



Module 2 – Attacker Perspective



Capgemini

Threat Modeling and Analysis



Capgemini

Foundational Analyst Security Training

Agenda



THREATS | THREAT MODELING | THREAT ANALYSIS METHODOLOGY |



Topic Learning Objectives

Upon completion of this topic, the student should be able to:

- Identify and prioritize appropriate threat actors.
- Identify applicable attack scenarios.
- Understand the security implications to a system.
- Utilize threat information to help specify controls.
- Provide quantitative and qualitative analysis of threats, risks, and controls.



“If you think technology can solve your security problems, then you don't understand the problems; and you don't understand the technology.”

Bruce Schneier

Introduction



It is often said that, to succeed in securing a system, one must be able to think like an attacker.

While this is true, it is an oversimplification of the methodologies needed to secure and defend an environment.

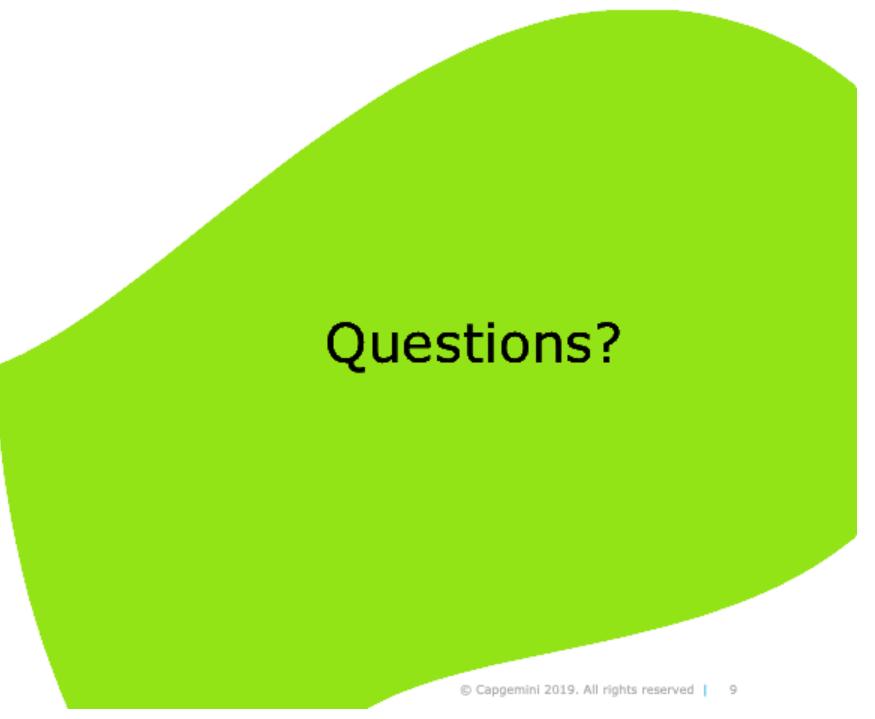
- Understanding the attacker's methods and motivations must be coupled with an understanding of the systems and technologies, as well as security controls within the environment.

Purpose



This module presents methodologies, practices, and concepts that security practitioners, engineers, and analysts can utilize to guide security activities and make reasonable decisions about security controls.

This module will teach you the key components of a threat model so you understand how security controls are selected and implemented.



Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 9

Threat Models



Capgemini

Wise Words...



“

True cybersecurity is preparing for what's next, not what was last.”

-Neil Rerup



Archaic Approaches vs. Threat Modeling

Outdated Approaches to
Security Engineering

System Categorization



Select and Design Controls

Security Engineering Methodologies



"Threats First" approach to securing architecture, engineering, and operations.

This contrasts with a "Controls First" or "Vulnerabilities First" approach.



Security Engineering Methodologies



Controls Driven

Vulnerability Driven

Threat Driven

Select controls from a catalog, based on system criticality.



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 14

Security Engineering Methodologies



Controls Driven

Vulnerability Driven

Threat Driven

Select controls to mitigate specific attacks or vulnerabilities.

Typically based on intelligence developed either internally or externally.



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 15

Security Engineering Methodologies



Controls Driven

Vulnerability Driven

Threat Driven

Determine what threats are relative to the system, then develop and implement controls that can mitigate those threats.

Typically the most effective method, combining the best of controls and vulnerability approaches with real-world threats to the system.



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 16

Controls Driven - Concerns



Controls do not actually mitigate specific threats.

Adding more controls is not always effective.

Adds cost and increases complexity.



Controls Driven – Concerns



Ineffective controls can leave your network unprotected.

This gives the appearance of contributing to security while not offering any meaningful contributions to security.



Controls Driven – Concerns



Controls that are not relative to the system or do not take into account how critical the network is.

Contribute to increasing instead of reducing vulnerability.

Increases cost.



Vulnerability Driven - Concerns



Vulnerabilities are constantly changing, and there is no way to mitigate or predict them all.
Mitigation is an IT priority not a security priority.





Vulnerability Driven – Concerns

The number of vulnerabilities found or mitigated is not a good indicator of a good security posture.
Can be a good measure of a bad security posture.
"Zero Day" problem.



Threat Driven - Concerns

A threat-driven approach may not meet requirements of a "standards"-based audit.
Threat models are created and never used.
A threat-driven approach to implementing controls requires advanced security expertise.





Threat Driven Advantages

Good controls alignment
Threat / Risk posture output
Excellent for new technology
Good for "what if?" scenarios

Good functional coverage
Design focused
Technology agnostic
Uses familiar artifacts



Threat-Driven Disadvantages



Does not document details of attack paths (use attack trees for this)



Why the Threat-Driven Approach?



Threats are consistent and are always present.

Threat agents initiate attacks on their timetable.

Threats are what impacts networks, organizations, and people.

Controls and vulnerability-driven approaches are more about compliance than protections.





To Comply or Not to Comply

Although a threat-driven methodology is primarily designed to respond to specific threats to the network, there are also compliance concerns associated with regulatory and business requirements.





To Comply or Not to Comply

Care must be taken to ensure that the threat-driven methodology drives the process and not a checklist!



Checklists are a great tool, but they cannot be used exclusively.

Use threat-based analysis to review the process actively that is relative to the asset.

Threat Modeling vs. Checklists



Useful information: There are multiple allowances within Compliance Models for Threat Analysis and Tailoring.

