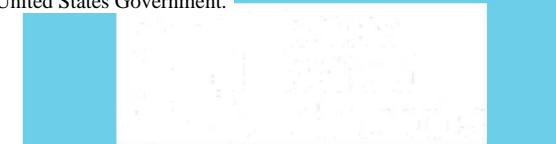


Threat Based Cybersecurity Investments



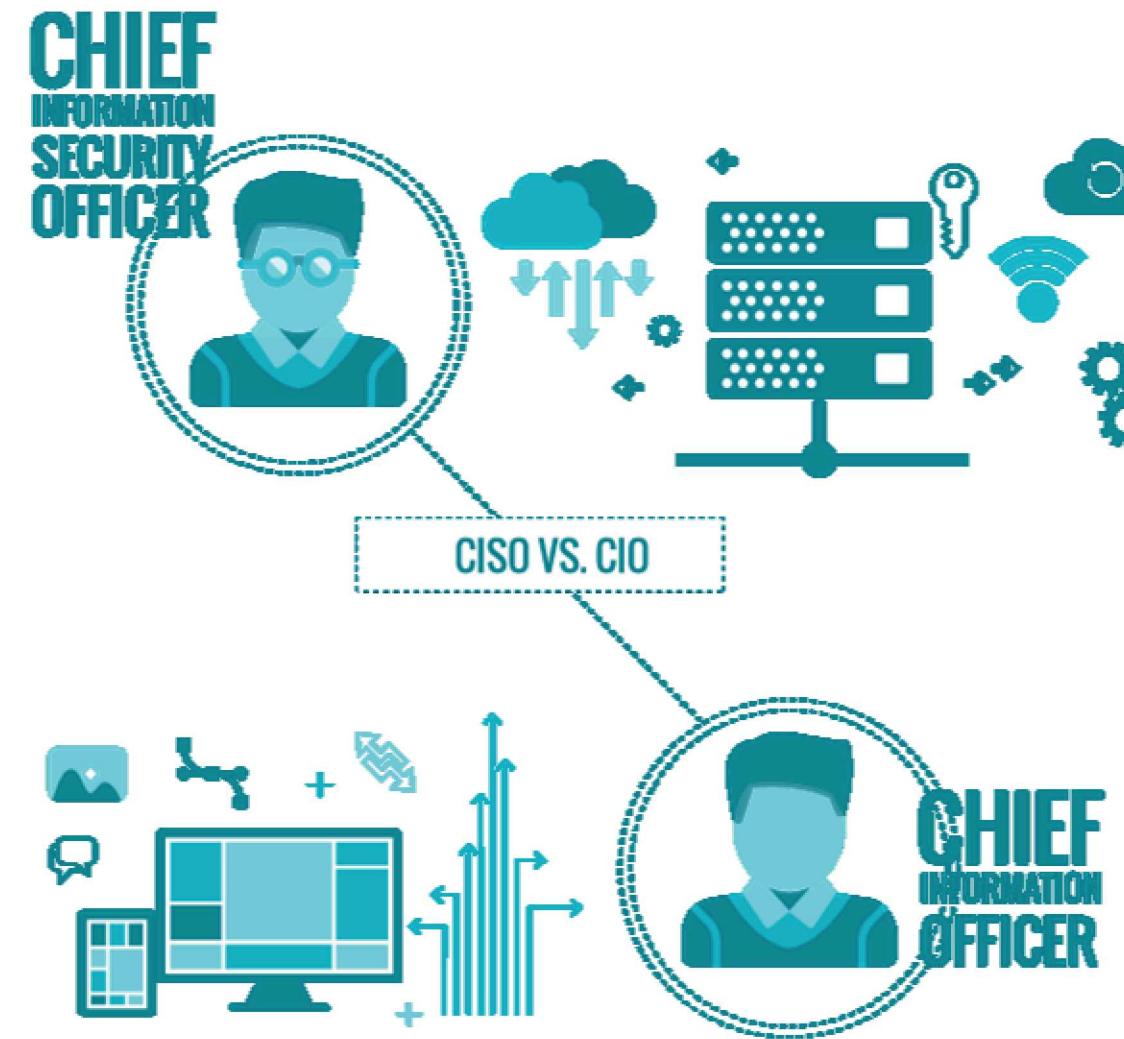
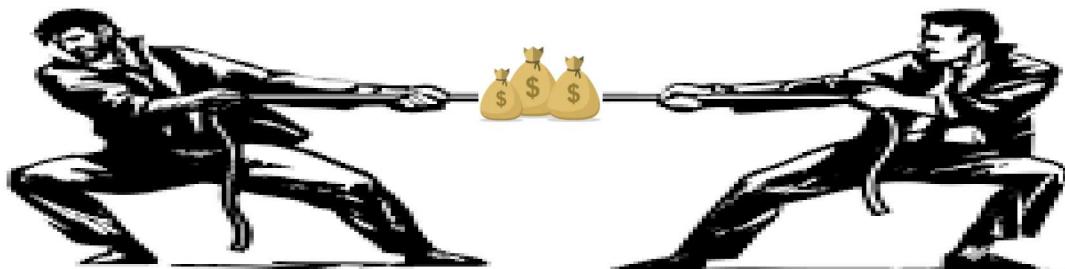
PRESENTED BY

