OWASP
The Open Web Application Security Project

Attack is easy, let's talk defence

From threat modelling to intelligence driven defence.

Teodor Cimpoesu
Technical Director
UTI-CERT, certSIGN

Cosmin Anghel
CERT Services Manager
UTI-CERT, certSIGN

About Me

OWASP
The Open Web Application Security Project

@Teodor:

- 0x01 – Worked at GeCAD / RAV
- 0x02 – Moved to Kaspersky Lab for development
- 0x03 – Investigations / forensics enthusiast
- 0x04 – Linux / OSX main land
- 0x05 – Speaker at various cyber conferences / LE training
- 0x06 – Consultant and advisor on cyber security topics
- 0x0a – Building first private SOC/CSIRT at UTI Grup

@Cosmin:

- 0x01 - CERT Services Manager at certSIGN
- 0x02 - Former Cyber Threats Expert at National CyberInt Center
- 0x04 Interests in: Incident response/ Digital forensics/ Malware analysis/ Cyber investigations

Agenda

1. Attack vs. Defence
2. Structured Defence Approach
3. Defence Best Practices
4. Live Incident Response
5. Demo – GRR & Volatility

1. Attack vs. Defence

From 0-day to 1-year

- In a Symantec study*, **11 of 18** identified vulns were not known 0-days.
- Attacks with 0-days lasted b/w **19 days – 30 months**, with a MED of **8** and AVG of **10** month.
- After disclosure, the **variants** exploiting them explode **183-85k** times, and **attacks** increase **2-100k** times
- Exploits for **42%** of vulns are detected within **30 days** after disclosure
- **200+ days** MED, **243 days** AVG, the attackers **reside** within a victim network **before detection**

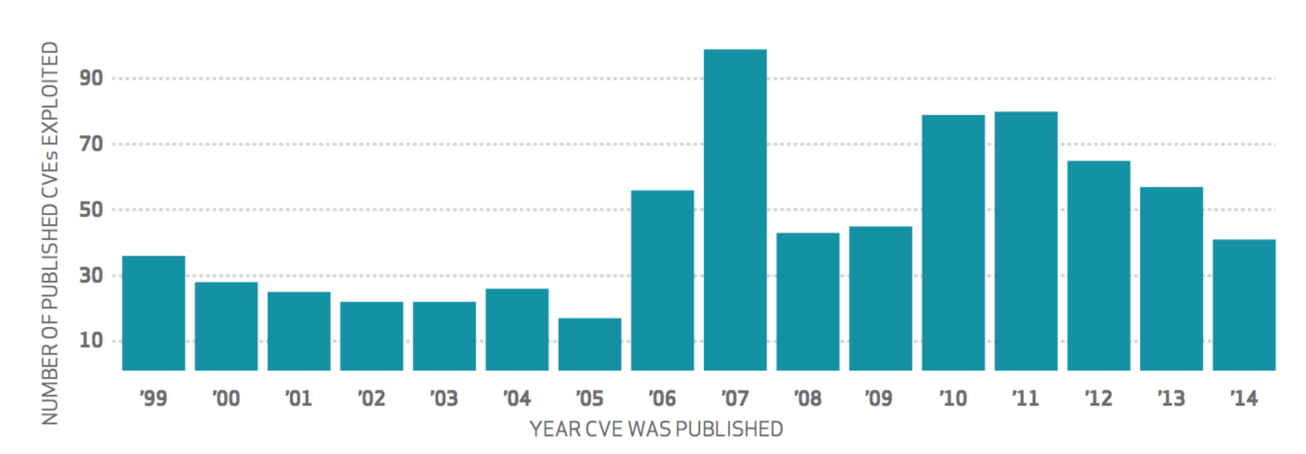
* Source: Before We Knew It - An Empirical Study of Zero-Day Attacks In The Real World, Tudor Dumitras et al., Symantec Research Labs

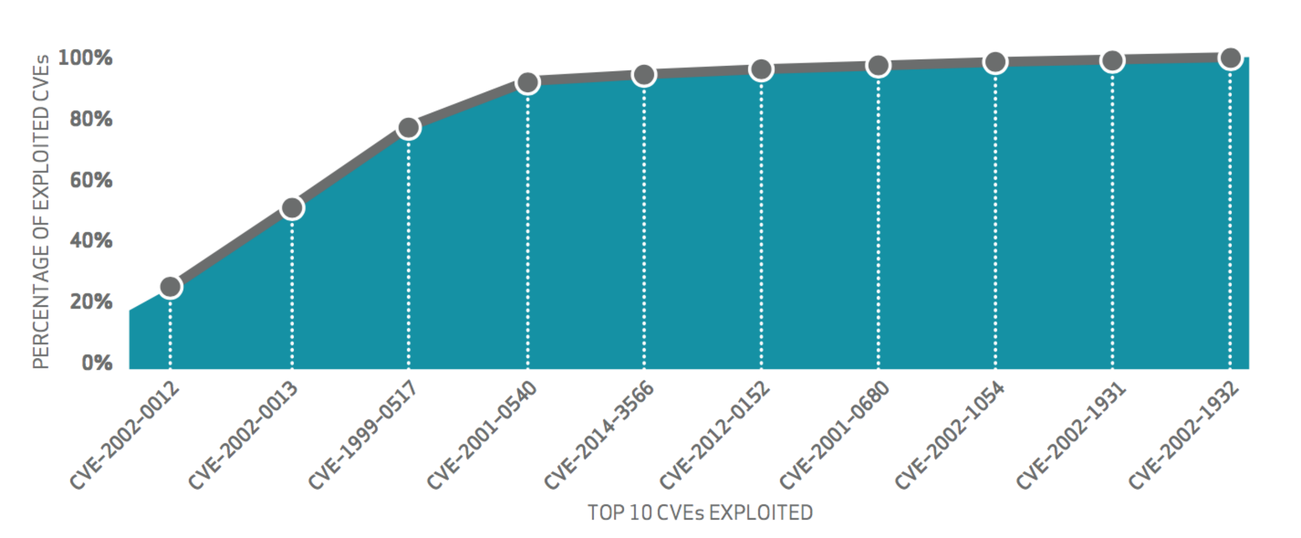
- **1 in 5** (~**20%**) of threat actors are **internal**
- **75%+** of all network intrusions are due to **compromised** user **credentials**
- **84% with no admin rights**
- **60%** of cases attackers compromise the org within **minutes**
- **Discovery** done within **days or less** is below **25%**
- **94%** of the breaches are **reported** by a **3rd party**

Sources: Microsoft Advanced Threat Analytics, HP Security, Verizon DBIR2015, ObserveIT

OWASP
The Open Web Application Security Project

Attack vs. Defence – mindset deficit



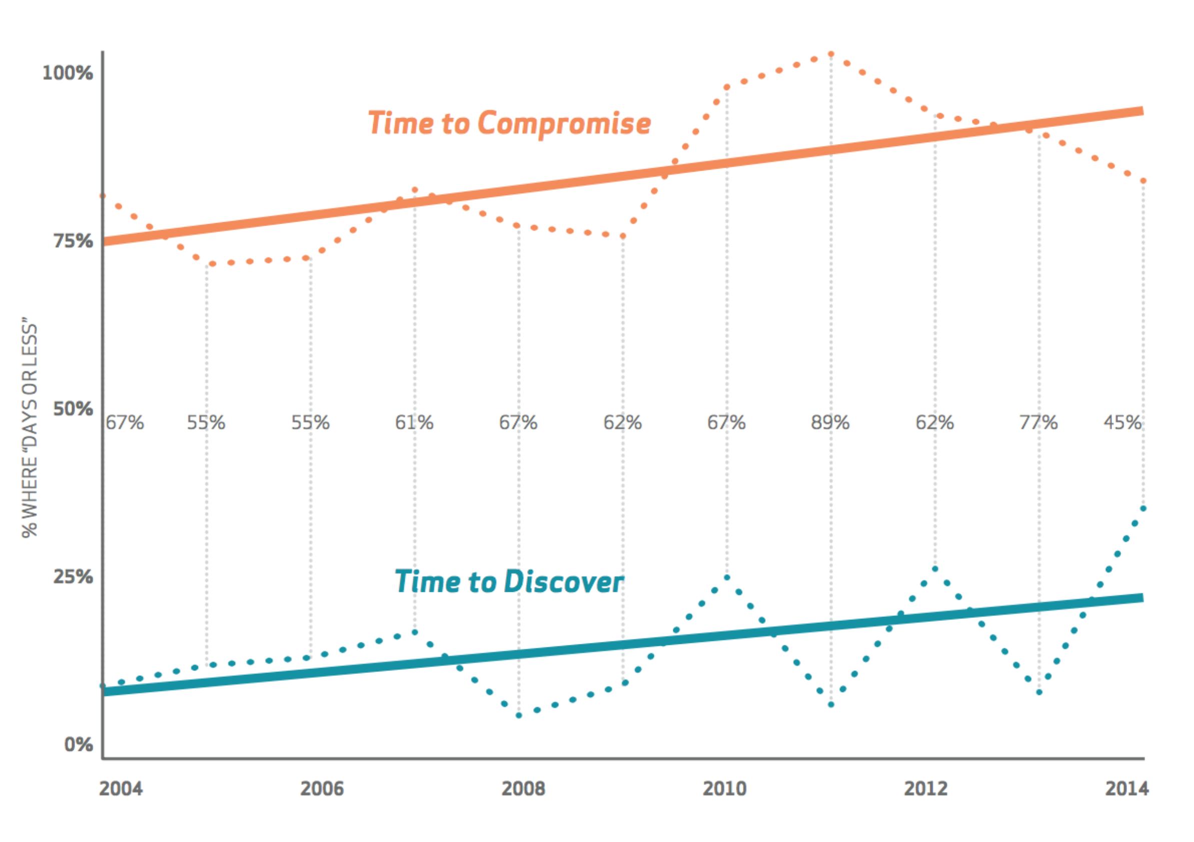


(goto)Fail to Patch

99.9% of the exploited vulns were compromised more than a year after the CVE was published