- DISA STIG, Application Security and Development, Sec 3
- DoD RMF (8510.1) – Step 2.c
- NIST 800-53 R4 – SA 8
- NIST 800-30 – Task 2-1
- NIST 800-39 – Task 1-1, 2-1, 2-2, 4-1
- NIST CyberSecurity Framework (Feb 2014) – per Exec Order 13636



The Threat-Driven Approach to Securing a System

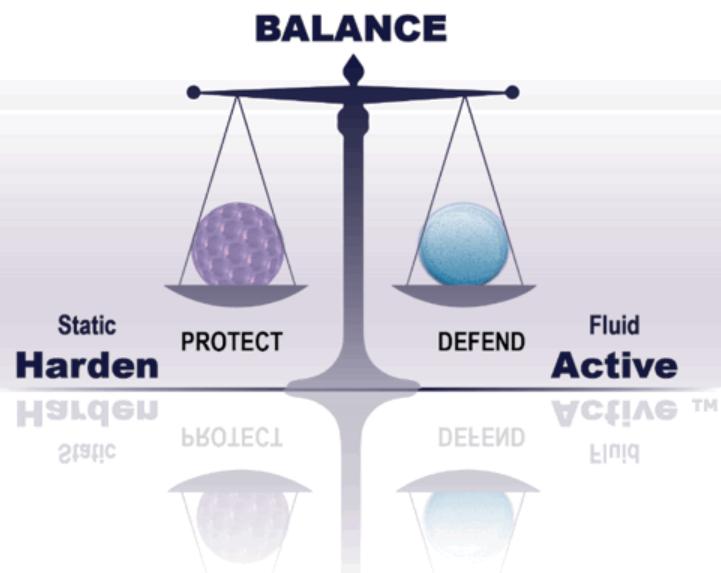


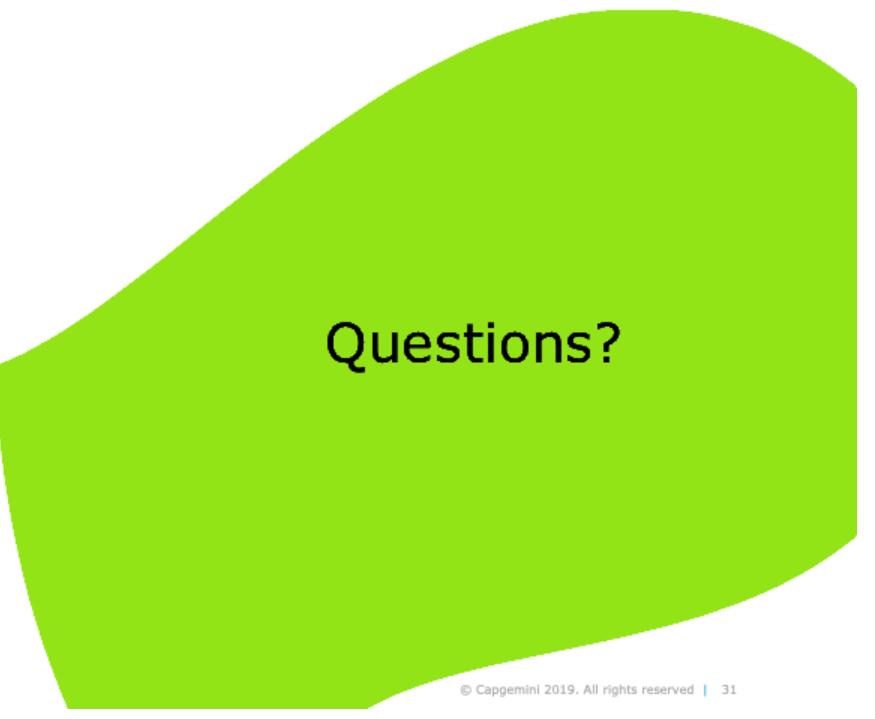
This course will provide you with the ability to do the following:

- ✚ Select **protection** and appropriate compensating controls.
- ✚ Design the system to be **defended** while it is built and operated.



The Proper Balance





Questions?



Foundational Analyst Security Training

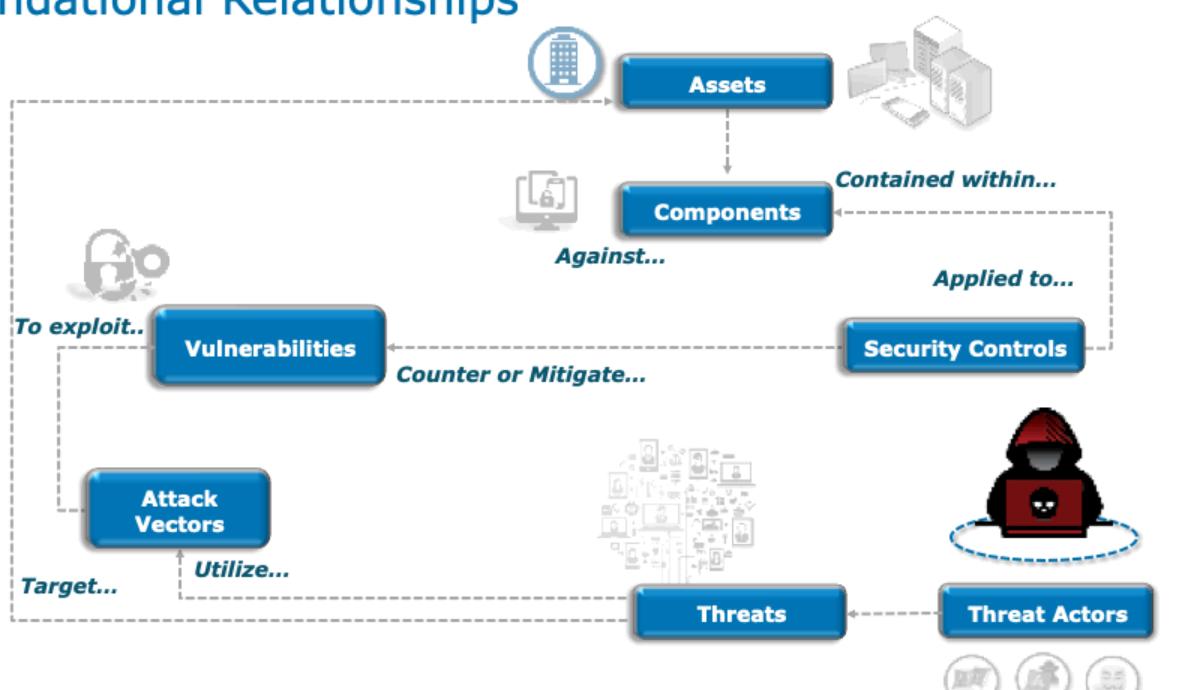
© Capgemini 2019. All rights reserved | 31