ANITA BHAT



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

The Unfortunate Reality



Current Trends

Cybersecurity spending seems to be sky rocketing

According to Gartner, companies will spend \$124 Billion on cybersecurity in 2019¹

Data from Strategic Cyber Ventures²:

VC funding for 2018 was 5.3 billion

20% higher than 2017

80% higher than 2016

Predicted to exceed **ONE TRILLION DOLLARS by 2021!!!**

¹ <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

² <https://scvgroup.net/2018-cybersecurity-venture-capital-investment/>

Cost of Breaches

According to the Ninth Annual Cyber Crime Study by Accenture and the Ponemon Institute published on March 6, 2019³:

The average cost of cybercrime for an organization is now \$13.0 million.

ORGANIZATIONS SPEND MORE THAN EVER DEALING WITH THE COSTS AND CONSEQUENCES OF INCREASINGLY SOPHISTICATED ATTACKS

Cost of cybercrime is rising

\$11.7m → \$13.0m +12% =72%

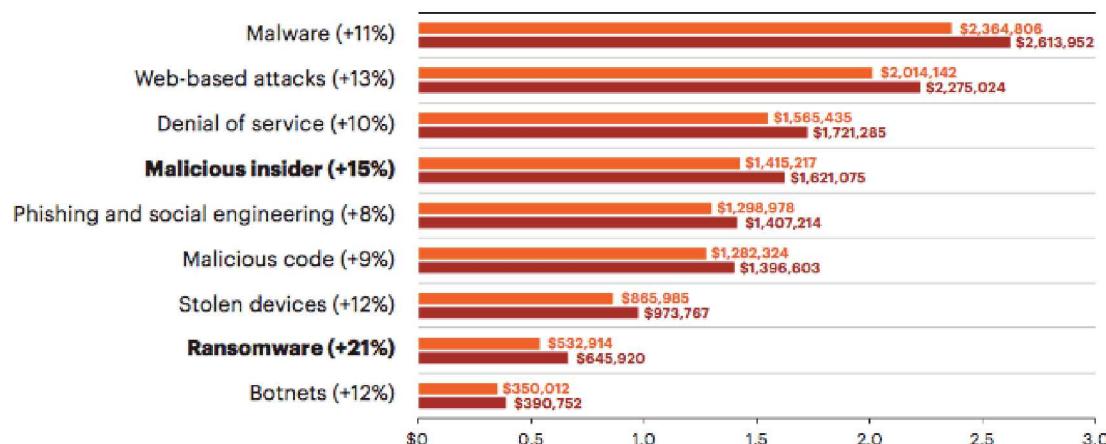
Average cost of cybercrime in 2017

Average cost of cybercrime in 2018

Increase in the last year

Increase in the last 5 years

People-based attacks have increased the most



Business consequences are expensive

\$4.0m

Cost of business disruption

\$5.9m

Cost of information loss

36%

Proportion of spend on discovering attacks in 2018



WHAT HAVE WE BEEN DOING?

Compliance-Based Cybersecurity!!!



WHAT DO WE NEED TO DO?



Think like the Adversary!