Source: Verizon DBIR2015

Attack vs. Defence - detection deficit



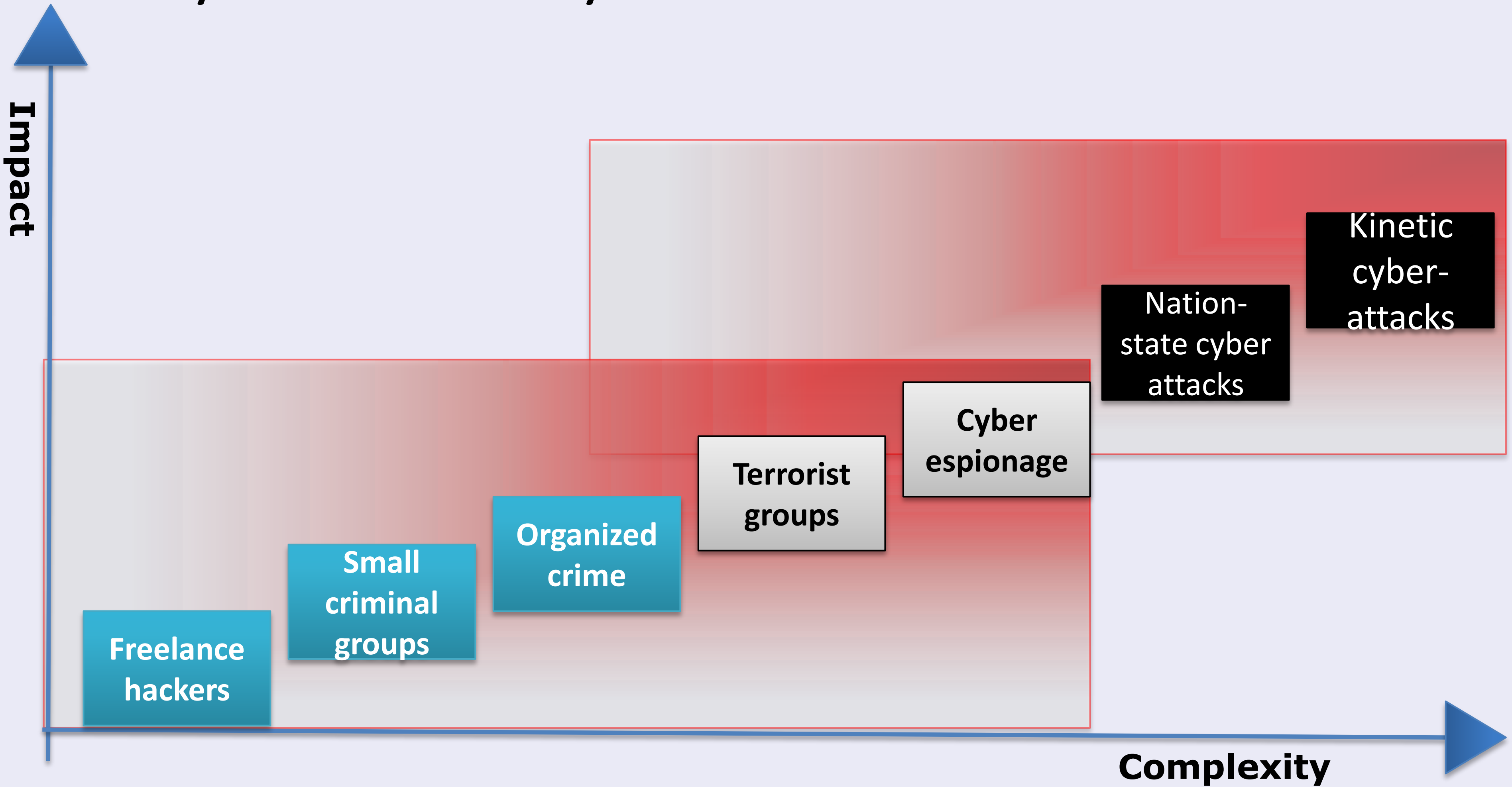
Source: Verizon DBIR2015

- Cyberspace favors **offense**
- Shift from ***total security*** to ***assume compromise***

A:"We only have to be lucky once.
You will have to be lucky always." (IRA,'84)

D:"There's no way that we are going to win the cybersecurity effort on defense. We have to go on offense."
(Steven Chabinsky, former head of FBI CyberIntelligence, CRO at CrowdStrike)

Cyber threats dynamics



“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position ***unassailable****.”*

- Sun Tzu, The Art of War, 513 BC

“*Attack and defence are things differing in kind and of unequal force. Polarity is, therefore, not applicable to them*”

“*Everything in war is very simple but the simplest thing is difficult*”

- Carl von Clausewitz, On War, 1823

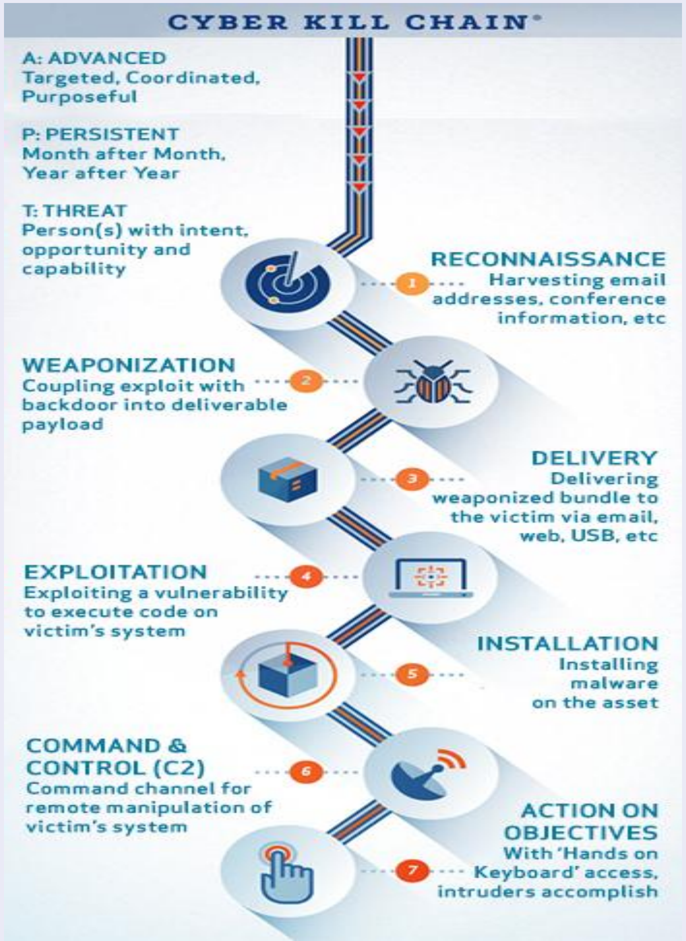
“*War in general is* ***not declared****. It simply begins with already developed military forces.*” – Georgy Isserson, New forms of combat, 1937