Defining Threat Concepts



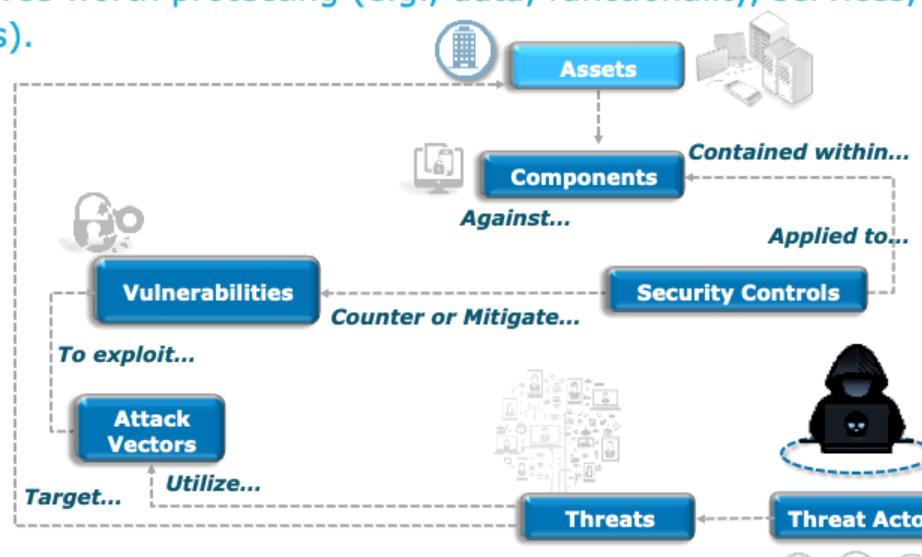
Capgemini

Foundational Relationships



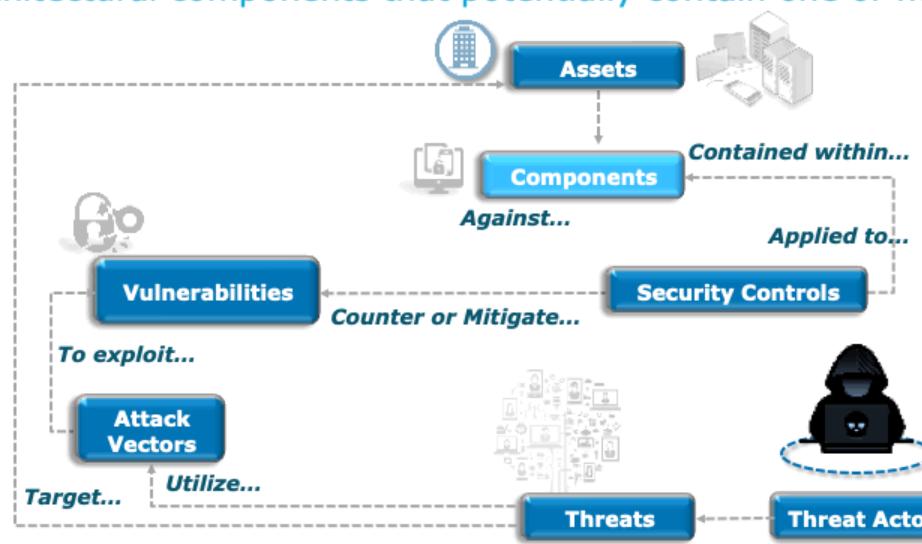
Important Vocabulary

Assets: Any resource worth protecting (e.g., data, functionality, services, people, physical resources).



Important Vocabulary

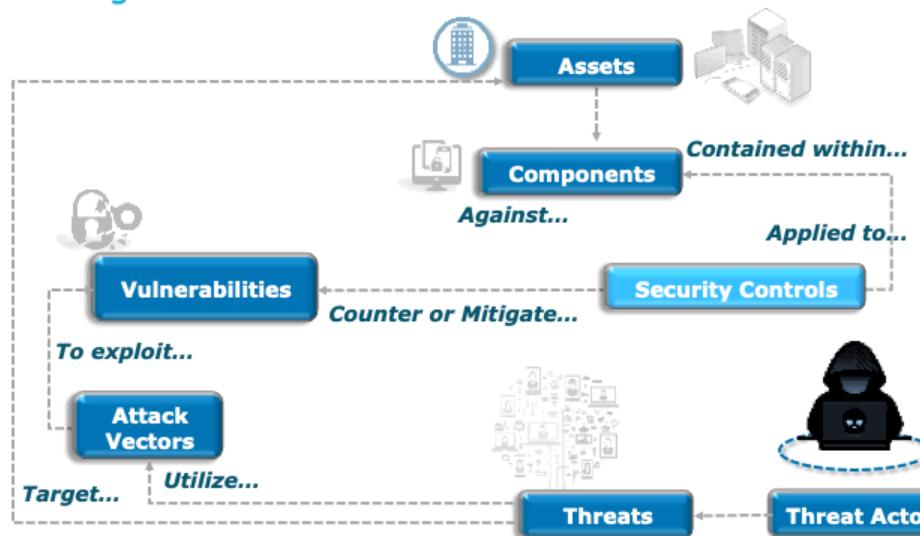
Components: Architectural components that potentially contain one or more assets.



Important Vocabulary



Security Controls: A mitigation or countermeasure to an attack or threat.

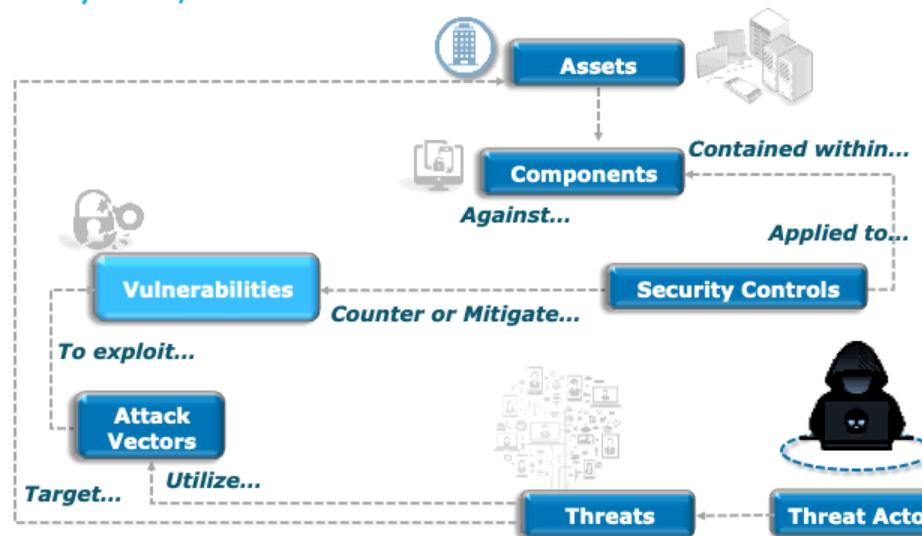


TM

Important Vocabulary



Vulnerabilities: Security flaw; weakness.