Move from Compliance to Threat-Based Risk Management



Compliance



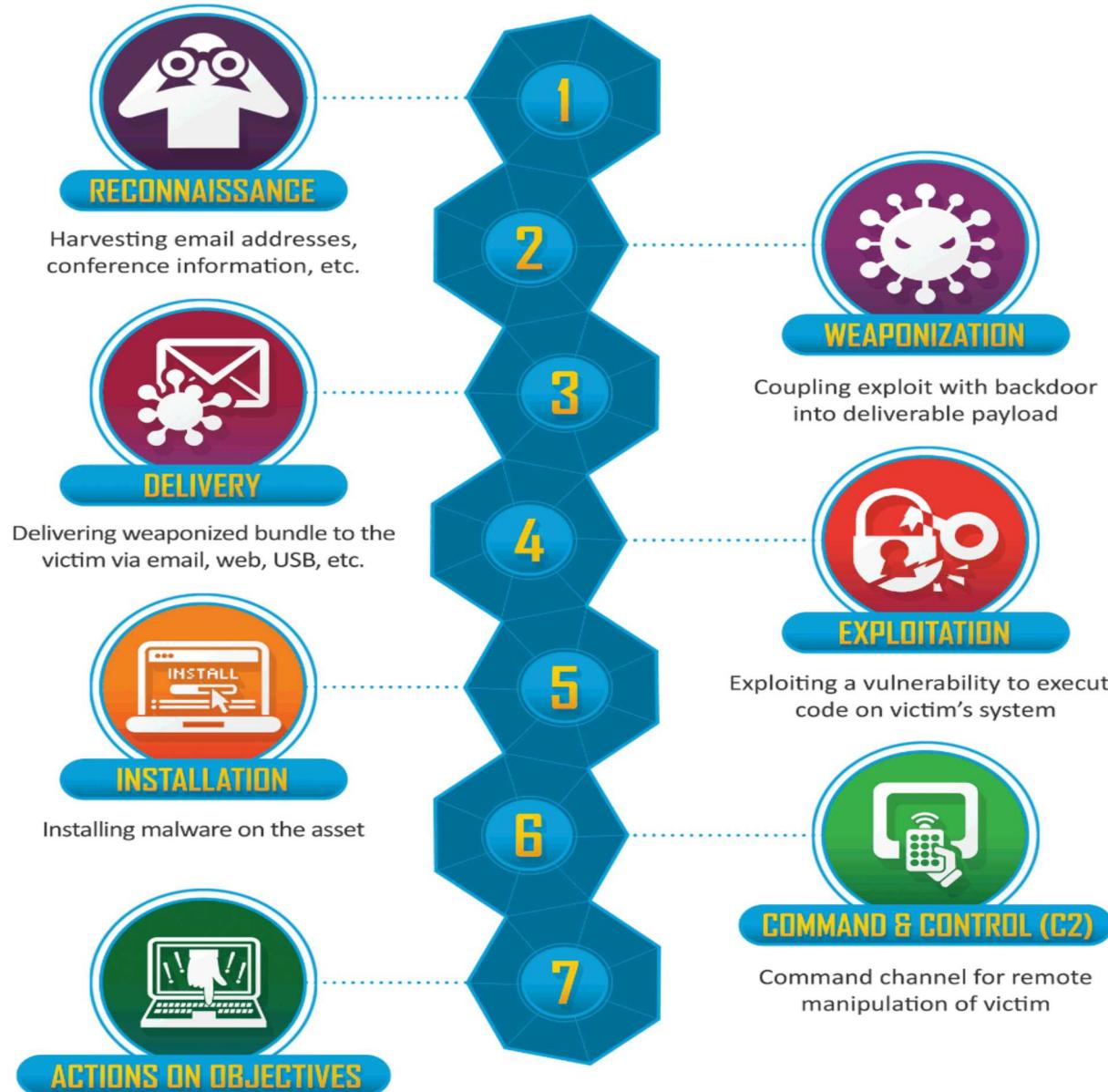
There Are Several Threat Frameworks to Choose From

- NIST – Special Publication 800-30 (Guide for conducting Risk Assessments) - Appendix E
- Lockheed Martin's Kill Chain
- MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)
- NSA Technical Cyber Threat Framework (NTCTF) v2

