This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-7396C

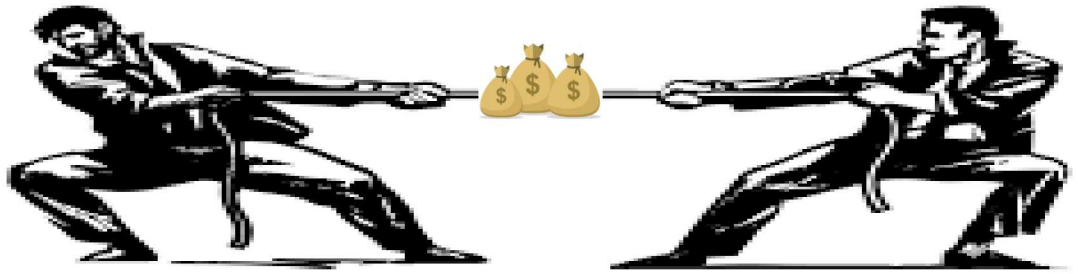
Threat Based Cybersecurity Investments

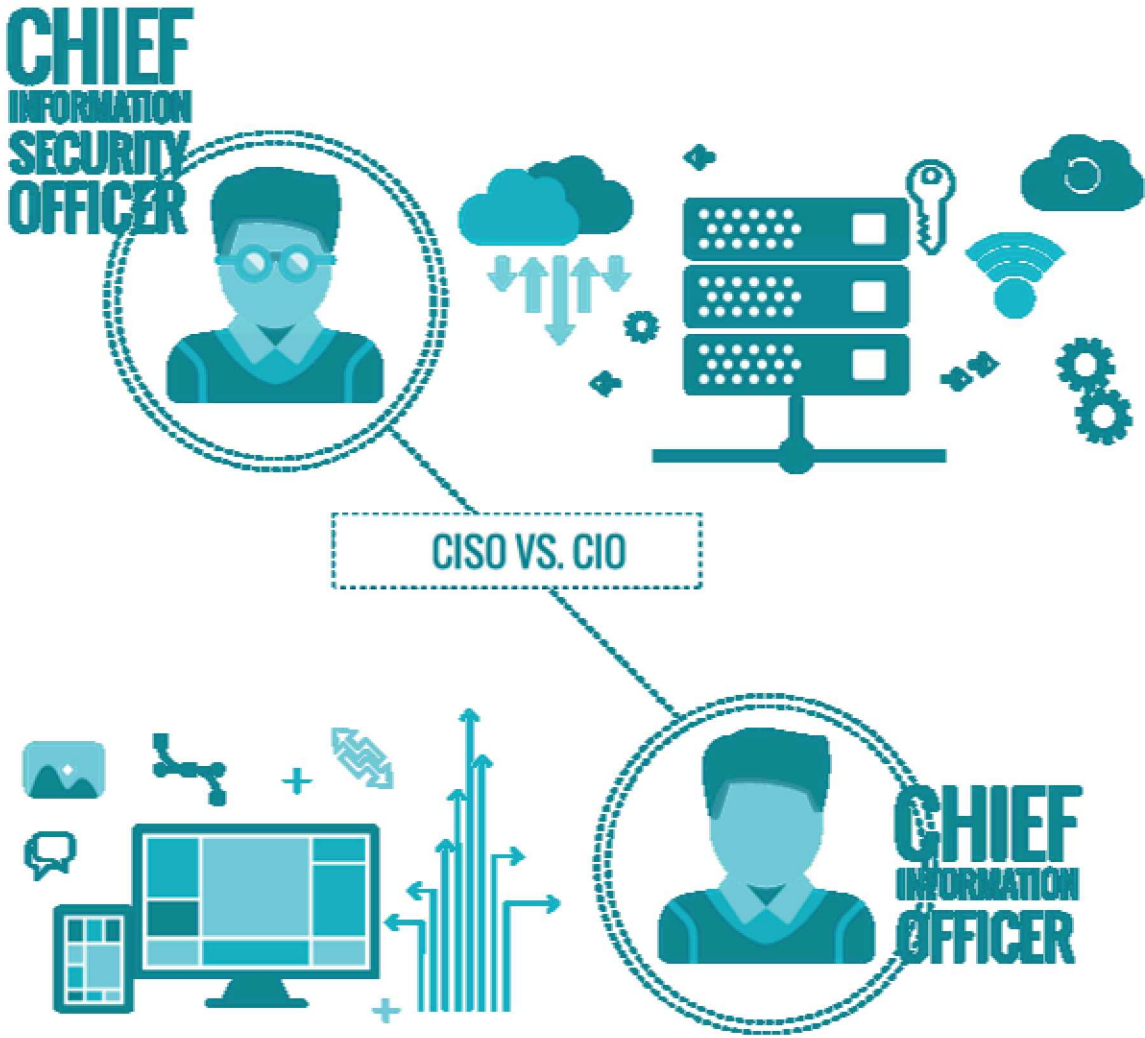
PRESENTED BY

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 2019[1]

Data from Strategic Cyber Ventures[2]:

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.

3 https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

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%**

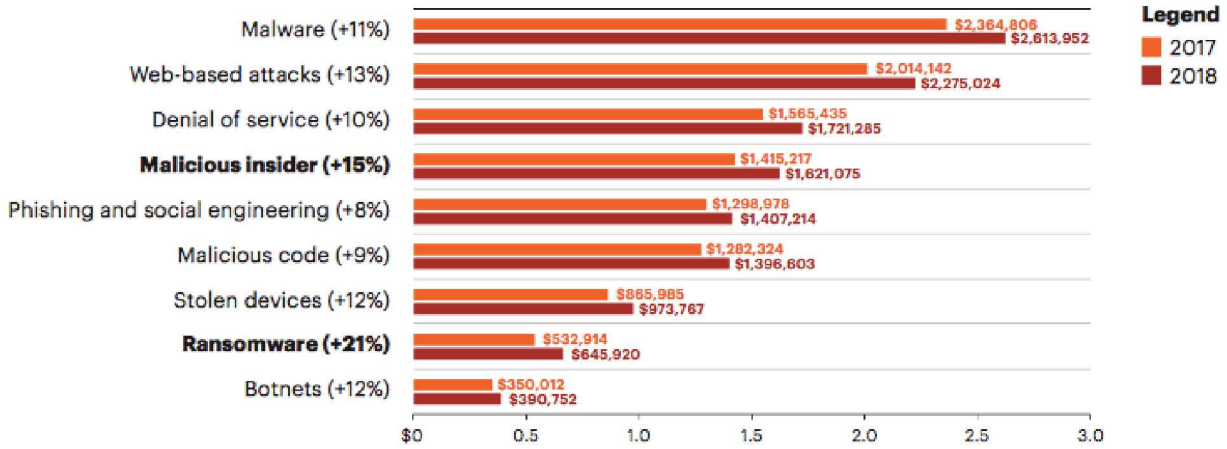
Average cost of cybercrime in 2017

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

Accenture-Cost-Cyber-Crime-Infographic.

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

NIST – Special Publication 800-30 (Guide for conducting Risk Assessments)

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's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)

MITRE ATT&CK MATRIX

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

Recon

- Motivation
- Preparation

MITRE ATT&CK:

- **Active Scanning**
- **Passive Scanning**
- **Determine Domain and IP Address Space**
- **Analyze Third-Party IT Footprint**

Weaponise

- Configuration
- Packaging

MITRE ATT&CK:

- **Malware**
- **Scripting**
- **Service Execution**

Delivery

- Mechanism of Delivery
- Infection Vector

MITRE ATT&CK:

- **Spearphishing Attachment/Link**
- **Exploit Public-Facing Application**
- **Supply Chain Compromise**

Exploitation

- Technical or human?
- Applications affected
- Method & Characteristics

MITRE ATT&CK:

- **Local Job Scheduling**
- **Scripting**
- **Rundll32**

Installation

- Persistence
- Characteristics of change
- Acquiring additional components

MITRE ATT&CK:

- **Application Shimming**
- **Hooking**
- **Login Items**

C2

- Communication between victim & adversary

MITRE ATT&CK:

- **Data Obfuscation**
- **Domain Fronting**
- **Web Service**

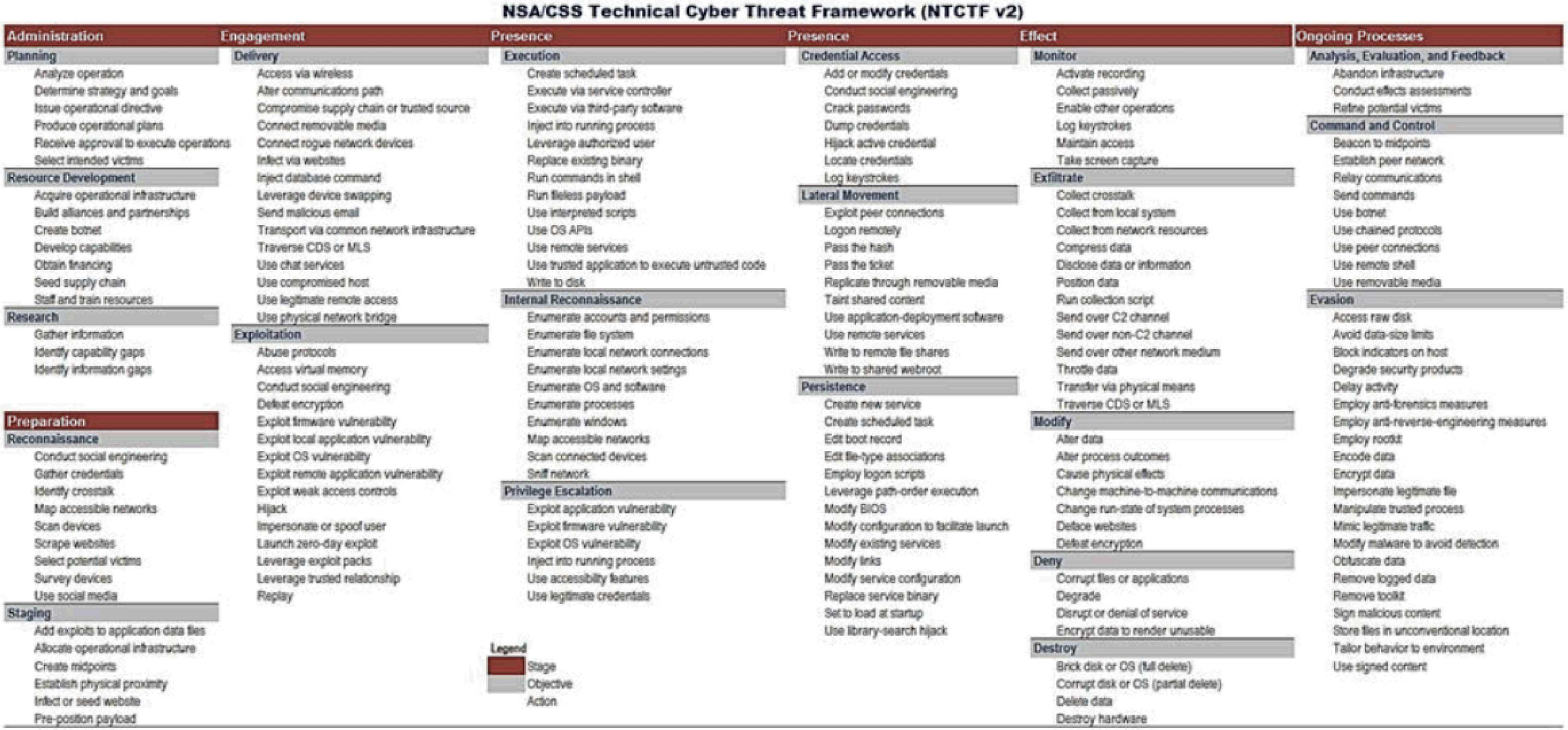
Actions & Objectives

- What the adversary does when they have control of the system

MITRE ATT&CK:

- **Email Collection**
- **Data from Local System/Network Share**

NSA Technical Cyber Threat Framework (NTCTF) v2 * (13 November 2018)

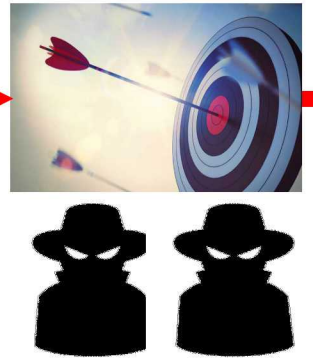


* https://www.nsa.gov/Portals/70/.../ctr-nsa-css-technical-cyber-threat-framework.pdf