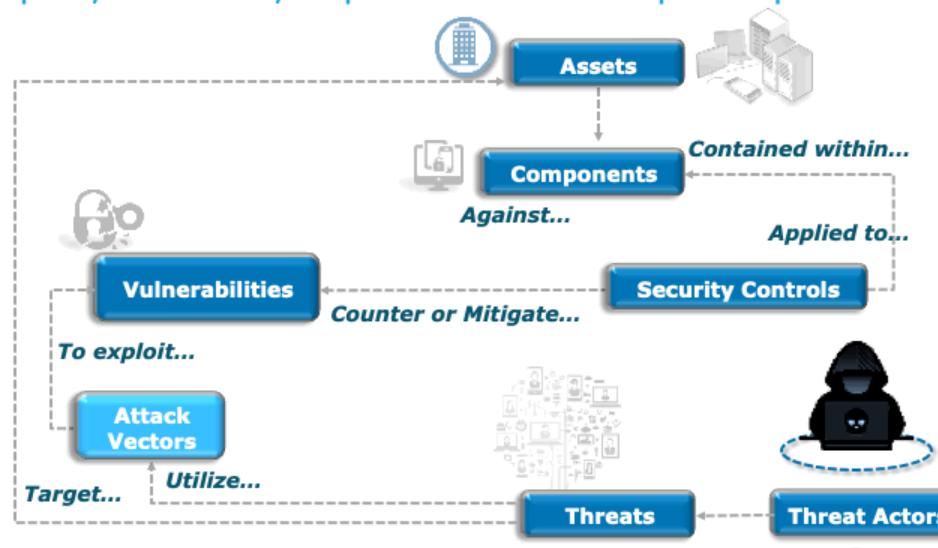


TM

Important Vocabulary



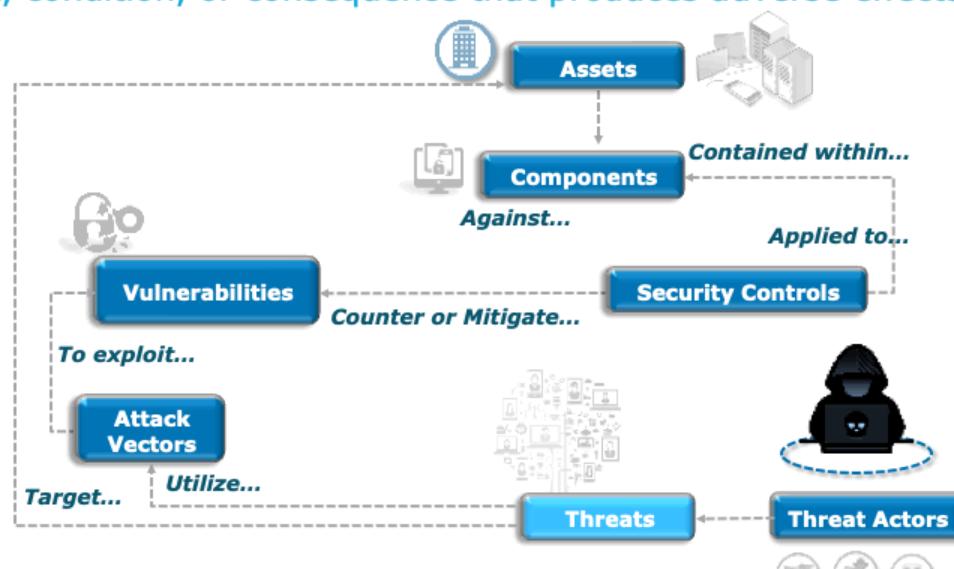
Attack Vectors: Exploit, execution, or performance of a specific path of attack.



Important Vocabulary



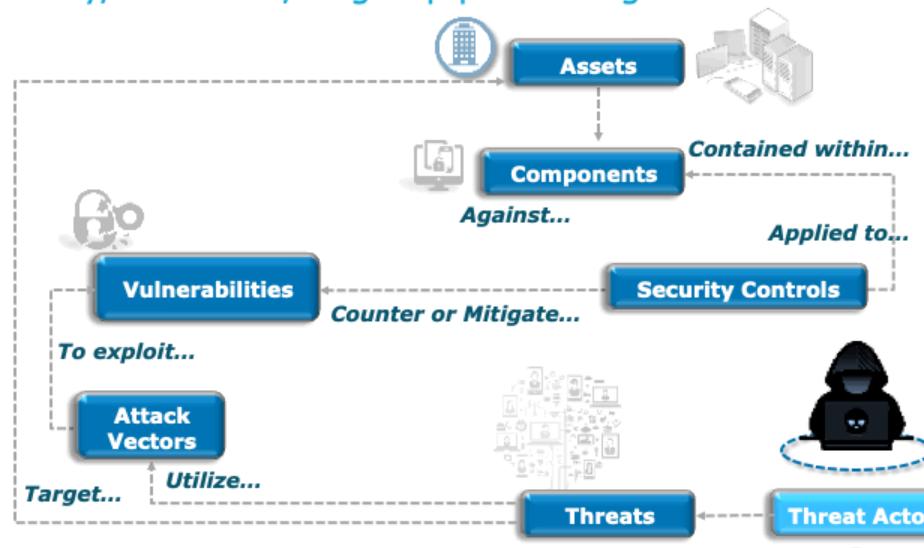
Threats: An event, condition, or consequence that produces adverse effects or undesired results.



Important Vocabulary



Threat Actor: The entity, individual, or group performing the attack.



TM

Important Vocabulary

Risk: Relative value produced by the analysis of probability and impact of a threat being realized or an exploit occurring.





Threat vs. Risk vs. Vulnerability

As we now know, a Threat is an event, condition, or consequence that produces adverse effects or undesired results.

Can you have Risk without a Threat?

Can you have a Vulnerability without a Threat?





Threat vs. Risk – A House in the Woods

Living in a secluded cabin in the woods, there are very few threats.

You can sleep at night with your windows open.

You create a vulnerability, but there is only a small risk of exploitation.



Threat vs. Risk – A House in the City



Living in a large city, there are more threats.

Just like in the woods, you can sleep at night with the windows open.

You create the same vulnerability as you did in the woods; but, because there are more threats to exploit the vulnerability, this creates risk.



What are the Threats We See Today?



The Threat Landscape

	 Advanced Persistent Threat (APT)	 CYBERCRIME	 HACKTIVISM	 INSIDER THREATS	 NUISANCE THREATS	 CYBER TERRORISM
Attack Profile:	Targeted, organized, and funded attacks potentially associated to nation-state sponsorship or other powerful entities	Opportunistic, broad-based, motivated by financial gain	Organized attacks associated to groups of individuals with political, ethical, religious, or retaliatory motives	Legitimate internal user with hidden malicious intentions	Unskilled attackers, scanners and crawlers, spam, worms/viruses, basic malware	Disruptive or destructive acts on behalf of, or in support of, a terrorist group or organization
Primary Objectives:	Typically, medium to long term; exfiltration of intellectual property for purposes of eliminating years of R&D, competitive economic and/or nation-state advantage	Typically, short term; identity theft, credit card fraud, extortion, botnet creation and management	Typically, short term; cause havoc and chaos, disrupt operations, discredit and malign via disclosure of sensitive information	Short to long term; compromise of sensitive information, destruction, revenge, espionage, harassment	Often unknown or irrelevant; recognition and status, reconnaissance, financial	Targeted network attacks and exploitation; typically medium- to long-term, sophisticated Tactics, Techniques, and Procedures (TTPs) with clear objectives and supporting ideology
Attack Methods:	Social engineering, spear phishing, watering hole, and drive-by download attacks, espionage, focused perimeter breaches	Phishing attacks, hosting malware on legitimate websites, spam-related attacks, cyber extortion techniques	Distributed Denial of Service (DDoS) attacks, traditional hacking techniques, spear phishing, etc.	Access via legitimate credentials and privileges, data exfiltration, physical and logical sabotage, surveillance	Automated scanners, public exploitation kits, generic spam email, propagating worms/viruses, adware, scareware	DDoS, public and custom exploitation kits, custom malware, sophisticated delivery methods



Threat Actors (aka Attack Agents)