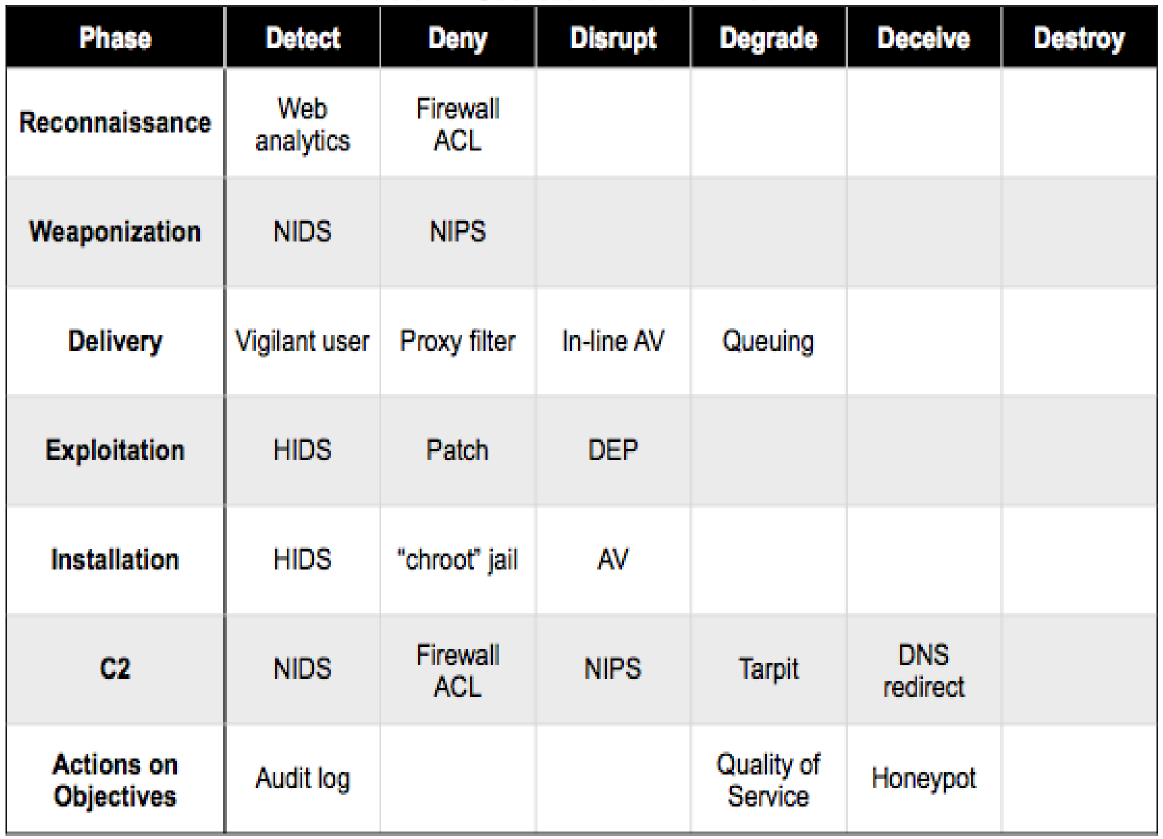
“*Action taken to* ***disrupt****,* ***deny****,* ***degrade*** *or* ***destroy*** *information resident in a computer and/or computer network, or the computer and/or computer network itself.*”

- NATO AAP-06 Edition 2014

2. Structured Defence Approach

Intelligence-driven defense

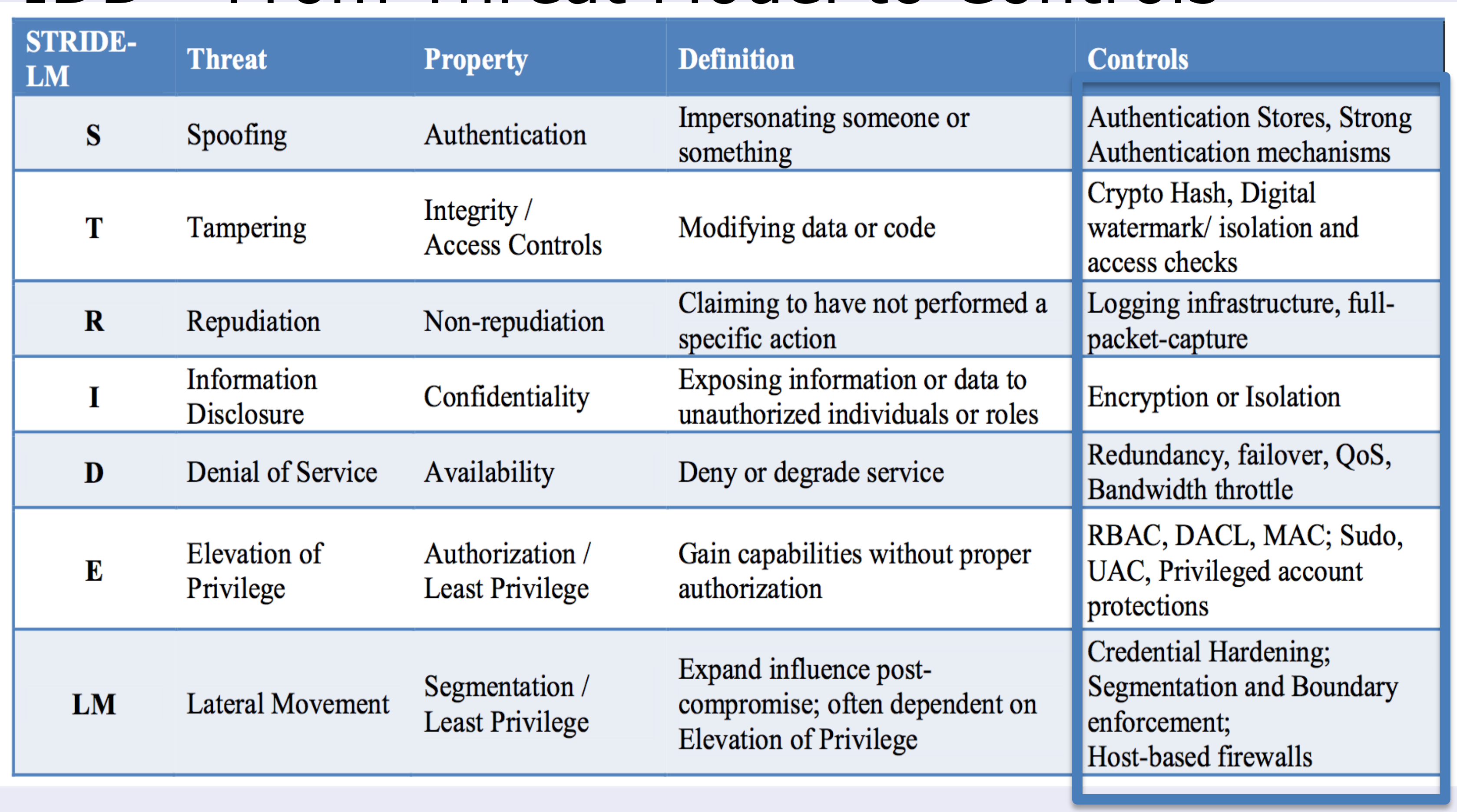

CYBER KILL CHAIN®
A: ADVANCED
Targeted, Coordinated, Purposeful
P: PERSISTENT
Month after Month, Year after Year
T: THREAT
Person(s) with intent, opportunity and capability
1
RECONNAISSANCE
Harvesting email addresses, conference information, etc
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim's system
7
ACTION ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Source: "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Eric M. Hutchins et al.