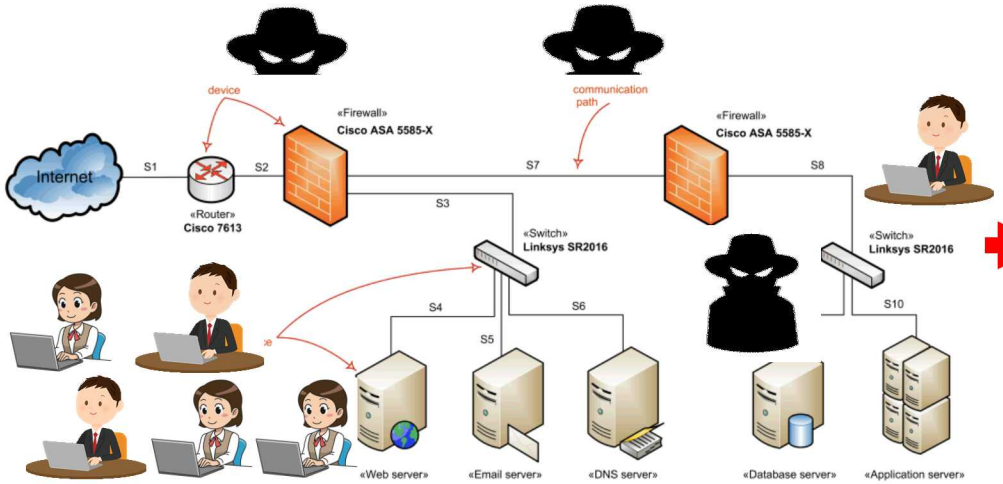
Lifecycle of a Threat

Pre-event

Get-in

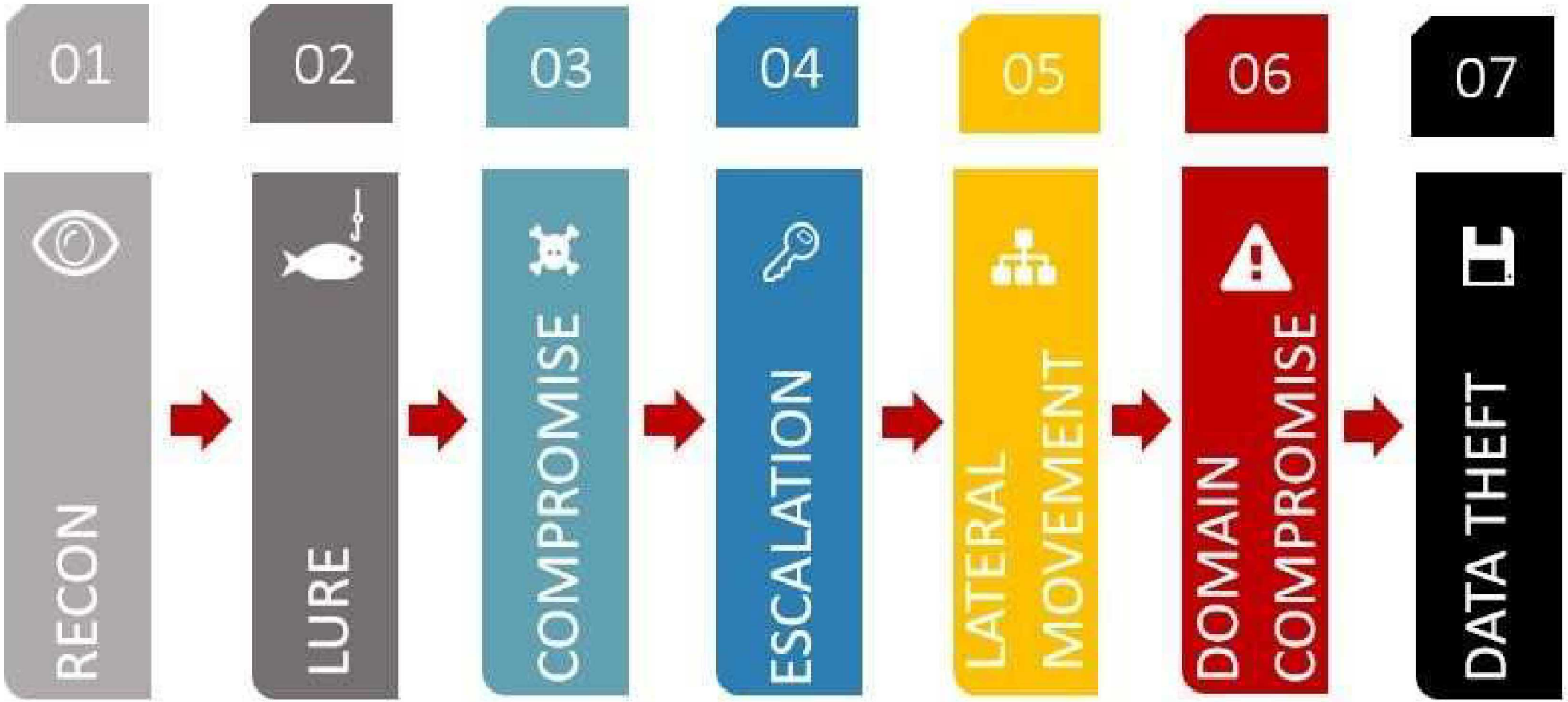


Stay-in



Act

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: …