Appendix E lists Threat Events

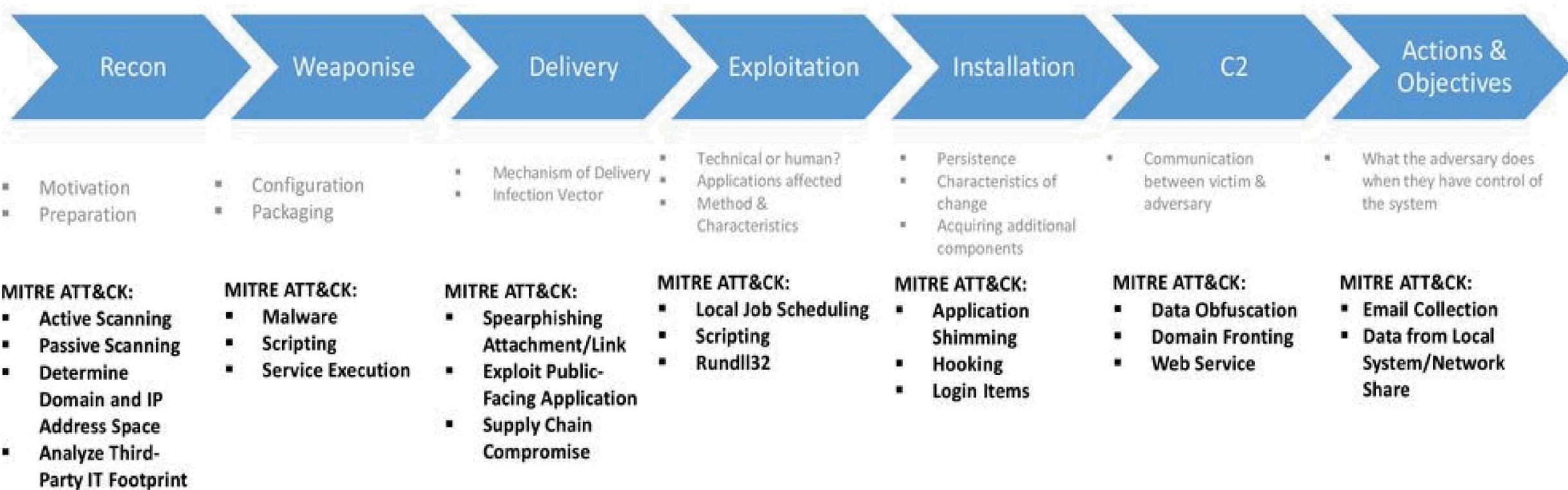
- Perform perimeter network reconnaissance/scanning.
- Perform network sniffing of exposed networks.
- Craft phishing attacks.
- Craft counterfeit certificates
- Deliver malware to information systems
- Exploit split tunneling
- Conduct wireless jamming attacks
- Conduct Denial of Service attacks
- ...
- ...
- ...

Lockheed Martin's Kill Chain



MITRE ATT&CK MATRIX

- Builds on the Kill Chain
- Provides deeper level of granularity



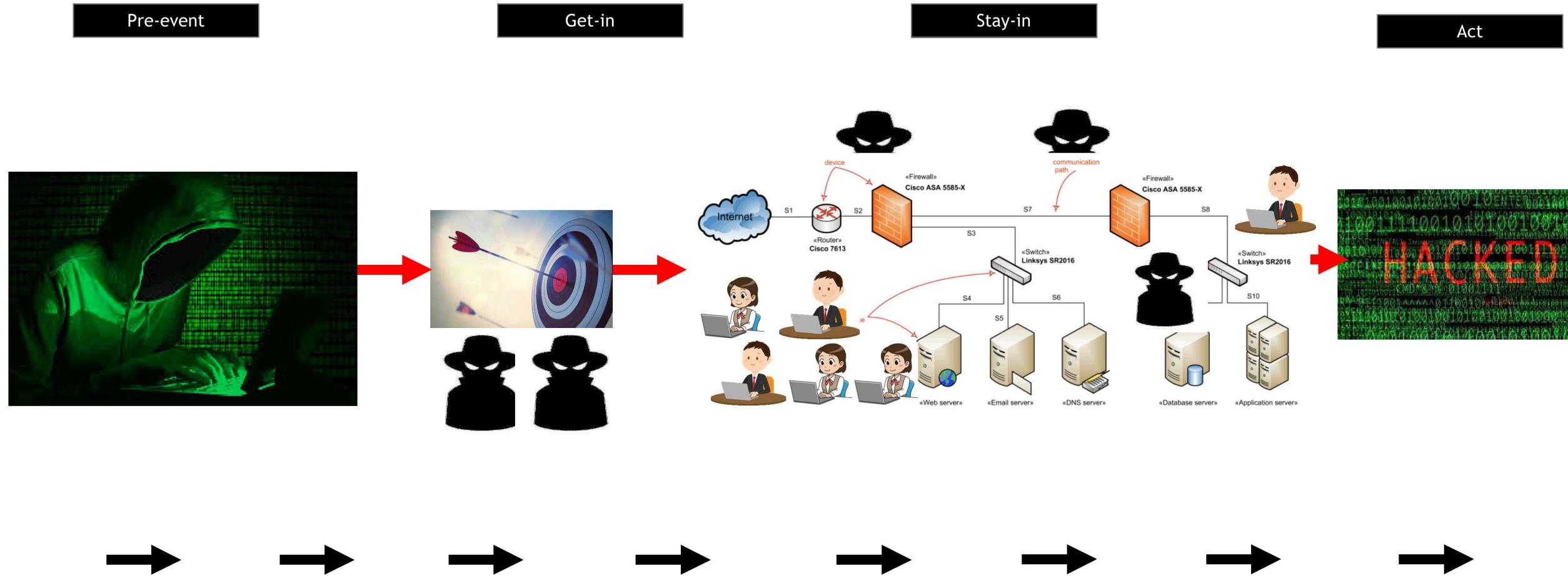
NSA Technical Cyber Threat Framework (NTCTF) v2 *