IDD - From Threat Model to Controls

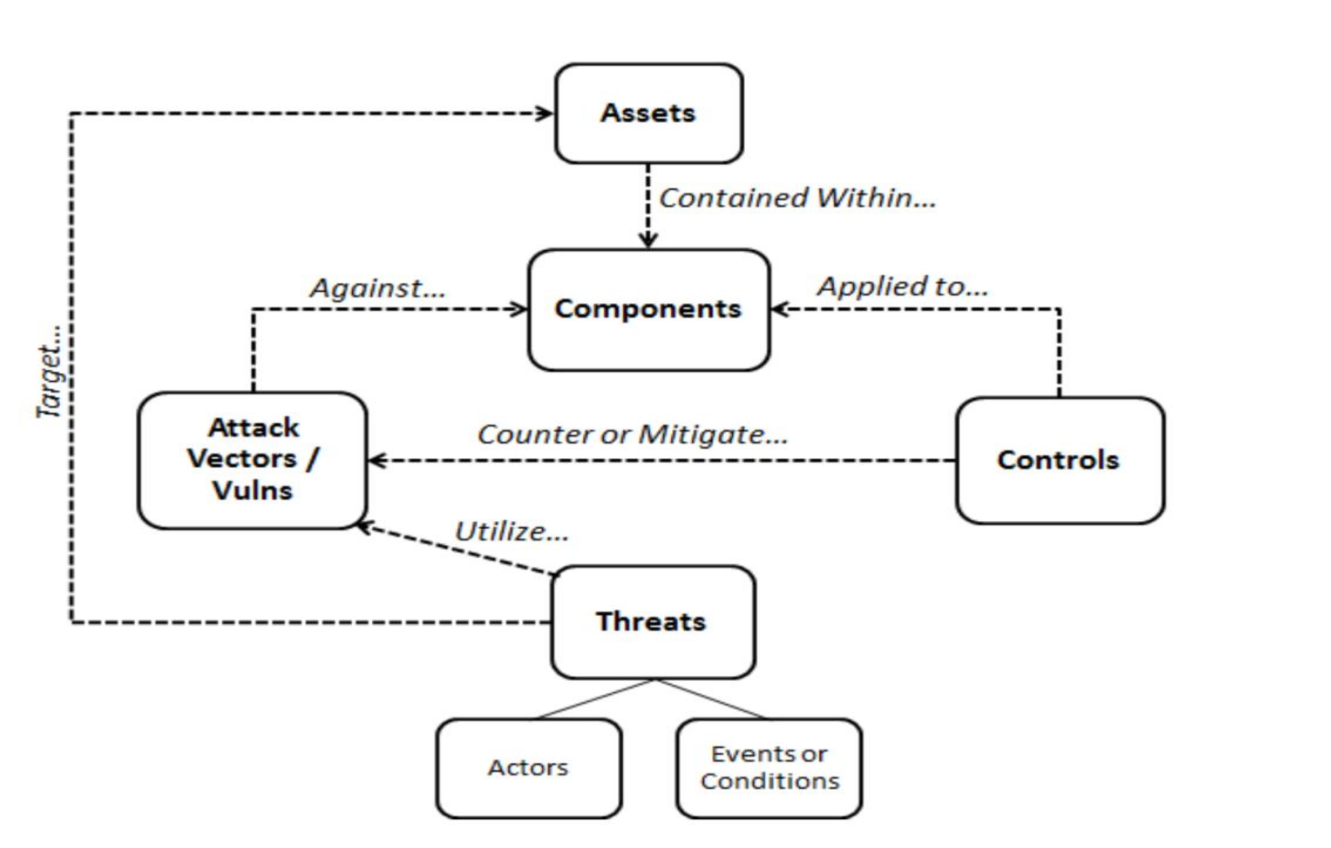


STRIDE-LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections

LM	Lateral Movement	Segmentation / Least Privilege	Expand influence post-compromise; often dependent on Elevation of Privilege	Credential Hardening;
				Segmentation and Boundary enforcement;
				Host-based firewalls

Source: "A Threat-Driven Approach to Cyber Security - Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization", Lockheed Martin Corp.

Threat Modeling



Source: “A Threat-Driven Approach to Cyber Security - Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization”, Lockheed Martin Corp.

IDDIL/ATC Methodology

I. Discovery

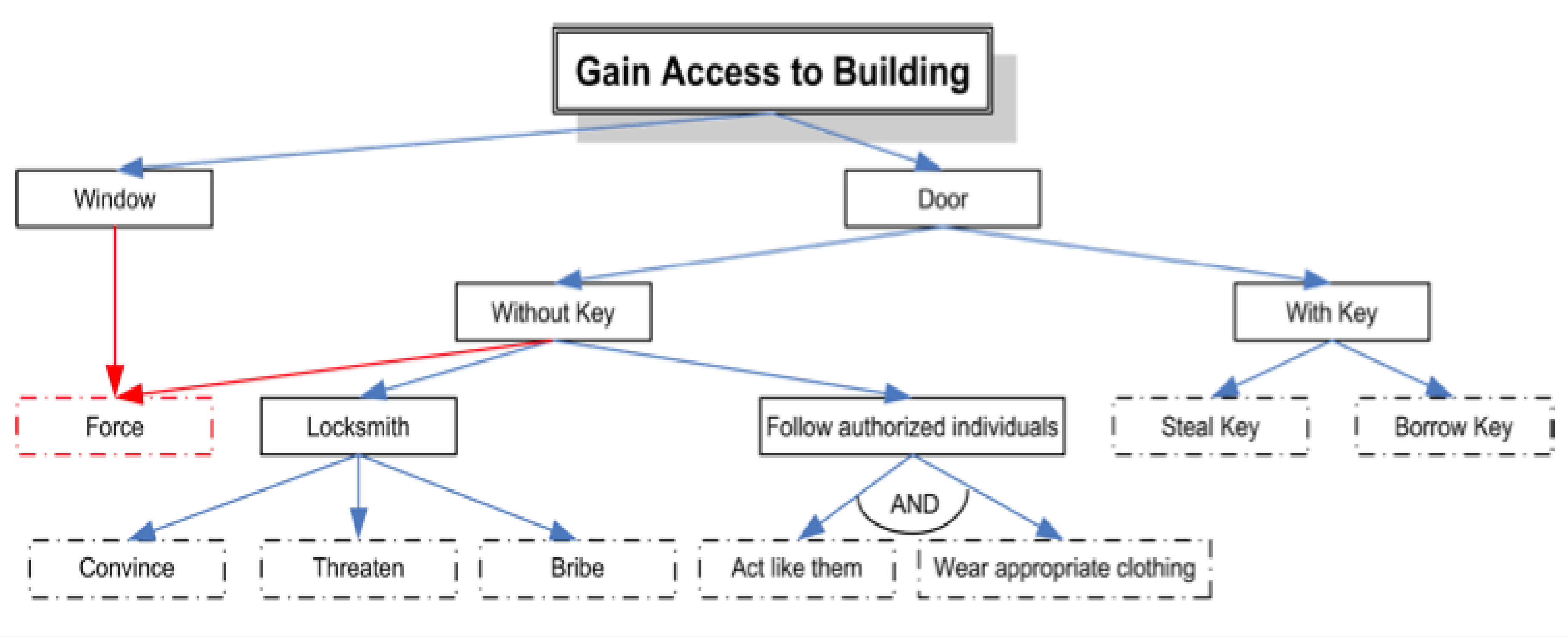
- ✓ Identify ASSETS
- ✓ Define the ATTACK SURFACE
- ✓ Decompose the SYSTEM
- ✓ Identify ATTACK VECTORS
- ✓ List THREAT ACTORS (W&W)

II. Implementation

- ✓ Analysis & assessment
- ✓ Triage
- ✓ Controls

Covers critical security controls (SANS / ISO27001)

Attack Modeling



Gain Access to Building

Window

Door

Without Key

With Key

Force

Locksmith

Follow authorized individuals

Steal Key

Borrow Key

AND

Convince

Threaten

Bribe

Act like them

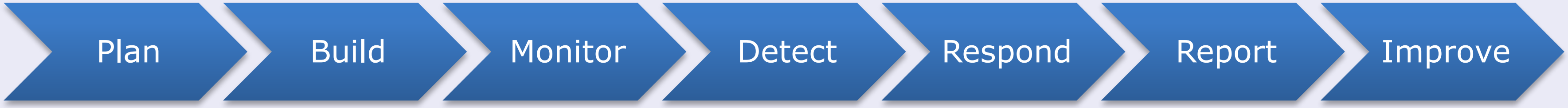
Wear appropriate clothing

Recon → Weaponize → Deliver → Exploit → Install → Command → Action

Tree source: "Design and Implementation of a Support Tool for Attack Trees", Alexander Opel