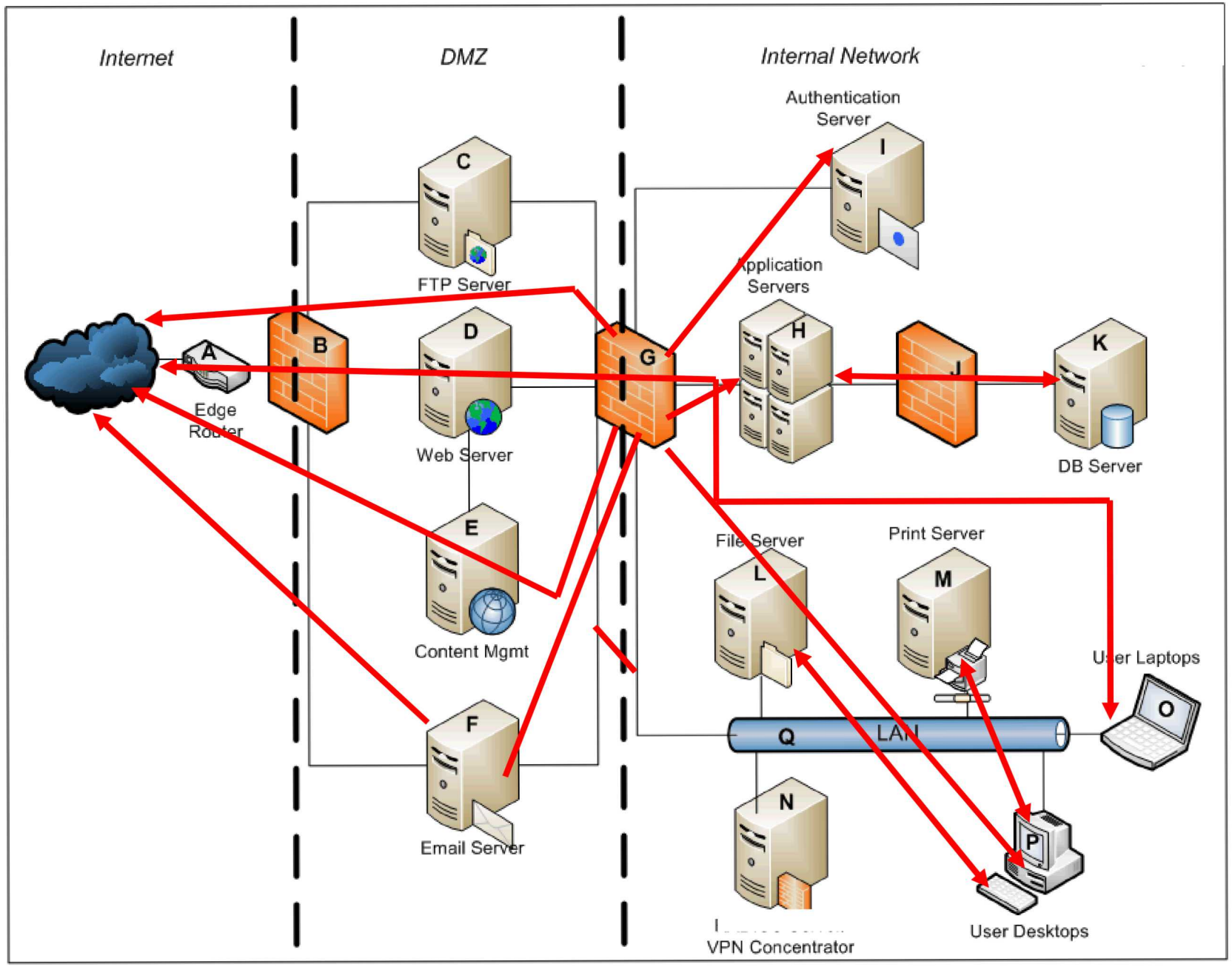
Objective: Alter/Deceive
- Action: Full Data Deletion
- Action: Denial of Service
- Action: Cause Physical Effects
- Action: …