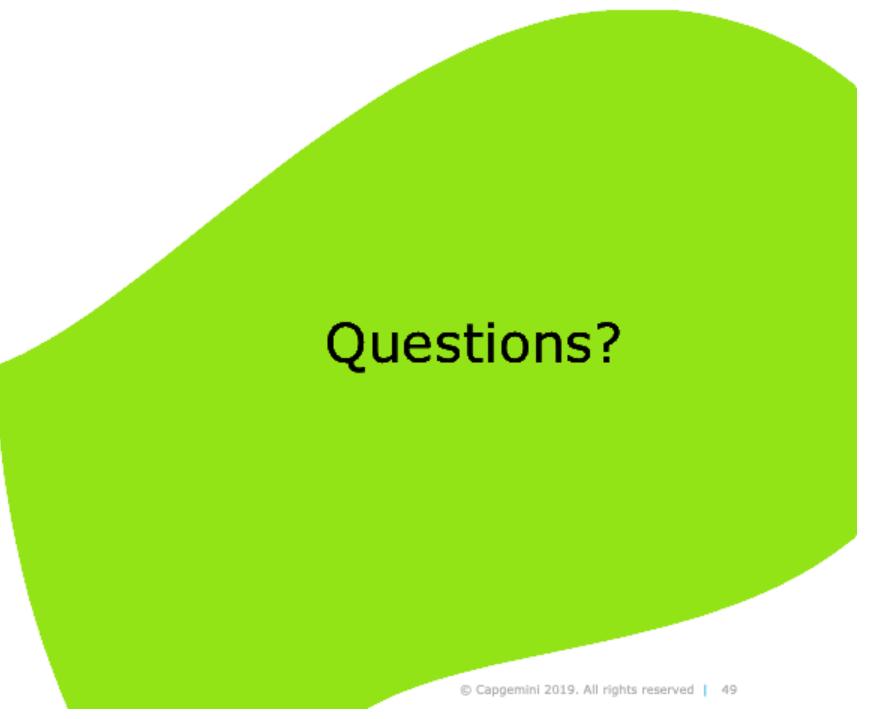
Threat Actor	Motivation	Resources	Skills	Objective
 Advanced Persistent Threat (APT)	Financial	Organizational	Advanced	Theft
 Nation State	Technology Advantage; Geopolitical Advantage	National	Highly Advanced	Theft Damage
 Hactivist	Notoriety	Reduced Organizational	Various – High Watermark @ Advanced	Embarrassment Disclosure Theft Damage Embarrassment Disclosure
 Lone Wolf/Small Team	Financial Notoriety	Limited	Advanced	Theft Damage Embarrassment Disclosure
 Malicious Insider	Financial Revenge	Limited – but Pre-Existing Access could be Significant	Dependent upon Role	Theft Damage Embarrassment Disclosure
 Malicious Partner	Technology Advantage; Business Advantage	Limited	Dependent upon Role	Theft
 Espionage	Technology Advantage; Geopolitical Advantage; Business Advantage	Organization to National	Highly Advanced	Theft Damage

Attack Vectors: Then and Now



Beginning of 21 st Century		TODAY
Adversary attack patterns are becoming more varied and sophisticated.	Email "Spoofing"	"Man-in-the-Mailbox"
	Parking lot entry vector	Lateral movement, exfiltration
	Fake sites that look real	Legitimate website hosting malware
	Vulnerabilities and misconfigurations	Vulnerabilities and misconfigurations
Are your processes and procedures tailored to combat the threats of today?	Suppliers/Partners are not on the radar	Complex attacks leverage established, trusted relationships

TM



Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 49

Why is this Important?



Capgemini

Art or Science?



Threat analysis is as much an art as a science.

- Just like there is no one way to create art, there is no one way to protect a system.
- Every system, every protection schema is different.

Like art, there is a general idea of good art vs. bad art.



Requires subject matter expertise, or tradecraft.

What Are My Resources?

To keep your network from becoming compromised, you must constantly be learning and growing and stay current with security trends.

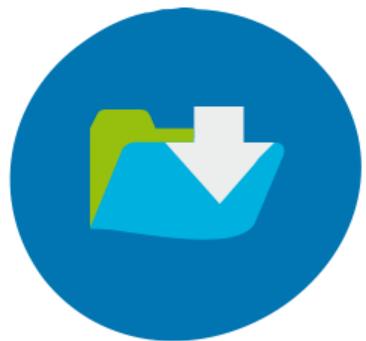
There are many resources that can help you do this:

- White Papers
- Lab Scenarios (Real and Virtual Reality [VR])
- Industry Publications
 - National Institute of Standards and Technology (NIST)
 - Institute of Electrical and Electronics Engineers (IEEE)
- Threat Modeling Resources Online
- Professional Journals



What Are My Resources?

Utilizing the tools you have at your disposal is essential to combating threats to your organization effectively.





You Have to Get Your Mind Right!

Always look at your environment from the front gate of the network architecture.

Examine everything between it and your asset.

- You must always be thinking "How could I break this? How can it perform outside of specifications?"



EX001:Defining Threat Concepts



Group Exercise: Think Like the Adversary



Mindset



So lets put that attacker mindset to work.....



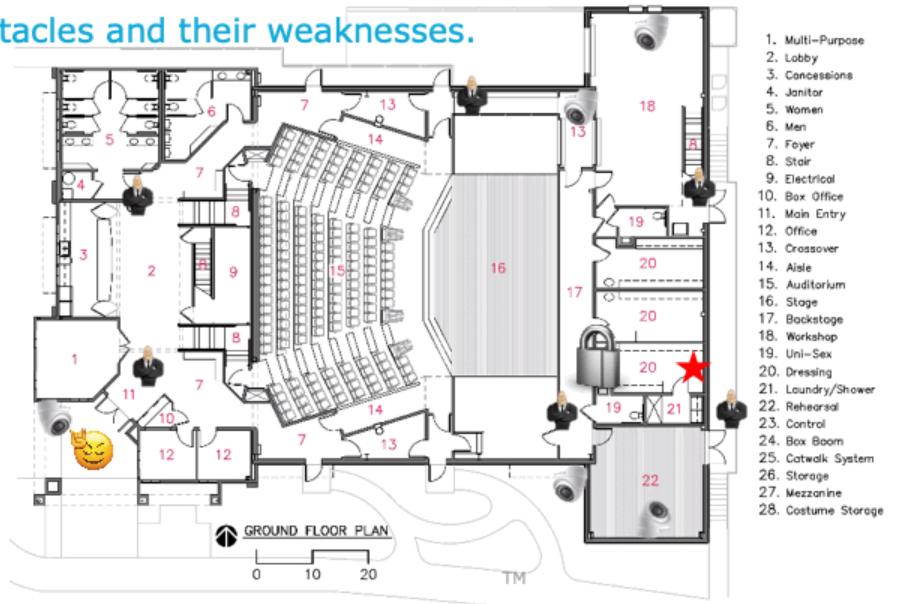
You want to get backstage with the band, but you don't have a ticket...