(13 November 2018)

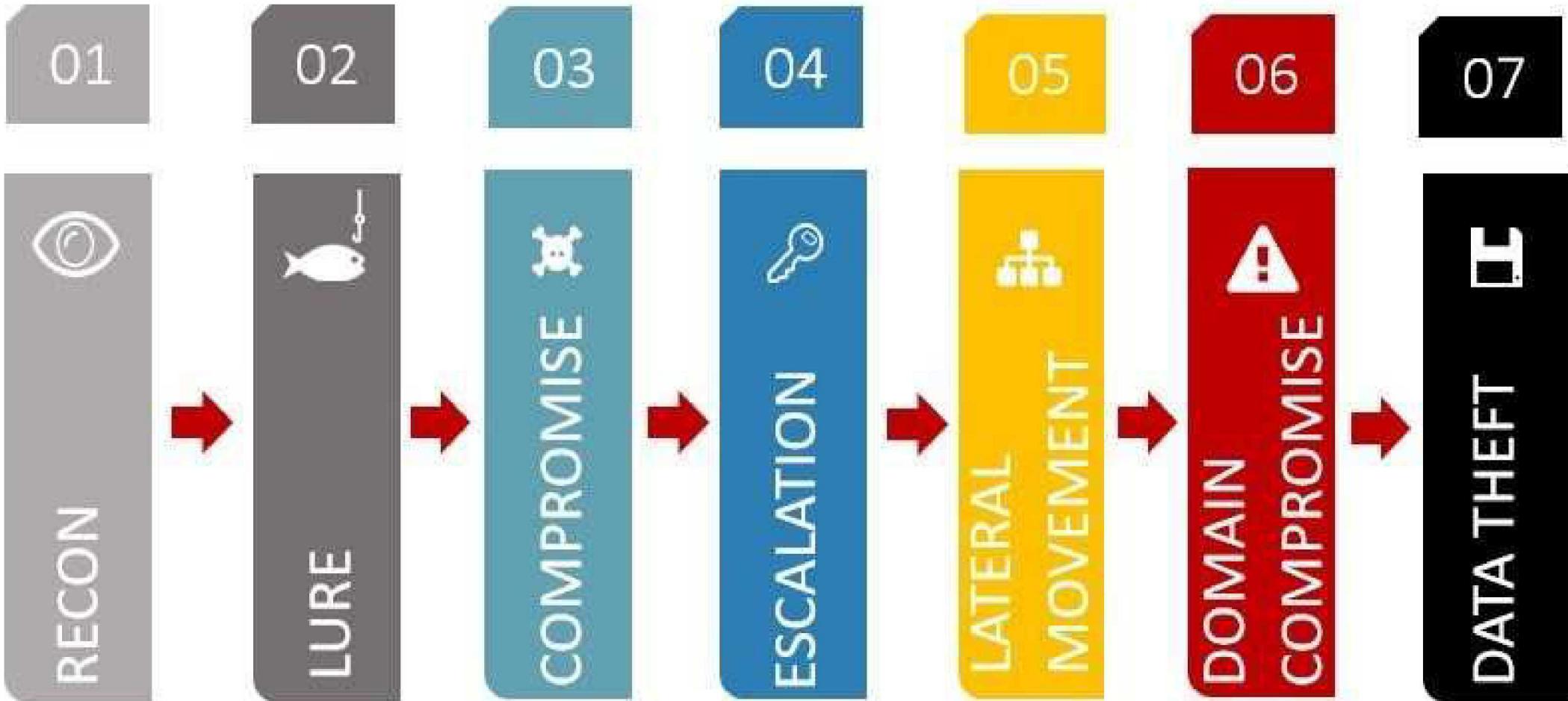
NSA/CSS Technical Cyber Threat Framework (NTCTF v2)