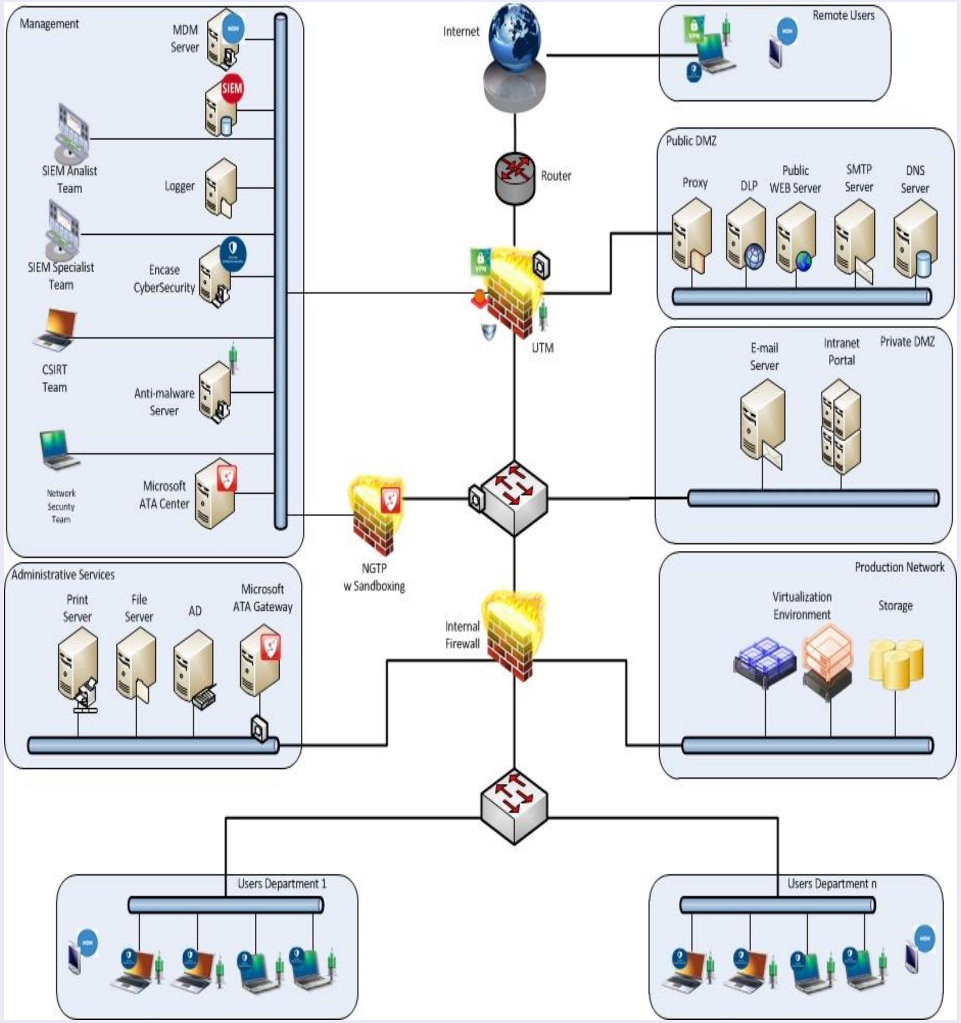
Defense Cycle – CMMI Approach

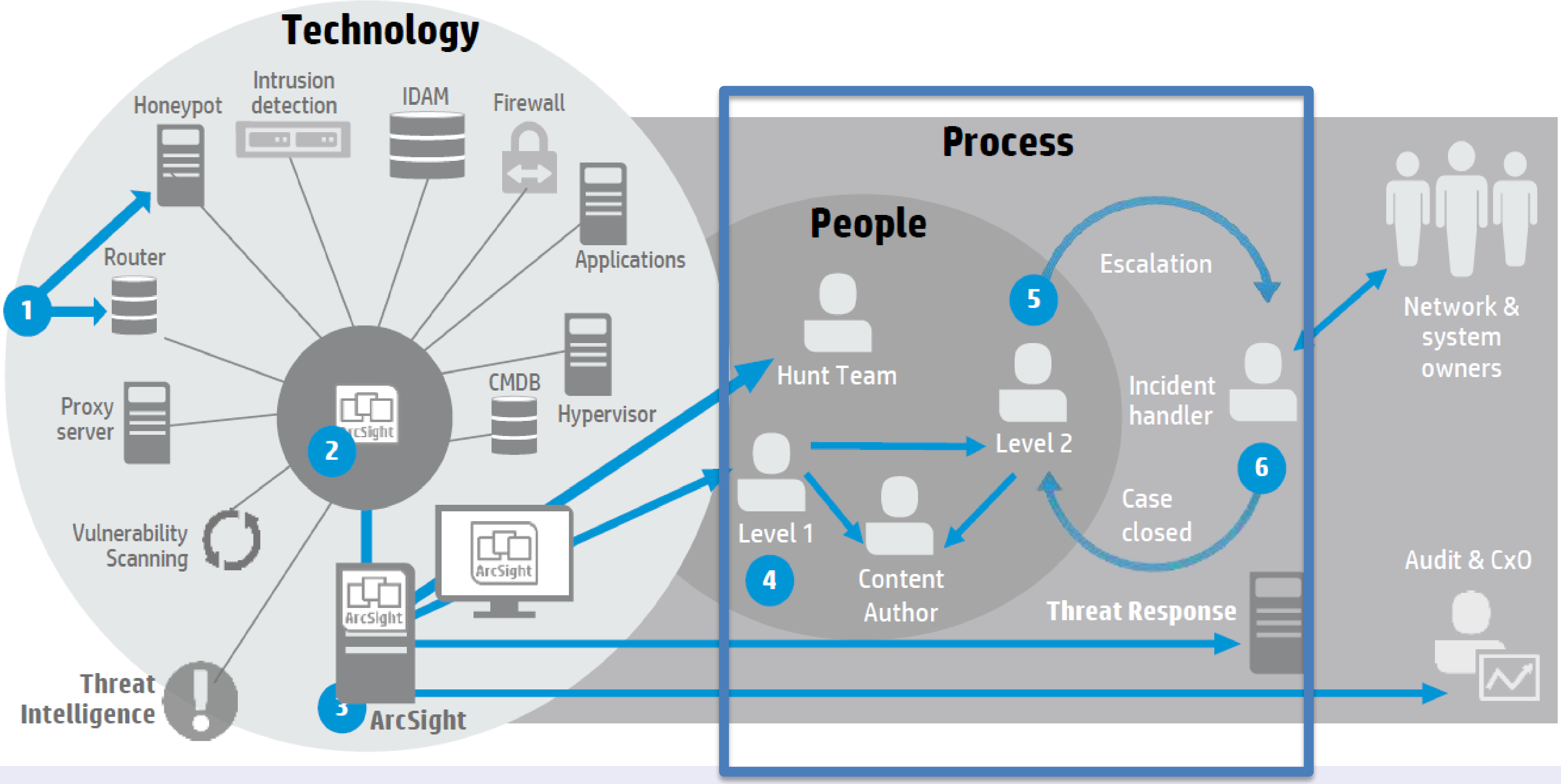
- **Plan** – what to protect, what are your assets, policies, what type of protective controls. What data sources.
- **Build** – acquire competencies, build skills specialists, acquire tools (after teams). Implement the solutions in your company
- **Monitor** – operate the technical solutions have operational NSM/SIEM systems, perform reviews and drills (incident response exercises)
- **Detect** – check the output of monitoring systems, validate the alerts and do proactive search of IoA (indicators of attack)
- **Respond** – exercise the incident response plans; investigate, contain and remediate
- **Report** – gather information, analyze it, communicate to the right people
- **Improve** – keep the tools, procedures and processes in a maturing loop



3. Defence Best Practices

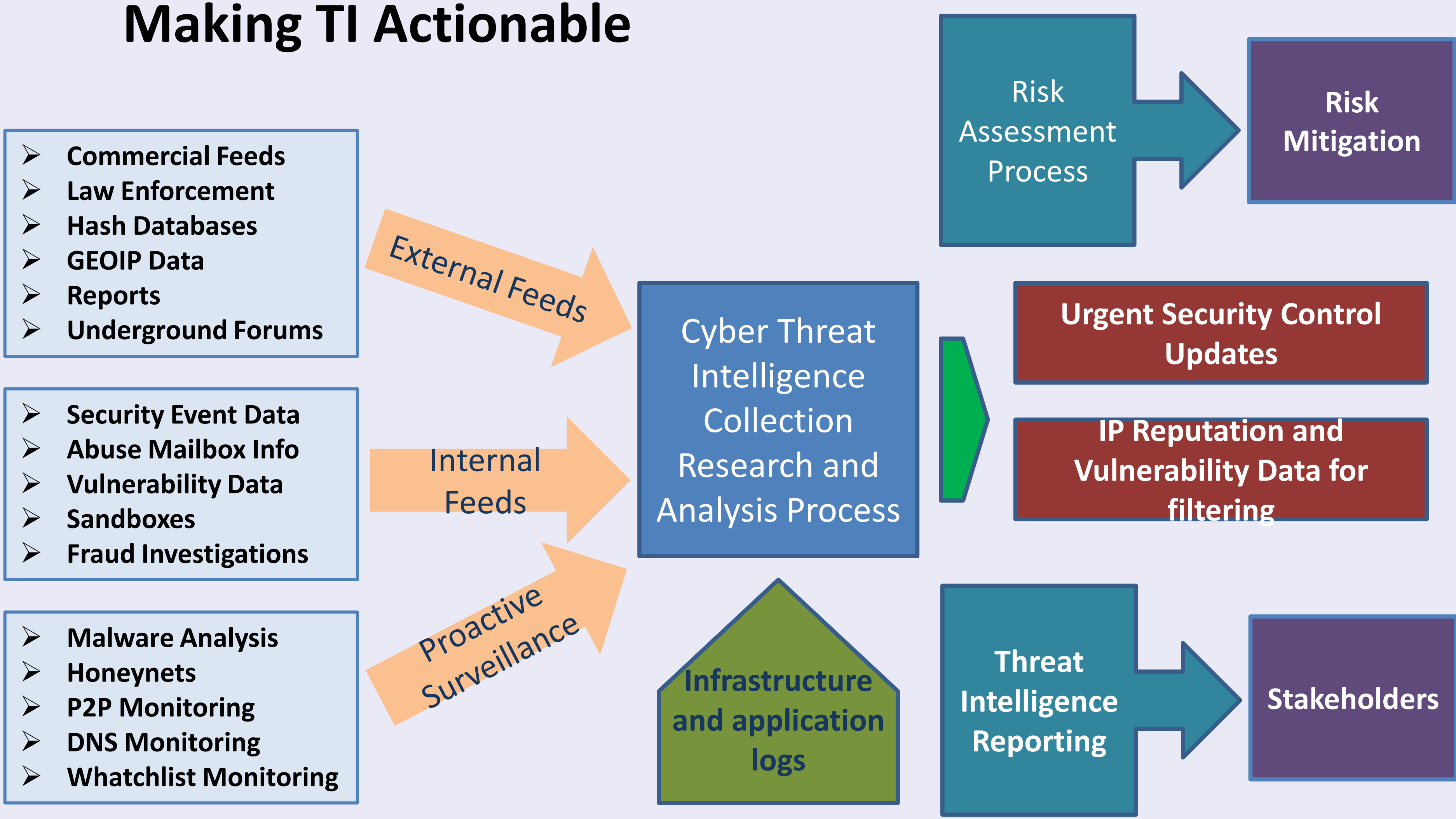
- ✓ Covers critical security controls (SANS / ISO27001)
- ✓ Features modern NGGW / NGIPS / NGTP
- ✓ Features ATA with sandboxing before ETD
- ✓ Has information security mechanisms implemented (DLP/DRM)
- ✓ Has central SIEM with solid TI & integrated with (automated) IR
- ✓ Has account activity monitoring (e.g. MS ATA, Rapid7 UserInsight)