*So, how would **YOU** do it... ???*

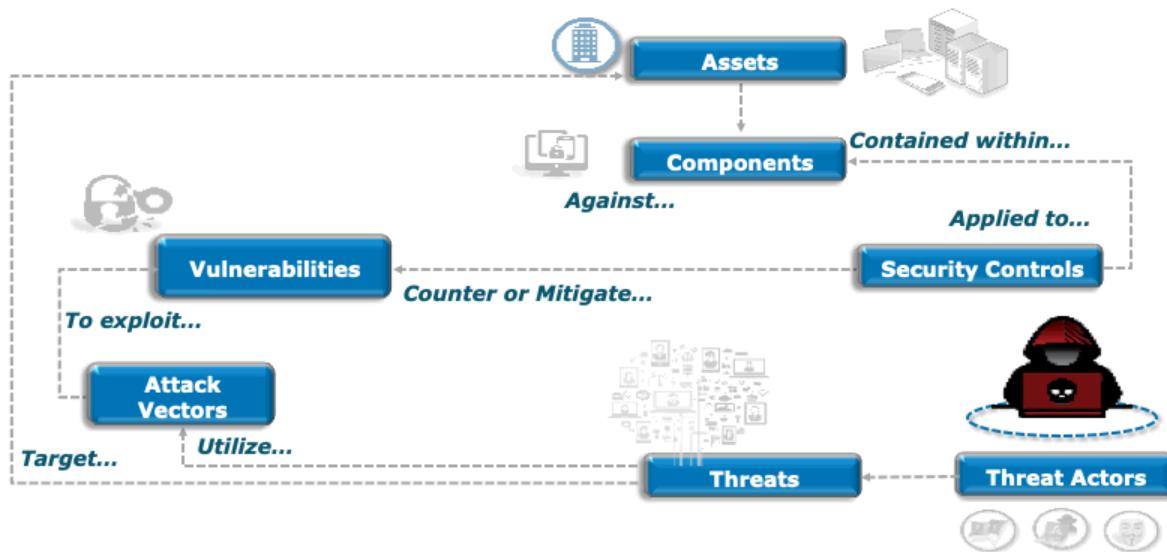
Mindset



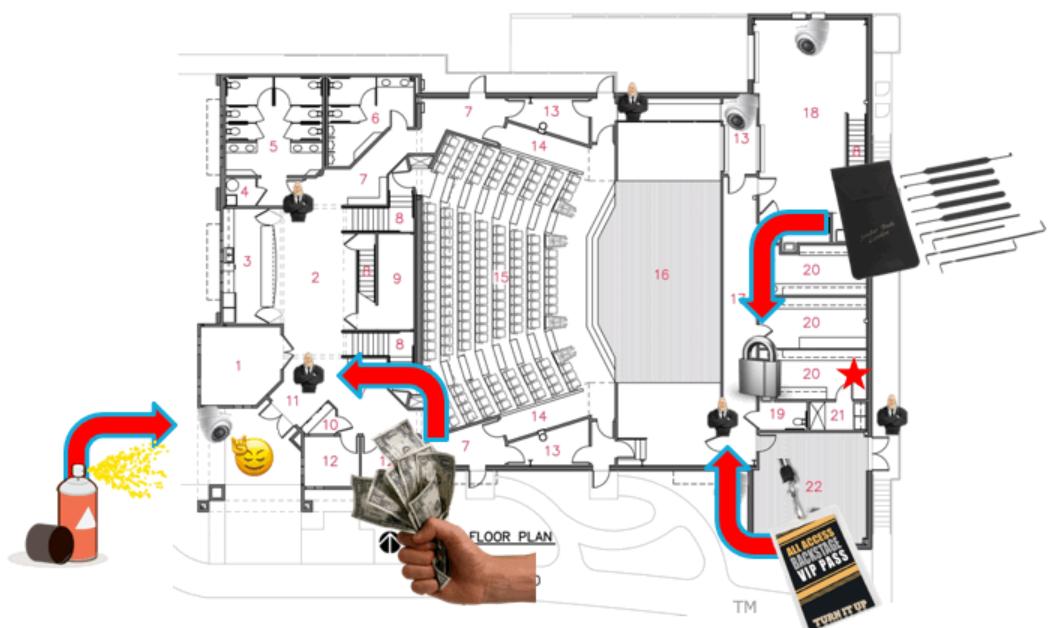
Consider the current obstacles and their weaknesses.

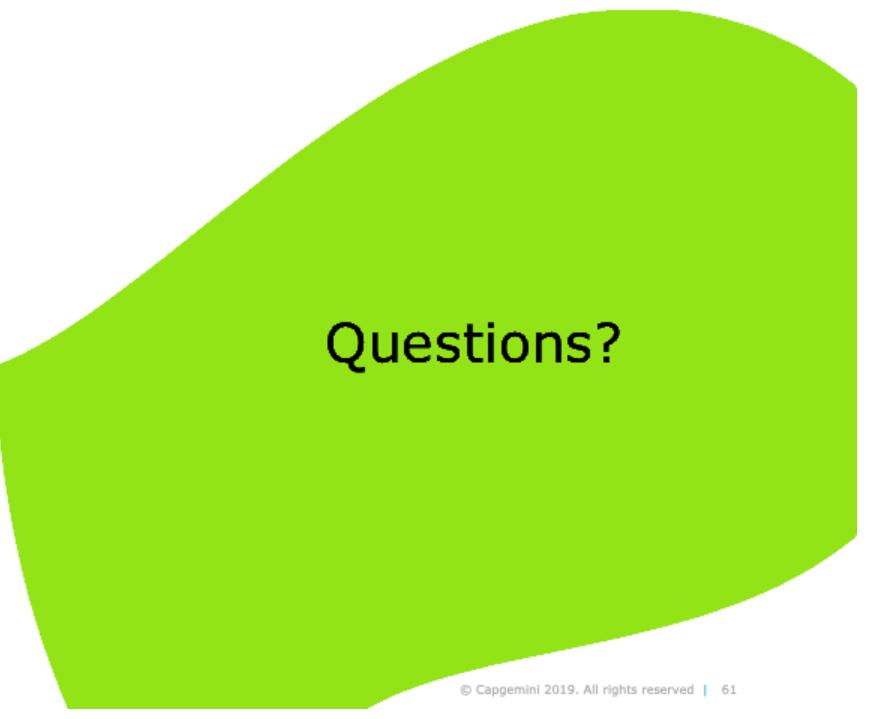


Foundational Relationships



Mindset





Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 61

Threat Models: Analysis



Capgemini

Foundational Analyst Security Training

Disclaimer



This section presents tools that can be used to perform attack analysis.

- This list of tools/concepts is not comprehensive, nor is it the only way for analysis to be done.

We are presenting options for you to build in to your toolbox of possible attack analysis tools.

Threat models and the Cyber Kill Chain®, as well as defendable architectures, deal with the cause of attacks.

STRIDE-LM describes the effect of a threat.



Threat Analysis Techniques

Technique	Description
Threat Models	Depict data flows, data stores, processes, and system and trust boundaries
CIA Triad	Analyze the system for concerns in Confidentiality, Integrity, and Availability
STRIDE-LM	Analyze the system using defined attack categories
Cyber Kill Chain®	Analyze security posture using 7-step process of the attacker activities
Doomsday Scenarios	Analyze worst case scenarios
Attack Trees	Decomposition of <i>how</i> a threat against an asset can be realized
Threat Profiles	Tabular summary of threats against a system or component



The CIA Triad

Confidentiality, Integrity, and Availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

The elements of the triad are considered the three most crucial components of security.



STRIDE-LM



STRIDE-LM	Threat	Property	Definition	Typical Controls	Examples
S	Spoofing	Authentication	Impersonating someone or something	AD, ADFS, RSA, SmartCard, Password Vaulting	Pretending to be Marilyn Hewson, Microsoft.com, an IP address, a critical OS library or piece of executable code
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks	Modifying any data/code or the format(s) of data/code, whether it is on disk, in memory or traversing a network
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	LAMS, SIMS, EnCase, FPC	"I didn't send that email" - "I did not visit that web site" - "I didn't run that program"
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation	Reading another employee's files/email; viewing someone else's payroll or health records; publishing a list of credit cards or SSNs
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle	Crashing the OS or application; flooding network with packets; disrupting critical network devices
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC, Sudo, UAC, Avecto, Password Vaulting	A standard user can perform admin/root functions; also - there is "horizontal" privilege access: a standard user performs other actions as another user (related to Spoofing and Repudiation)
LM	Lateral Movement	Defense-in-Depth / Least Privilege	Expand influence post-compromise; often related to Elevation of Privilege	Credential Hardening, Segmentation and Boundary enforcement, Host-based firewalls	A compromise of a single system allows expansion of influence to multiple systems and potentially across trust boundaries

STRIDE-LM and the CIA Triad

The CIA Triad works well for analyzing threats to mission assets.

