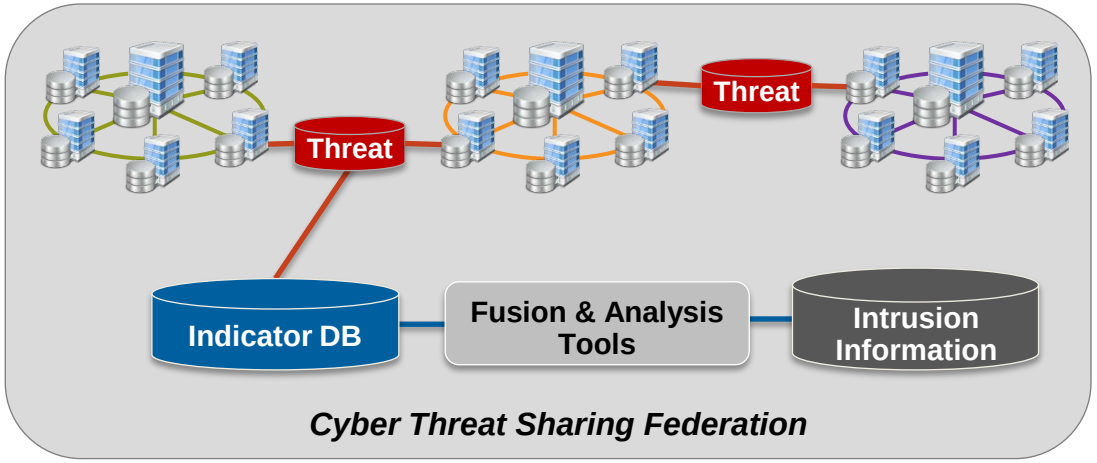
Evolve the Information Sharing Landscape Everyone Can Contribute