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


Internet
DMZ
Internal Network
Authentication Server
I
C
FTP Server
Application Servers
H
D
Web Server
A
Edge Router
B
G
J
K
DB Server
E
Content Mgmt
File Server
L
Print Server
M
User Laptops
O
F
Email Server
Q
LAN
N
P
VPN Concentrator
User Desktops

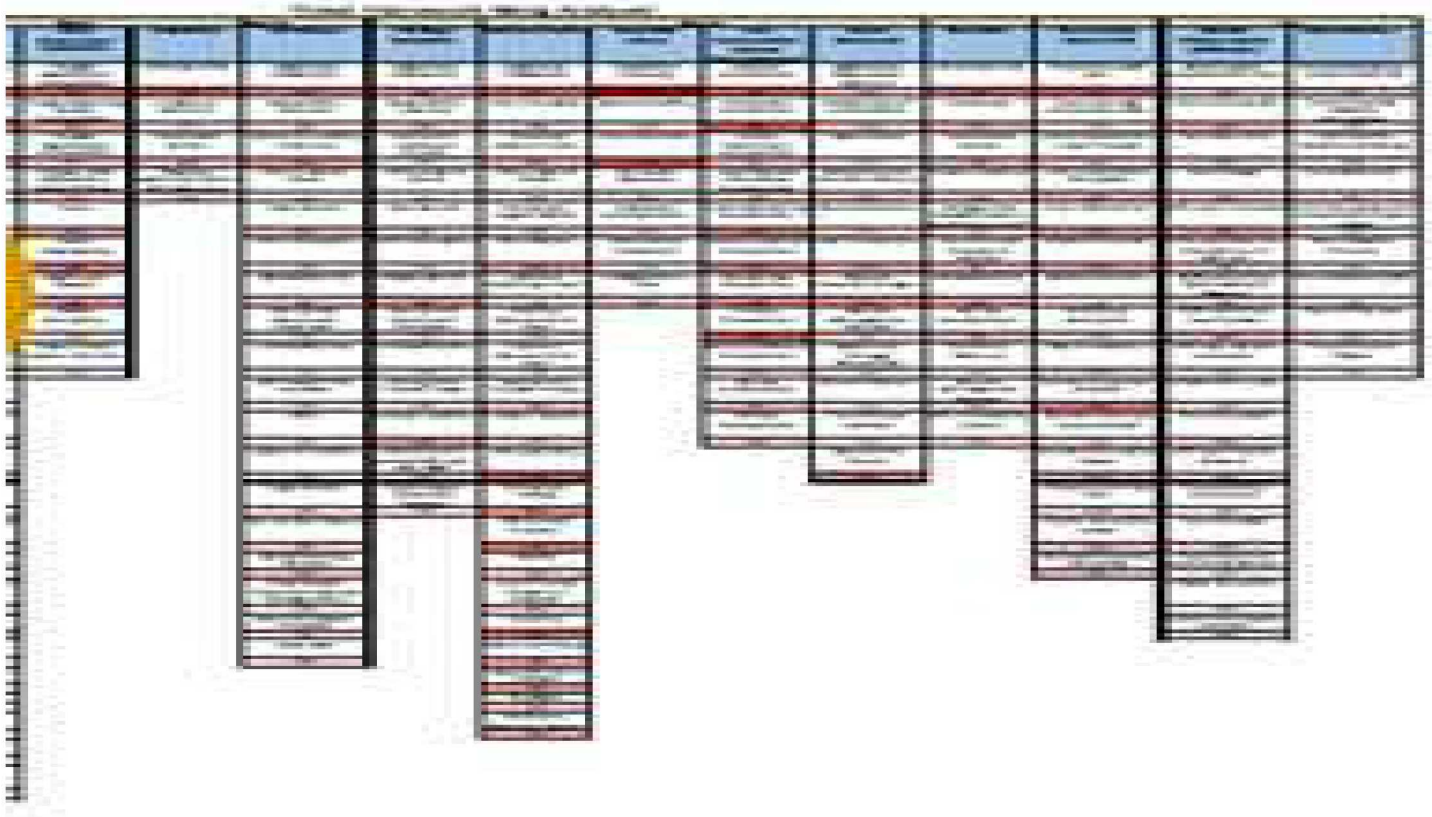
Exemplar Security Capabilities

- 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					
	Detailed Capability Description	Is Enhanc	% Scoring Comple	Threat Action Y			Threat Action z		