STRIDE-LM works well for analyzing threats to system assets.



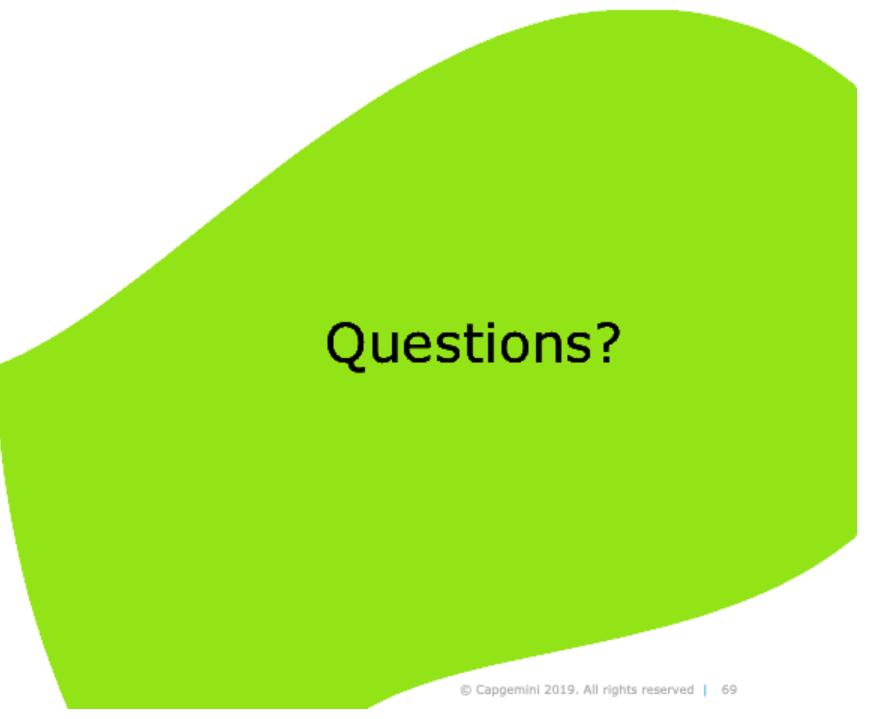
Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 67

STRIDE-LM and the CIA Triad



CIA Property	STRIDE-LM Threat Type
Confidentiality	Information Disclosure
Integrity	Tampering
Availability	Denial of Service



Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 69

Threat Models: Threat Profiles



Capgemini



Threat Profiling

Threat profiling promotes assessment of threats and triage activities when needed.

Effective summary and communications process.

Threat profiles are typically based on a prior assessment, either threat models or attack trees.

Threat Profiles



Uses a table to summarize both threats and attacks.

Begin with the following:

- What assets need to be protected?
- What are the most significant threats/attack types that should be considered?

Threat Profile Example – TimeExpense System



Asset/Objective	Threat Types	Resultant Condition(s)	Attack Surfaces/Vectors	Controls
HR Data	<ul style="list-style-type: none"> • Spoofing • Tampering • Repudiation • Information Disclosure • Elevation of Privilege 	• Unauthorized Data Access and Modification	<ul style="list-style-type: none"> • Database Server • Web Service • Web Application 	<ul style="list-style-type: none"> • Hardening • Secure Coding • Least Privilege
TimeExpense Data	<ul style="list-style-type: none"> • Spoofing • Tampering • Repudiation • Information Disclosure • Elevation of Privilege 	• Unauthorized Data Access and Modification	<ul style="list-style-type: none"> • Mainframe • Web Application 	<ul style="list-style-type: none"> • Hardening • Secure Coding
PassTicket	<ul style="list-style-type: none"> • Spoofing 	• Unauthorized Access to Mainframe	<ul style="list-style-type: none"> • Web Service • PassTicket Generation Service 	<ul style="list-style-type: none"> • Least Privilege • Restricted Access

Threat Profile Example



Technique	Description
Asset	HR Database
Threat Types(s) STRIDE-LM	Spoofing Identity, Tampering, Repudiation, Information Disclosure, Elevation of Privilege <ul style="list-style-type: none">• Database files on the server• Database server itself• Web service that interacts with HR database• Backup servers and services
Attack Surface	<ul style="list-style-type: none">• Gain access to database server and download database files<ul style="list-style-type: none">• Attack services and applications running on server• Interact with database service on server (local or remote)• Gain access to database by interacting with web service• Attack backup disk where database copies are stored• Attacks via web application, such as SQL Injection, or posing as another user
Attack Vector	<ul style="list-style-type: none">• Malicious insider/corporate espionage• Threat actor looking for financial gain• Disgruntled employee
Compromise Result	<ul style="list-style-type: none">• An adversary could gain access to sensitive data, such as Personally Identifiable Information (PII), and sell it• A disgruntled employee could modify HR data such as salary information

STRIDE-LM Analysis of Human Resources (HR) Database



Primary Threats: STRIDE-LM

- Spoofing → Control: Authentication and Access Controls
 - Design:
 - Strong authentication and access control on web front end
 - Strong authentication to access server (Two-Factor Authentication [2FA], certificates)
 - Harden database server against privilege escalation attacks
- Tampering → Control: Validation of Data
 - Design:
 - Restrict input to that which is not already stored in applications (user cannot provide username to app after login, for example)
 - Parameterized queries
 - Whitelist-based input validation where possible
- Repudiation → Control: Logging
 - Design: Entries and approvals are logged, and alerts are created when database rows are updated unexpectedly
- Information Disclosure → Control: Principle of Least Privilege
 - Design: Limit data that is passed to web application User Interface (UI) and browser cache
- Elevation of Privilege → Control: Principle of Least Privilege
 - Design: Limit privileges on accounts used to access database

Threat Profile Lessons Learned



Based on threat analysis techniques, including Threat Models, Attack Trees, etc.

Communicate messages clearly by grouping assets, types of threats, and possible conditions that could arise if the threat materializes.



Threat Profile Lessons Learned

Split up risk rating for current controls and recommended controls to make analysis more clear.