From government-led, top-down distribution



To new constructs



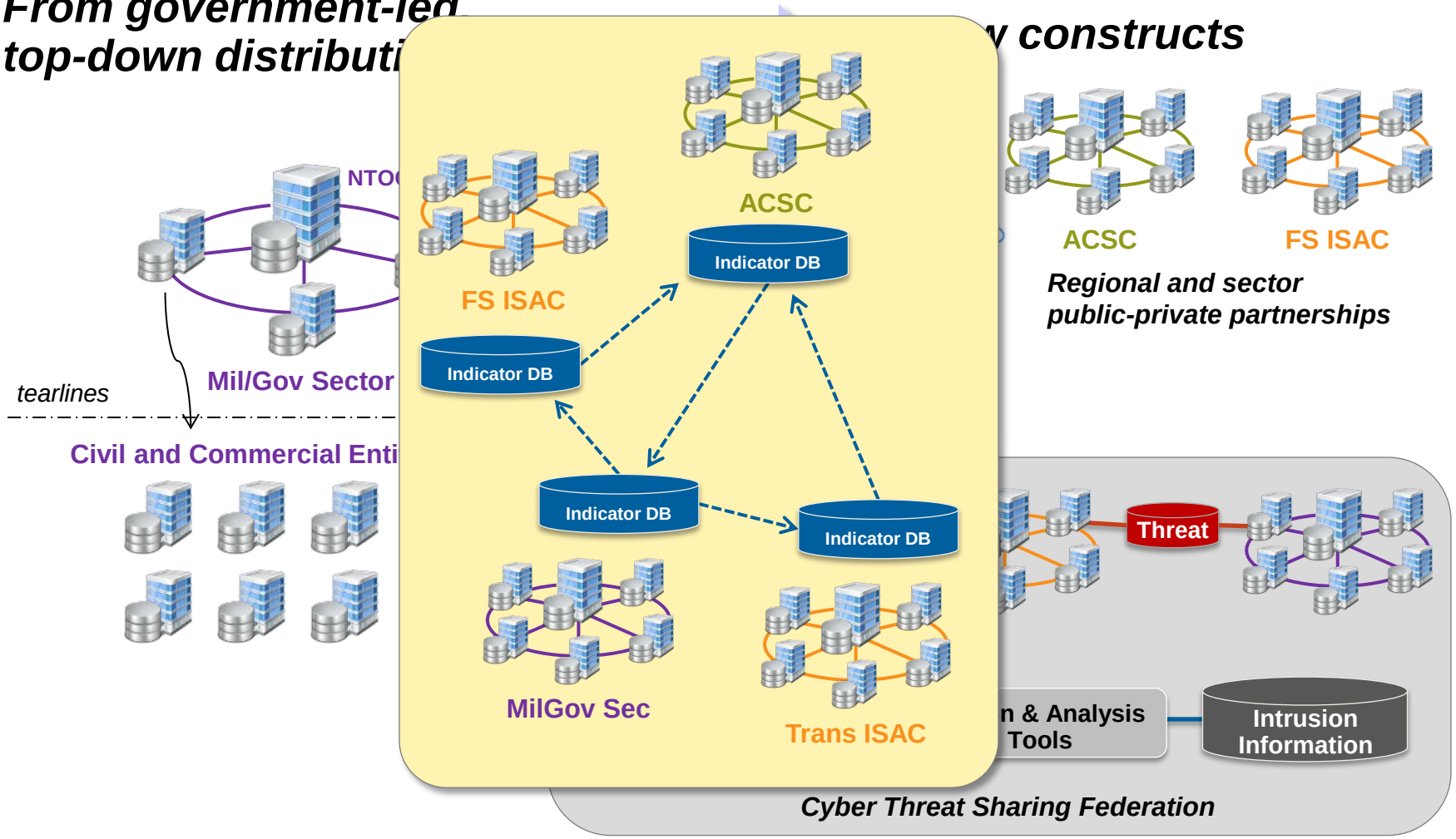


MITRE

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

DCISE

AV vendors

ISPs, MSSs

MITRE CRITS: Structured Threat DB

Sharing Partners

Internal Feeds of Operational & Analyst Threat Information

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

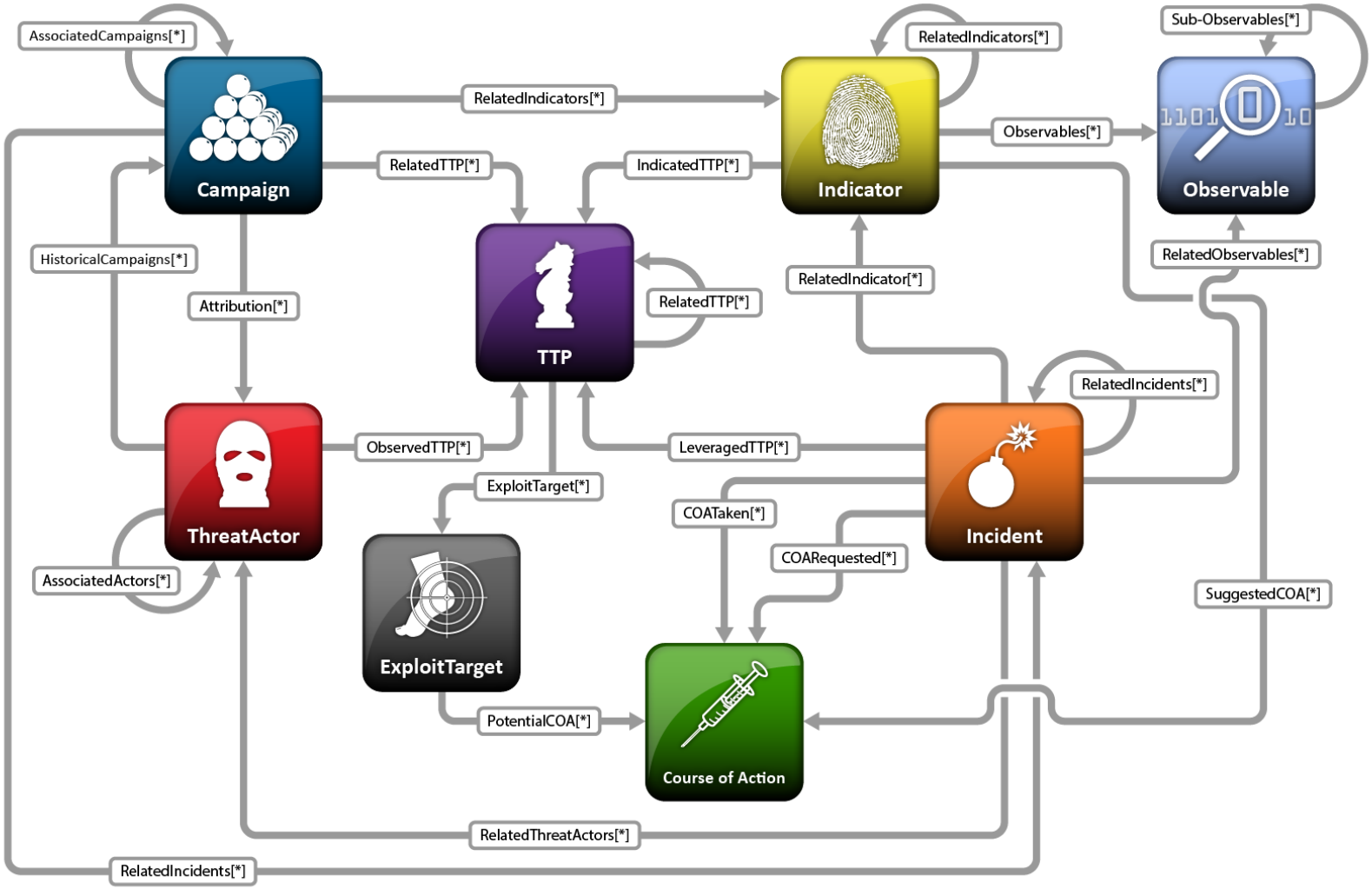
MITRE

What is “Cyber (Threat) Intelligence?”