Source: HP Security

Making TI Actionable



- Commercial Feeds
- Law Enforcement
- Hash Databases
- GEOIP Data
- Reports
- Underground Forums

External Feeds

- Security Event Data
- Abuse Mailbox Info
- Vulnerability Data
- Sandboxes
- Fraud Investigations

Internal Feeds

- Malware Analysis
- Honeynets
- P2P Monitoring
- DNS Monitoring
- Whatchlist Monitoring

Proactive Surveillance

Cyber Threat Intelligence Collection Research and Analysis Process

Infrastructure and application logs

Risk Assessment Process

Risk Mitigation

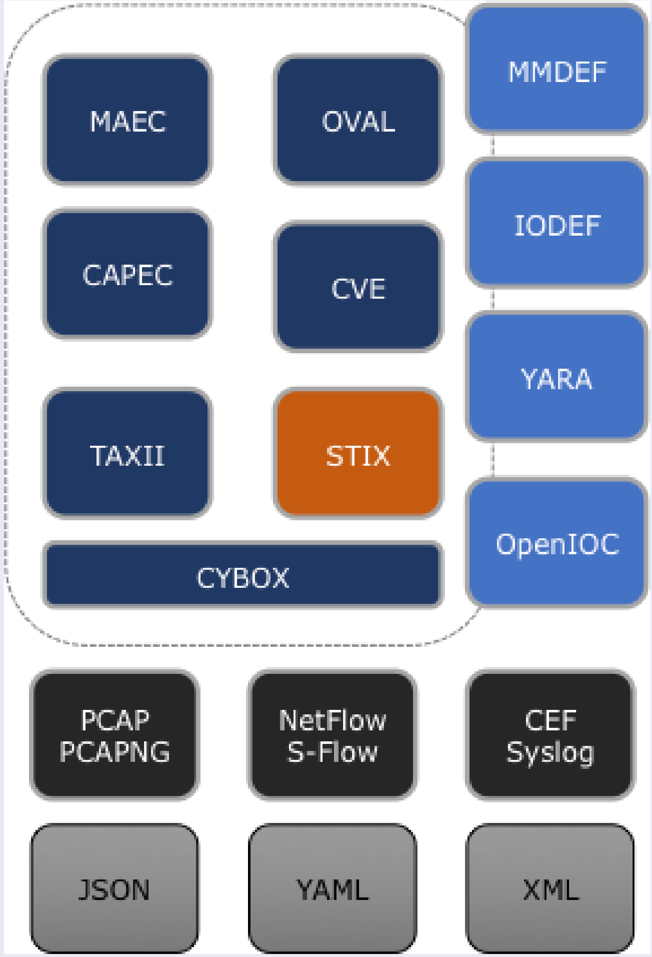
Urgent Security Control Updates

IP Reputation and Vulnerability Data for filtering

Threat Intelligence Reporting

Stakeholders

TI Frameworks / Formats



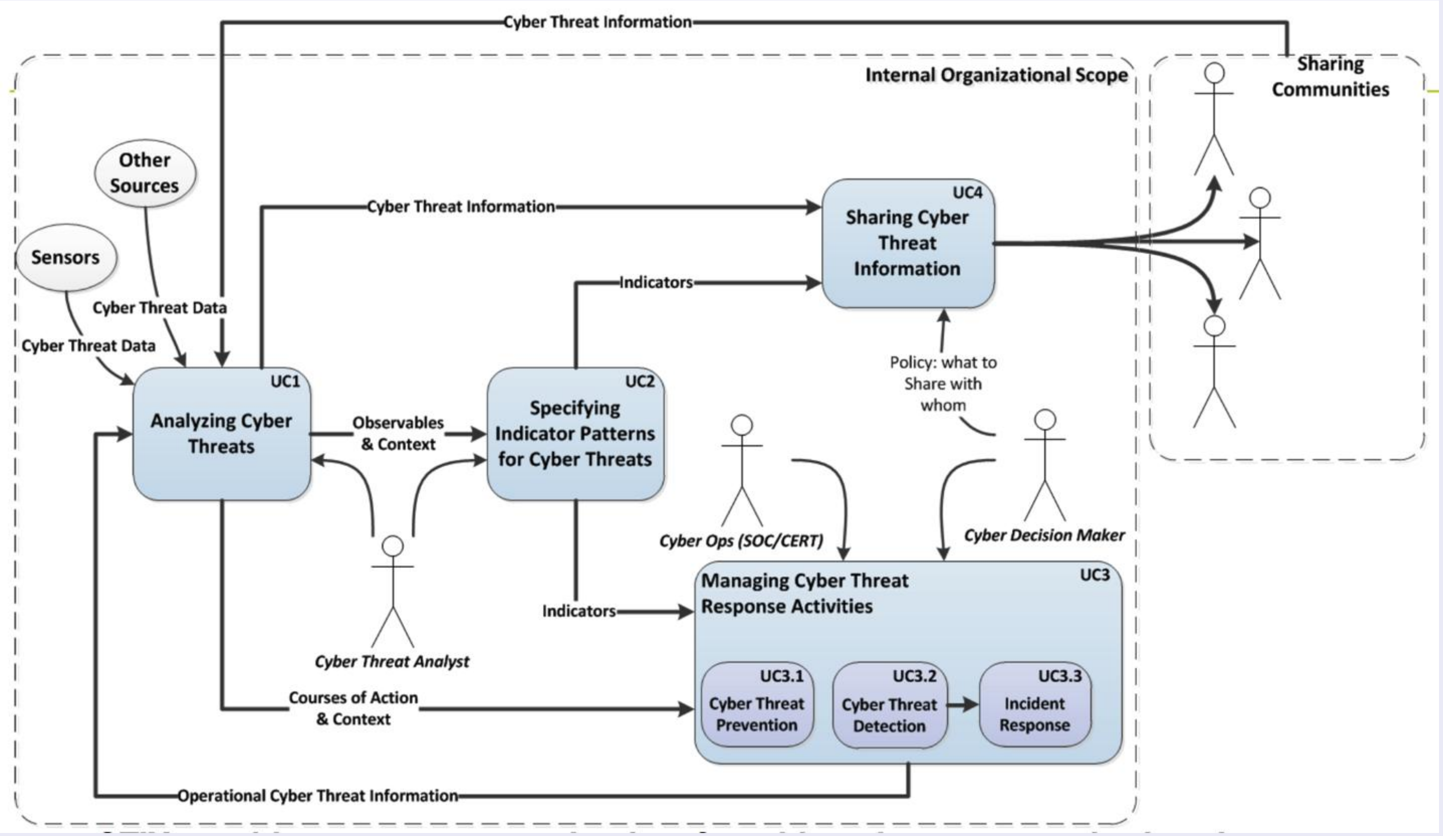
Indicators

- **STIX** – Structured Threat Information eXpression (MITRE/OASIS)
- **TAXII** – Trusted Automated eXchange of Indicator Information (MITRE/OASIS)
- **CYBOX** – Cyber Observable eXpression (MITRE/OASIS)
- **OpenIOC** – Open Indicators of Compromise (FireEYE/Mandiant)
- **IODEF** – Incident Object Description Exchange Format (IETF – RFC5070).
- **YARA** - Yet Another Regex Analyzer – binary pattern scanning (OSS)
- **SNORT** - real-time analysis of network traffic (CISCO).