				Protect	Detect	Respond	Protect	Detect	Respond
Capabilities	To create new Capabilities, select the entire row of an			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"

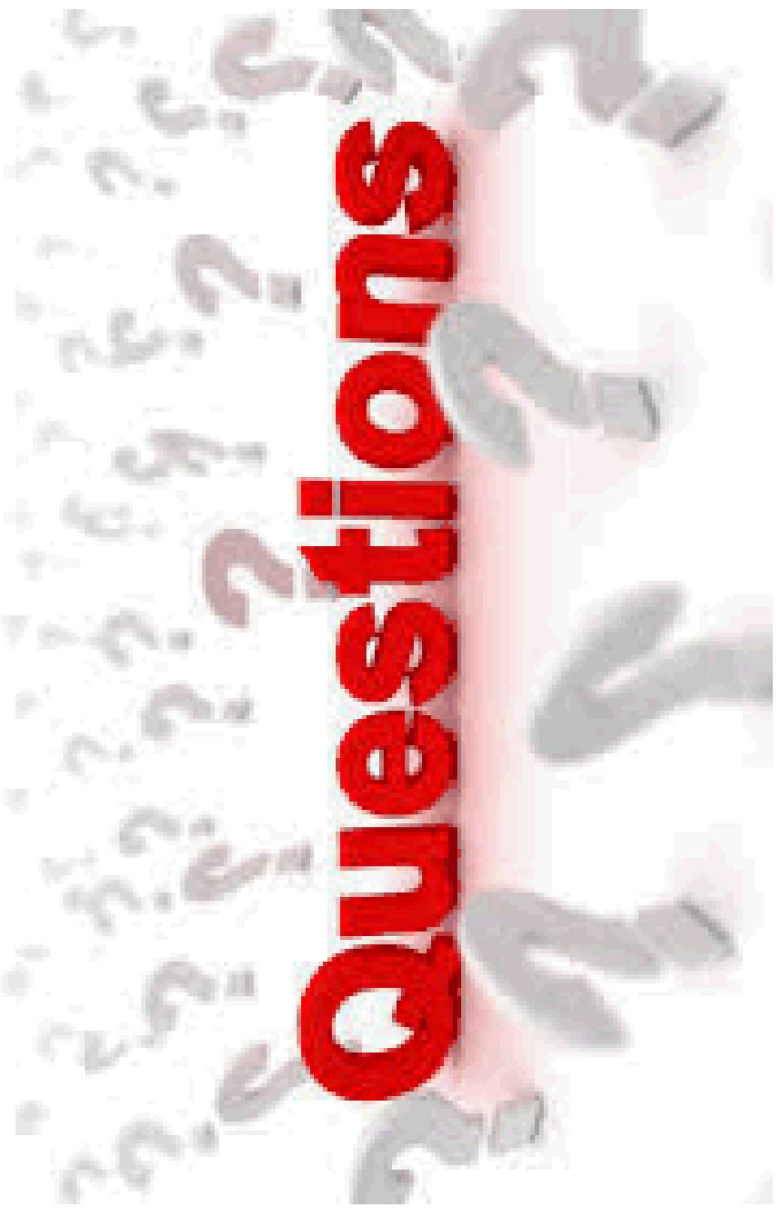
3. Based on the scoring map we prioritize technologies

4. We calculate the cost of implementing the prioritized technologies

Cost of Technology + Cost of Labor

Further Considerations…

- Assessments
- Red Teaming


Questions