Administration	Engagement	Presence	Presence	Effect	Ongoing Processes
Planning	Delivery	Execution	Credential Access	Monitor	Analysis, Evaluation, and Feedback
Analyze operation Determine strategy and goals Issue operational directive Produce operational plans Receive approval to execute operations Select intended victims	Access via wireless Alter communications path Compromise supply chain or trusted source Connect removable media Connect rogue network devices Infect via websites Inject database command Leverage device swapping Send malicious email Transport via common network infrastructure Traverse CDS or MLS Use chat services Use compromised host Use legitimate remote access Use physical network bridge	Create scheduled task Execute via service controller Execute via third-party software Inject into running process Leverage authorized user Replace existing binary Run commands in shell Run fileless payload Use interpreted scripts Use OS APIs Use remote services Use trusted application to execute untrusted code Write to disk	Add or modify credentials Conduct social engineering Crack passwords Dump credentials Hijack active credential Locate credentials Log keystrokes	Activate recording Collect passively Enable other operations Log keystrokes Maintain access Take screen capture	Abandon infrastructure Conduct effects assessments Retire potential victims
Resource Development			Log keystrokes	Exfiltrate	Command and Control
Acquire operational infrastructure Build alliances and partnerships Create botnet Develop capabilities Obtain financing Seed supply chain Staff and train resources			Exploit peer connections Logon remotely Pass the hash Pass the ticket Replicate through removable media Taint shared content Use application-deployment software Use remote services Write to remote file shares Write to shared webroot	Collect crosstalk Collect from local system Collect from network resources Compress data Disclose data or information Position data Run collection script Send over C2 channel Send over non-C2 channel Send over other network medium Throttle data Transfer via physical means Traverse CDS or MLS	Beacon to midpoints Establish peer network Relay communications Send commands Use botnet Use chained protocols Use peer connections Use remote shell Use removable media
Research	Exploitation				Evasion
Gather information Identify capability gaps Identify information gaps	Abuse protocols Access virtual memory Conduct social engineering Defeat encryption Exploit firmware vulnerability Exploit local application vulnerability Exploit OS vulnerability Exploit remote application vulnerability Exploit weak access controls Hijack Impersonate or spoof user Launch zero-day exploit Leverage exploit packs Leverage trusted relationship Replay	Enumerate accounts and permissions Enumerate file system Enumerate local network connections Enumerate local network settings Enumerate OS and software Enumerate processes Enumerate windows Map accessible networks Scan connected devices Sniff network			Access raw disk Avoid data-size limits Block indicators on host Degrade security products Delay activity Employ anti-forensics measures Employ anti-reverse-engineering measures Employ rootkit Encode data Encrypt data Impersonate legitimate file Manipulate trusted process Mimic legitimate traffic Modify malware to avoid detection Obfuscate data Remove logged data Remove toolkit Sign malicious content Store files in unconventional location Tailor behavior to environment Use signed content
Preparation		Internal Reconnaissance	Persistence	Modify	
Reconnaissance					
Conduct social engineering Gather credentials Identify crosstalk Map accessible networks Scan devices Scrape websites Select potential victims Survey devices Use social media			Create new service Create scheduled task Edit boot record Edit file-type associations Employ logon scripts Leverage path-order execution Modify BIOS Modify configuration to facilitate launch Modify existing services Modify links Modify service configuration Replace service binary Set to load at startup Use library-search hijack	Alter data Alter process outcomes Cause physical effects Change machine-to-machine communications Change run-state of system processes Delete websites Delete encryption	
Staging		Privilege Escalation		Deny	
Add exploits to application data files Allocate operational infrastructure Create midpoints Establish physical proximity Infect or seed website Pre-position payload				Corrupt files or applications Degrade Disrupt or denial of service Encrypt data to render unusable	
		Legend		Destroy	
		Stage		Brick disk or OS (full delete)	
		Objective		Corrupt disk or OS (partial delete)	
		Action		Delete data	
				Destroy hardware	

Lifecycle of a Threat



What Actually Happens



Anatomy of a Threat

The NSA Technical Cyber Threat Framework depicts threats in layers:

1. **Stages:** The progression of cyber threat actions over time to achieve objectives
2. **Objectives:** The purpose of conducting an action or a series of actions
3. **Actions:** and associated resources used by an threat actor to satisfy an objective
4. **Indicators:** Discrete cyber threat intelligence data (company x reported to have created malware y)

Layers of a Threat

The NSA Technical Cyber Threat Framework depicts threats in three layers:

1. Stages:

- Pre-Event
- Get-in
- Stay-in
- Act

2. Each Stage has different Objectives

3. Each Objective has several Actions used to fulfill the Objective

4. Indicators or intelligence data that can be specific about adversary actions

Pre-Event Stage

Objective: Intent / Resource Development

Action: Intent/Resource Development

Objective: Reconnaissance / Staging

Action: Crawling Internet Websites

Action: Network Mapping (e.g. NMAP)

Action: Social Media

Action: Mid-points

Action: Vulnerability Scans

Objective: Weaponization

Action: Add Exploits to Application Data Files

Get-In Stage

Objective: Delivery

Action: Spear-phishing Emails w/ Attachments or w/ Malicious Link

Action: Websites

Action: Removable Media (i.e. USB)

Action: SQL Injection

Action: Virtualization Attacks

Action: DNS/Cache Poisoning

Action: ...

Objective: Initial Compromise / Exploitation

Action: Targets Application Vulnerability

Action: Target Operating System Vulnerability

Action: Targets Web Application Vulnerabilities (ex. XSS, CSRF)

Action: Trojan

Action: Exploit Weak Access Controls

Action: Defeat Encryption

Installation

Action: Writing to Disk

Action: In Memory Malware

Action: Replace Legitimate Binary with Malicious

Stay-In Stage

Objective: Persistence

- Action: Legitimate Credentials
- Action: Automatic Loading at Startup
- Action: Path Interception
- Action: Link Modification
- Action: Hypervisor Rootkit
- Action: Modify Existing Services
- Action : ...

Objective: Privilege Escalation

- Action: Process Injection
- Action: Credential Access
- Action: Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software)
- Action: ...

Objective: Defense Evasion

- Action: Binary Padding
- Action: Disabling Security Tools
- Action: Indicator Blocking
- Action: File Deletion
- Action: ...

Stay-In Stage

Objective: Credential Access

- Action: Credential Dumping
- Action: User Interaction
- Action: Network Sniffing
- Action: Password Recovery
- Action: ...

Objective: Host Enumeration

- Action: Account/File System/Permissions/Network/OS/Process Enumeration

Objective: Lateral Movement

- Action: Remote Services
- Action: Peer Connections
- Action: Remote Interactive Logon
- Action: Shared Webroot
- Action: ...

Objective: Command & Control

- Action: Commonly Used Port
- Action: Standard /Custom Application Layer Protocol
- Action: Peer Connections
- Action: Multiband Communications

Act Stage

Objective: Collection

Objective: Monitor / Exfiltration

Action: Exfil over C2 Channel

Action: Exfil over Network Resources

Action: Scheduled Transfer

Action: Exfil over Physical Medium

Action: ...