Enumerations

- **MMDEF** - Malware Metadata Exchange Format (IEEE)
- **MAEC** - Malware Attribute Enumeration and Characterization (MITRE).
- **CAPEC** – Common Attack Pattern Enumeration and Classification (MITRE).
- **CVE** - Common Vulnerabilities and Exposures (MITRE)
- **CVSS** - Common Vulnerability Scoring System (NIST)
- **CPE** – Common Platform Enumeration (NIST)
- **OVAL** - Open Vulnerability and Assessment Language (MITRE)
- **OSVDB** - Open Sourced Vulnerability Database (OSF)

Threat Intel Frameworks - STIX



- **STIX** - a language for the characterization and communication of **cyber threat information**

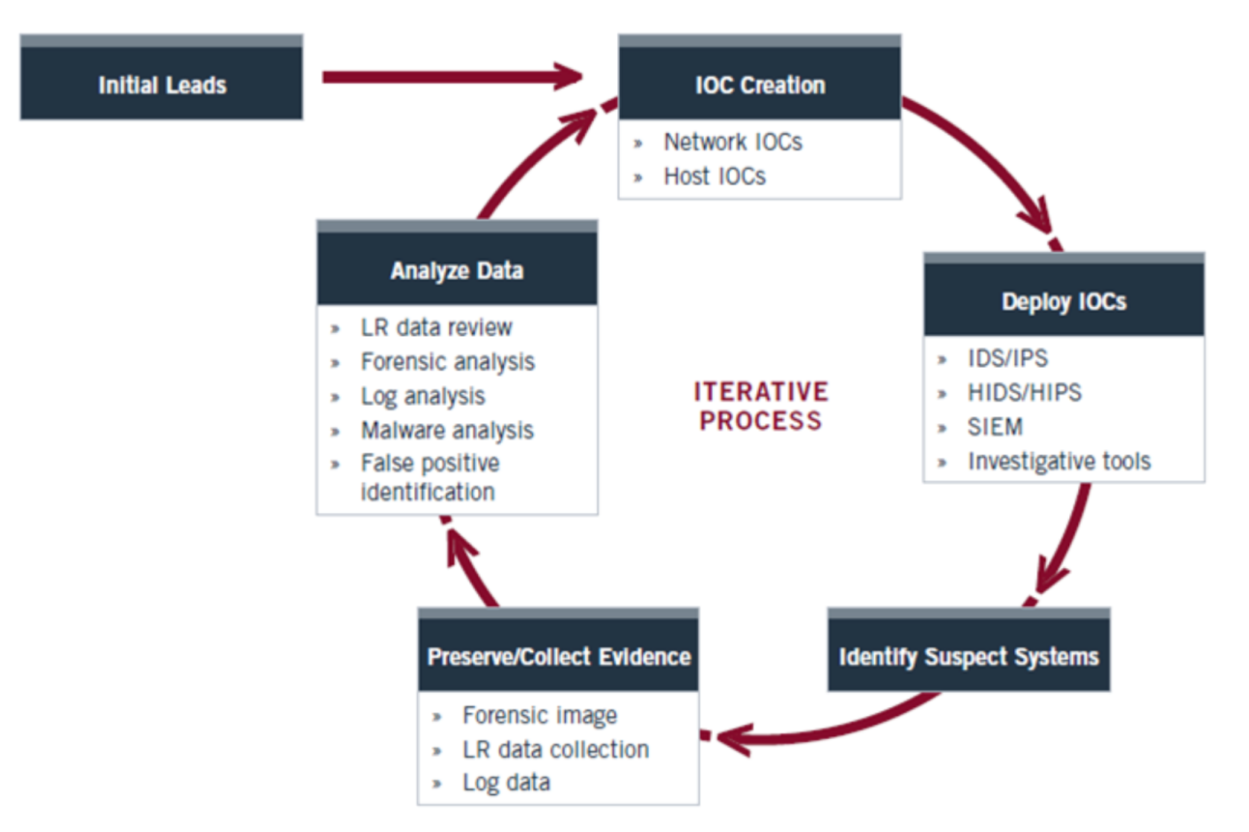
  expressive, flexible, extensible, automatable, and human-readable

  CybOX - convey specific instances of cyber observation (either **static** or **dynamic**) or **patterns** of what could potentially be observed.

Source: MITRE Org - https://stix.mitre.org

OWASP
The Open Web Application Security Project

Threat Intel – IR Lifecycle with IOCs



Investigative Lifecycle:

- Initial Evidence
- Create IOCs for Host&Network
- Deploy IOCs in the Enterprise – e.g. IDS/SIEM
- Identify Additional Suspect Systems
- Collect Evidence
- Analyze Evidence
- Refine & Create new IOCs

Source: "An Introduction to OpenIOC", Mandiant

Defense Security Metaphor

Centered, Deep

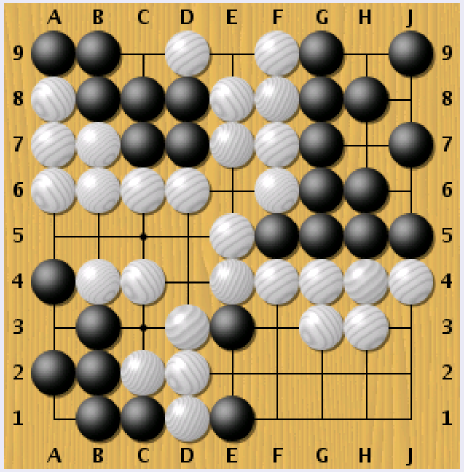
White moves first

Main strategic focus: the center, open fields
Objective: overwhelming attack (mate)
Asymmetric defense: obstruct
Key ability: master complexity / deep planning

Fluid, Responsive

Black moves first

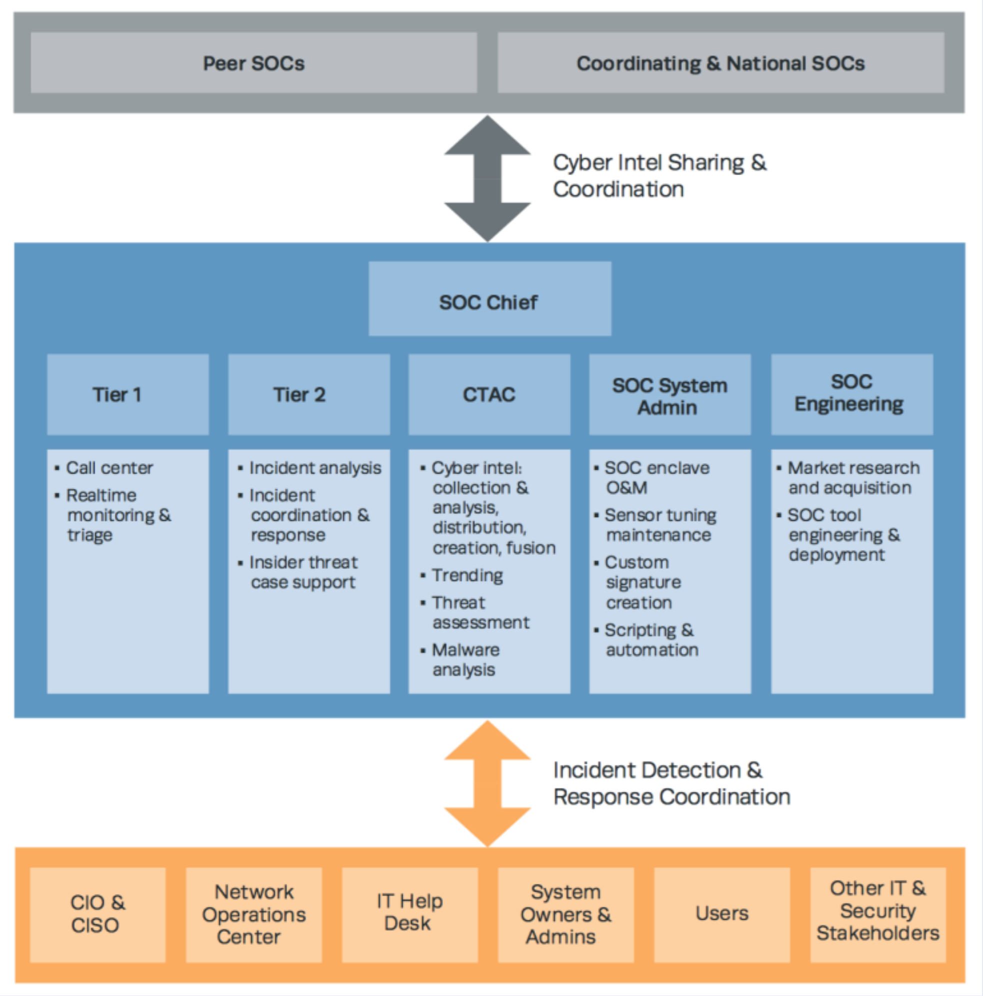
Main strategic focus: the corners, key points
Objective: expand controlled territory
Asymmetric-game: extra steps
Key ability: understand the threat, react timely



4. Live Incident Response

IR Teams - Roles

- **Duty officer / Tier 1 Analyst –** takes care of all incoming requests**.** Ensure that all incidents have owners.
- **Triage officer / Tier 1 Analyst –** deal with the reported incidents, decides whether it is an incident and is to be be handled, and by whom
- **Incident handler / Tier 2 Incident Responder** – works on the incident: analyze data, create solutions, resolve the technical details and communicates about the progress to the manager and the constituents.
- **Incident handler / Tier 3 Subject Matter Expert –** advanced analyst that deals with complex cases that involve a cross-filed investigation.
- **Incident manager** – responsible for the coordination of all incident handling activities. Represents the team in communicating to the outside 3rd parties.