Consider these questions:

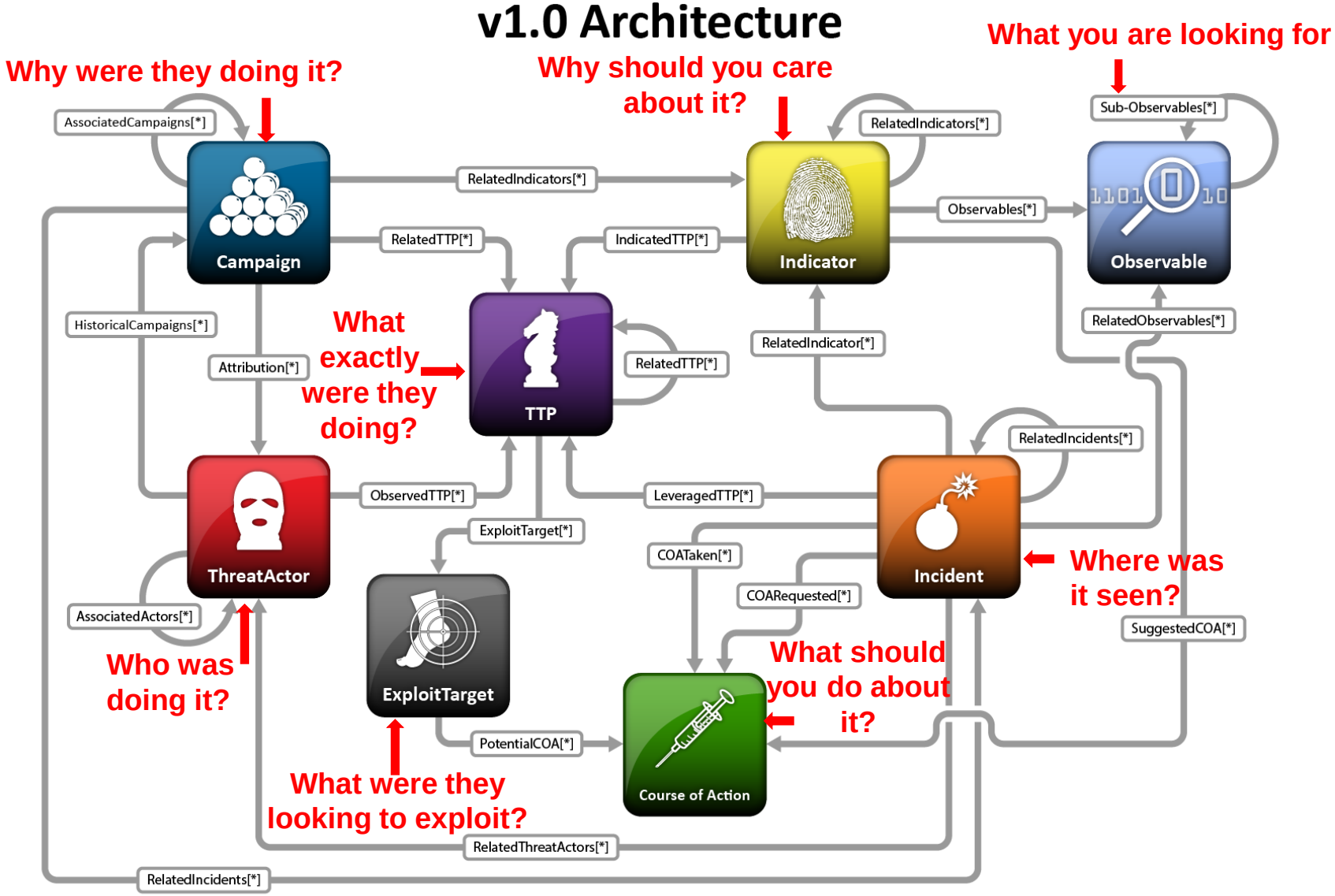
- What activity are we seeing? — Observable
- What threats should I look for on my networks and systems and why? — Indicator
- Where has this threat been seen? — Incident
- What does it do? — TTP
- What weaknesses does this threat exploit? — ExploitTarget
- Why does it do this? — Campaign
- Who is responsible for this threat? — ThreatActor
- What can I do about it? — Course of Action