Objective: Alter/Deceive

Action: Full Data Deletion

Action: Denial of Service

Action: Cause Physical Effects

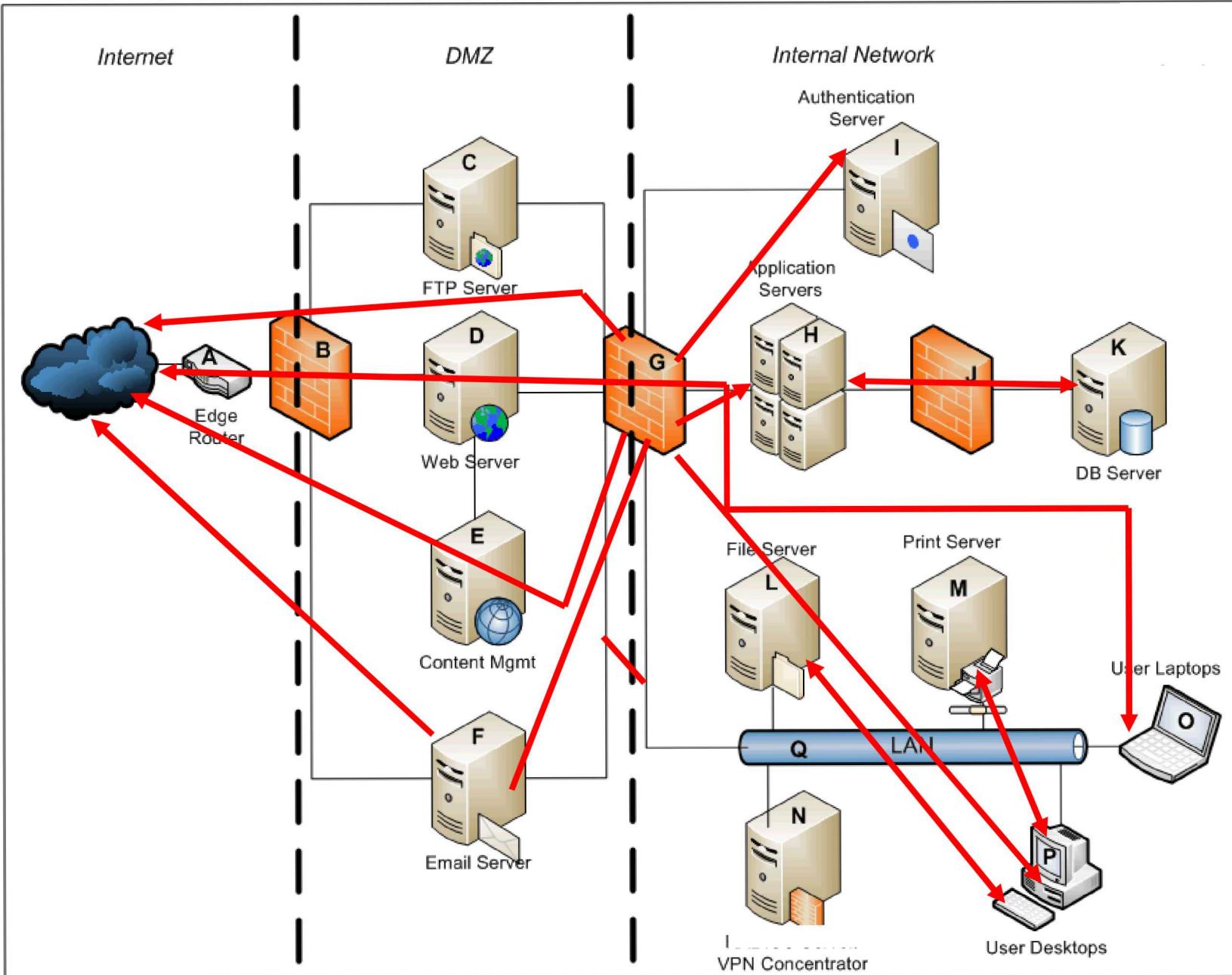
Action: ...

Applying the Threat Framework to Target Architecture

How do you evaluate how these threats affect your architecture?

Architectural features to consider:

- Traffic Flows
- Security Capabilities along those Flows
- Enumerate Security Capabilities
- Score each Capability against each Threat Action for its ability to Protect / Detect / Respond to the threat action



Exemplar Security Capabilities

- Next Generation Firewall
- SIEM
- Web Content Filtering
- Sand Boxing
- Virtual Desktop Infrastructure
- Inbound/Outbound SMTP Proxy
- Use of a Content Delivery Network
- Remote Access VPN
- DNS Proxy for inbound Queries
- Network Segmentation
- Network Access Control
- Host IPS
- Device Health Check
- Application Whitelisting
- Etc

Scoring

				Stage					
				Objective					
				Threat Action Y			Threat Action z		
				Protect			Protect		
				Detect			Detect		
				Respond			Respond		
Capabilities	Detailed Capability Description	Is Enhanc	% Scoring Complete	Threat Action Description			Threat Action Description		
Layer1									
A	Description			M	M	S	None	None	L
Rationale				P/D has some allowed paths. All actions are logged			Threat action is permitted but logged. Logs only persist 1 week		
Layer2									
B	Description			N/A	N/A	N/A	L	L	L
Rationale			0%				only covers one possible vector		
B (Enhancement)	Description			N/A	N/A	N/A	M	M	M
Rationale			0%				coverage include additional but not all vectors		

Coverage Map



So What?

2. We see where the gaps lie based on our own “Risk Tolerance”
3. Based on the scoring map we prioritize technologies
4. We calculate the cost of implementing the prioritized technologies

Cost of Technology + Cost of Labor

Further Considerations...

- Assessments
- Red Teaming

Questions