Peer SOCs

Coordinating & National SOCs

Cyber Intel Sharing & Coordination

SOC Chief

Tier 1	Tier 2	CTAC	SOC System Admin	SOC Engineering
▪ Call center ▪ Realtime monitoring & triage	▪ Incident analysis ▪ Incident coordination & response ▪ Insider threat case support	▪ Cyber intel: collection & analysis, distribution, creation, fusion ▪ Trending ▪ Threat assessment ▪ Malware analysis	▪ SOC enclave O&M ▪ Sensor tuning maintenance ▪ Custom signature creation ▪ Scripting & automation	▪ Market research and acquisition ▪ SOC tool engineering & deployment

Incident Detection & Response Coordination

CIO & CISO

Network Operations Center

IT Help Desk

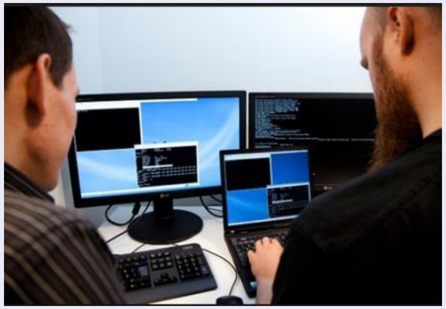
System Owners & Admins

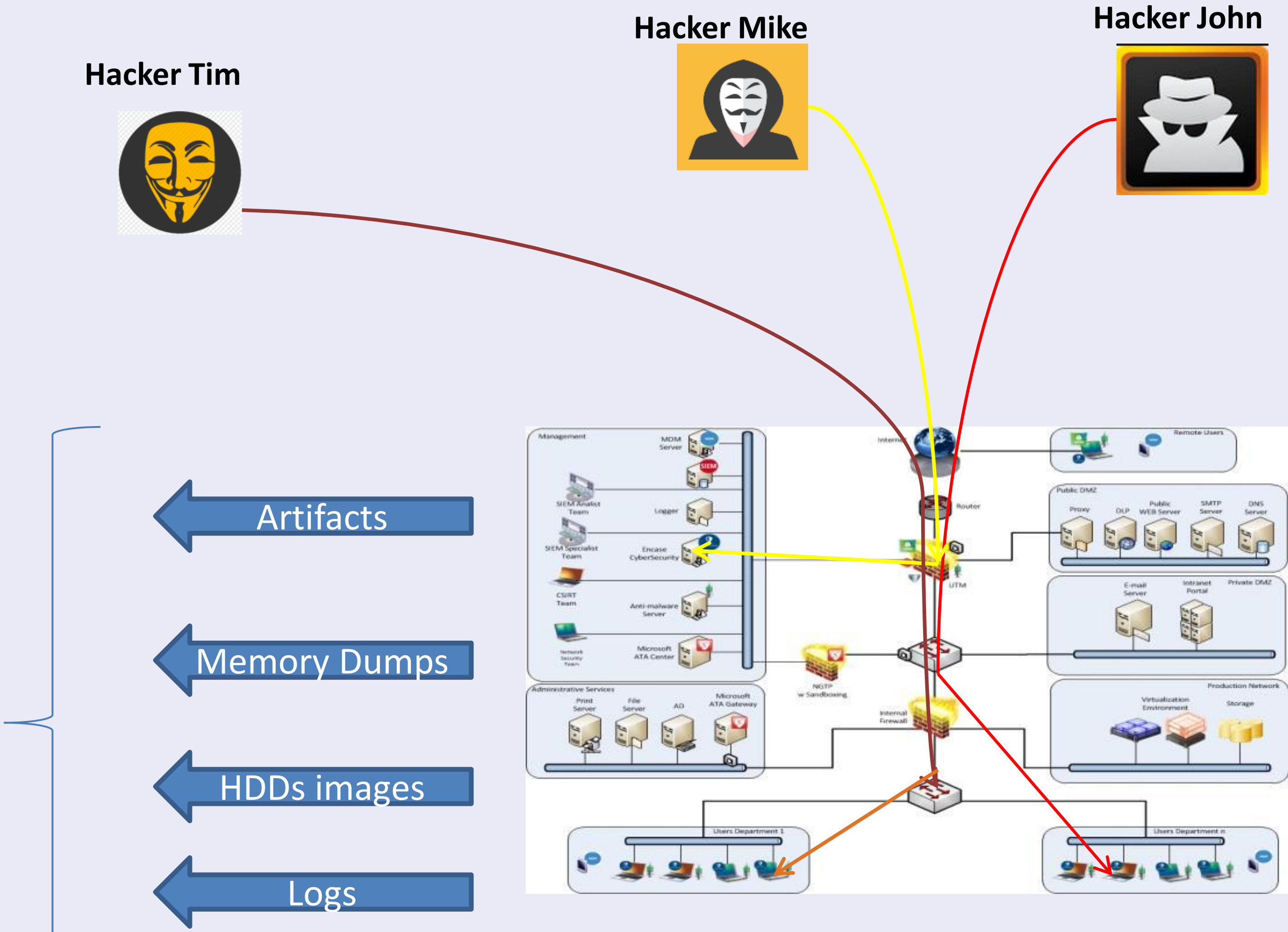
Users

Other IT & Security Stakeholders

Source: *"Ten Strategies of a World-Class Cybersecurity Operations Center"* (MITRE)

- ✓ Time pressure - fast response
- ✓ Many compromised systems
- ✓ Large amounts & different kinds of data





Hacker Tim

Hacker Mike

Hacker John

Artifacts

Memory Dumps

HDDs images

Logs

Heterogeneous network with hundreds systems

IR Pressure

- What is the extent of the incident?
- Is it still active? Should we stop or follow?
- What information was exposed/exfil?
- How did the attacker(s) get in?
- How do we stop the attack and remediate?
- What is the financial/non-fin impact?

Memory Forensics Advantages

- **Best place to identify malicious software activity**
  - ➢ Study running system
  - ➢ Identify inconsistencies in system
  - ➢ Bypass packers, binary obfuscations, rootkits.
- **Analyze recent activity on the system**
  - ➢ Identify all recent activity in context
  - ➢ Profile user or attacker activities
- **Collect evidence that cannot be found anywhere else**
  - ➢ Memory-only malware
  - ➢ Chat threads
  - ➢ Internet activities

1 • Identify rogue processes

2 • Analyze process DLLs and handles

3 • Review network artifacts

4 • Look for code injections

5 • Search for rootkits

6 • Dump suspicious processes and drivers

Volatility plugins			
apihooks	Find API hooks	procexedump	Dump a process to an executable file sample
connections	Print list of open connections	procmemdump	Dump a process to an executable memory sample
dlllist	Print list of loaded dlls for each process	pslist	print all running processes by following the EPROCESS lists
dlldump	Dump a DLL from a process address space	orphanthread	Locate hidden threads
files	Print list of open files for each process	mutantscan	Scan for mutant objects KMUTANT
getsids	Print the SIDs owning each process	pstree	Print process list as a tree
malfind	Find hidden and injected code	sockets	Print list of open sockets

Complete list: https://code.google.com/p/volatility/wiki/Plugins

5. Demo

Getting a quick hint with GRR & Volatility

1. Starting point: infection alert from SIEM
2. Get access on the machine – run GRR hunt
3. GRR fundamentals
4. Getting the basics – memory dump
5. Preliminary analysis with Volatility
6. Get artifacts for IOCs
7. What next? Mandiant IOC Editor

certSIGN® BY UTI

Thank you.

Teodor.Cimpoesu@certsign.ro
+40722.754.319, @cteodor

Cosmin.Anghel@certsign.ro
+40766.514.112

Incidents: CERT@uti.ro