Structured Threat Information eXpression (STIX) v1.0 Architecture



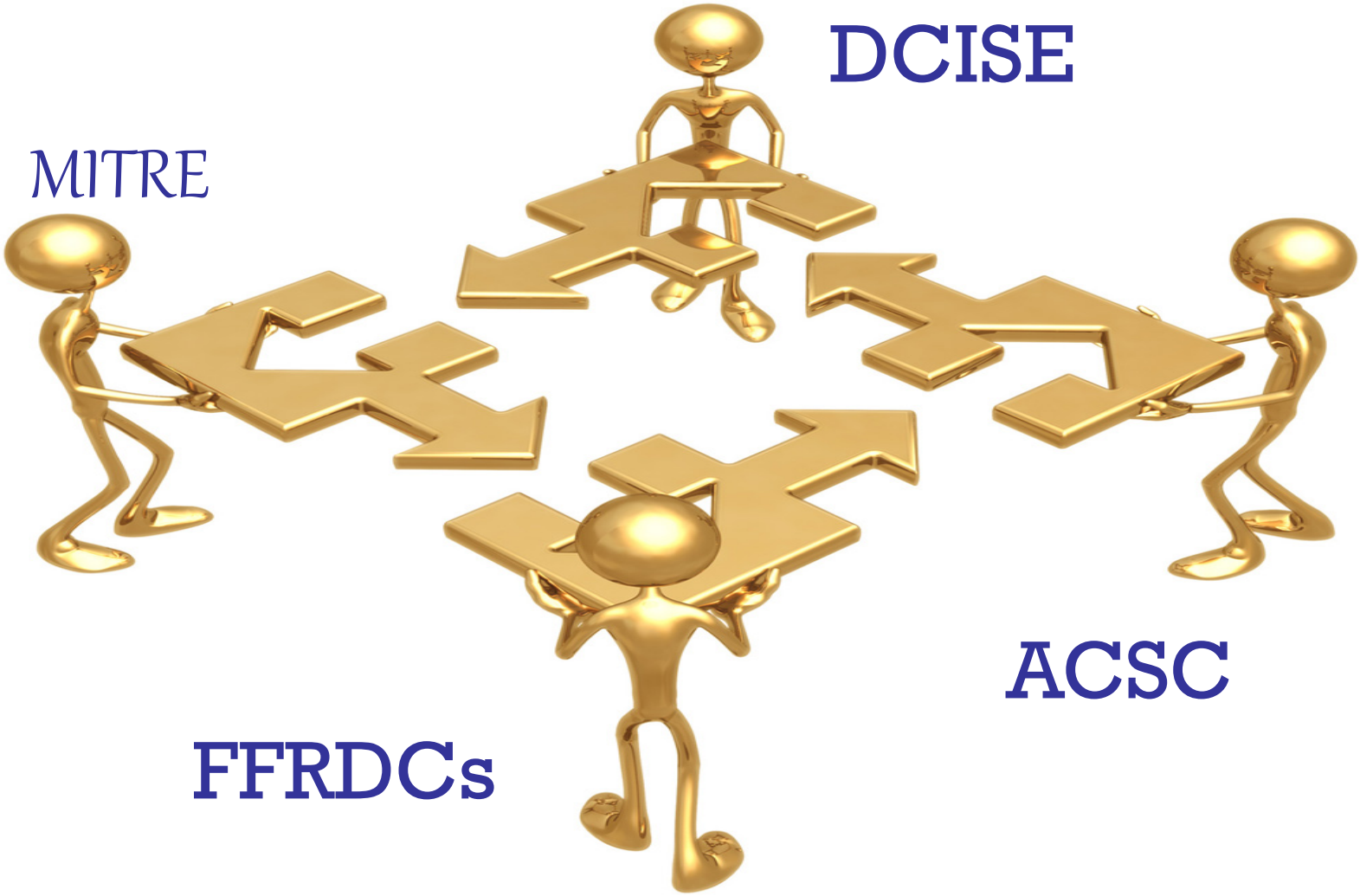
MITRE

Structured Threat Information eXpression (STIX) v1.0 Architecture



MITRE

Partnerships



MITRE

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