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 77

Summary of Threat Analysis Techniques

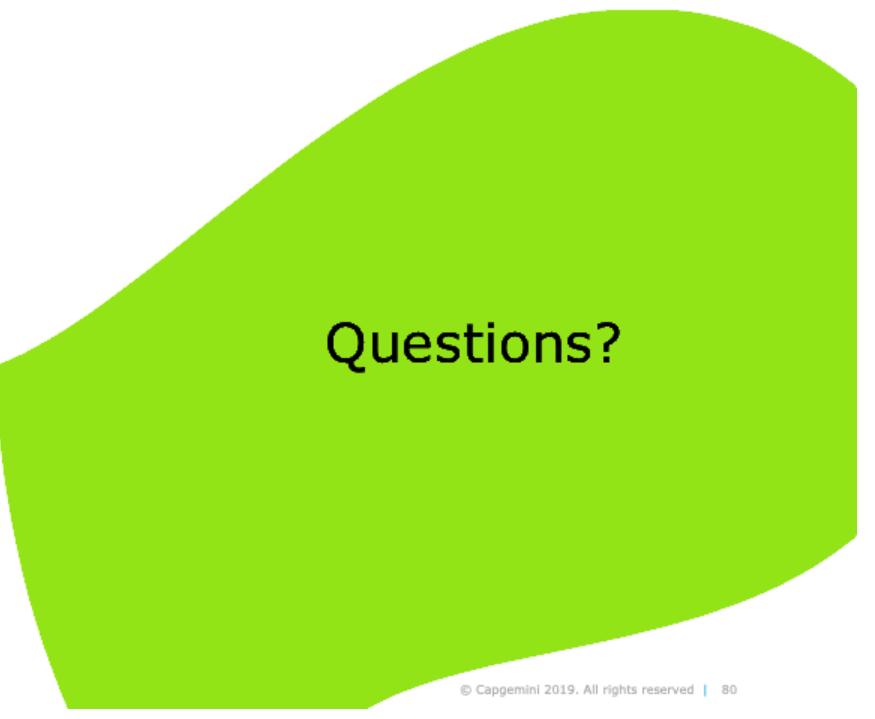


Technique	Description	Best Used For
Threat Models	Depict data flows, data stores, processes, and system and trust boundaries	<ul style="list-style-type: none">• Brainstorming• Defining attack surface• System-level analysis• Component-level analysis• Your go-to tool to get started• New technology or systems
CIA Triad	Method of analyzing system for concerns in Confidentiality, Integrity, and Availability	<ul style="list-style-type: none">• Basic security analysis• High level brainstorming• Defining security goals
STRIDE-LM	Method of analyzing system using defined attack categories	<ul style="list-style-type: none">• Analyzing threats to system assets
Cyber Kill Chain®	Seven-step process of attacker activities	<ul style="list-style-type: none">• Understanding adversary TTPs• Evaluating controls• Framework for threat intelligence

Summary of Threat Analysis Techniques



Technique	Description	Best Used For
Doomsday	Analysis of worst-case scenarios	<ul style="list-style-type: none">Identifying critical business threats
Attack Trees	Decomposition of <i>how</i> a threat against an asset can be realized	<ul style="list-style-type: none">Detailed analysis of specific attacksGenerally narrow in scope
Threat Profiles	Tabular summary of threats against a system or component	<ul style="list-style-type: none">CommunicationsDecision-makingCause and effect documented



Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 80

Common Attacks and Weak Links



Capgemini

Understanding Cyber Attacks



Attack analysis requires subject matter expertise.

- Involve Red Team professionals.
- Use intelligence data/threat briefings.

Cannot cover all attacks comprehensively.

- Focus on threat intelligence for common attacks.
- Ensure that attacks are relevant for a given threat.

Client-Side vs. Server-Side Attacks



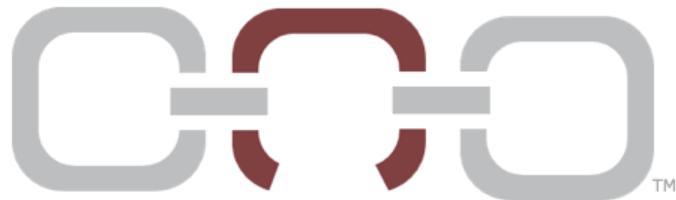
Threats will use any means to achieve their goals successfully.

- Including attacking people.
 - Social Engineering/Phishing.
 - Client-Side Attacks.
 - Physical Intrusion.
- Attackers often prefer client- over server-side attacks.
 - Do not need complex technical exploits.
 - Humans cannot be patched as easily.
 - Establish and exploit trust.

Weak Links



Security can be thought of as a chain; each link or layer in the network protections relies on the strengths of the others.



Understanding common weak links is imperative.

Users

Weakest link in the line of defenses.

Attackers entice users to do something they should not be doing.



Mitigations

- User access has deterred over **90 percent** of initial malware installations.
- Attackers often require **administrative rights**.
- Privilege escalation tool will **leave log activity** for post-intrusion analysis.
- User education and involvement in computer and network defense when interacting through **email** or **browsing the Internet**.

Weak Links – Regular Users



The best way to mitigate the threat from users, is to ensure they are aware and intelligent about the threats around them.

User cybersecurity awareness training is a key layer in the defense in depth model for network defense.

**Turn your biggest
weakness into
your best defense!**



Weak Links – Administrators



Administrator accounts are another weak link in the defense model.

Default Windows Administrator Accounts:

- Standardized username and password.
- Should be renamed or disabled and replaced with a managed account that has password length, complexity, and other controls in place.

Weak Links – Administrators



Service/Software Accounts:

- Users should have a “Super” account for administrative functions, with a normal user account for everyday use, email, meetings, etc.
- Each account should take into account least privilege and separation of duties.
- Isolate administrator interfaces, where possible.

Other Common Weak Links



Unpatched Software

Insecure Remote Access

Passwords

Insecure Software



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 89

Common Attacks



This is not a comprehensive list but does give you an idea of what types of attacks should concern you.

Threat modeling and analysis helps prepare your organization for almost any given attack.

Some examples are as follows:

- Social Engineering
- Lateral Movement
- Web Application Attacks
- Remote Code Exploitation

Social Engineering



Examples:

Anything that exploits default human trust behavior.

It is more than just phishing.

- Obfuscated web links
- Phishing sites
- Telephone calls to acquire information
- Help desk manipulation
- “Tailgating” into a secure facility

Lateral Movement



Common Tools:

- Pass-the-Hash Toolkit (original tool – effective up to Vista)
- Windows Credential Editor (WCE)
- Mimikatz
- gdump

These techniques typically require administrative privileges.

Takes advantage of Windows Single Sign-On (SSO) and Credential Management design.

Web Application Attacks



Cross-Domain attacks (XSS, CSRF, XSSI).

- No input validation/output encoding.
- No distinction between legitimate requests and forged ones.

SQL Injection.

- All major relational databases have issues.
- Root problem:
 - Poor coding practices at both the web application and database.
 - Excessive privileges on accounts that access the database from the web application.

Memory Corruption/Remote Code Execution



This covers all C/C++ Memory Corruption Attacks.

- Buffer Overflow
- Heap Overflow
- Heap Spray
- Heap Free()
- Return-Oriented Exploit (ROE)/Return-Oriented Programming (ROP)
- Pointer Manipulations (NULL Pointers)

MITRE ATT&CK



MITRE'S Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a threat actor behavior model that details activities a bad actor may take while attacking or operating inside an enterprise network.

Can be used alongside MITRE's Cyber Analytics Repository for behavioral-based intrusion detection analytics.

MITRE's Threat-Based Approach



Principle 1: Include Post-Compromise Detection

Principle 2: Focus on Behavior

Principle 3: Use a Threat-Based Model

Principle 4: Iterate by Design

Principle 5: Develop and Test in a Realistic Environment



Attack Analysis to Analyze Threats



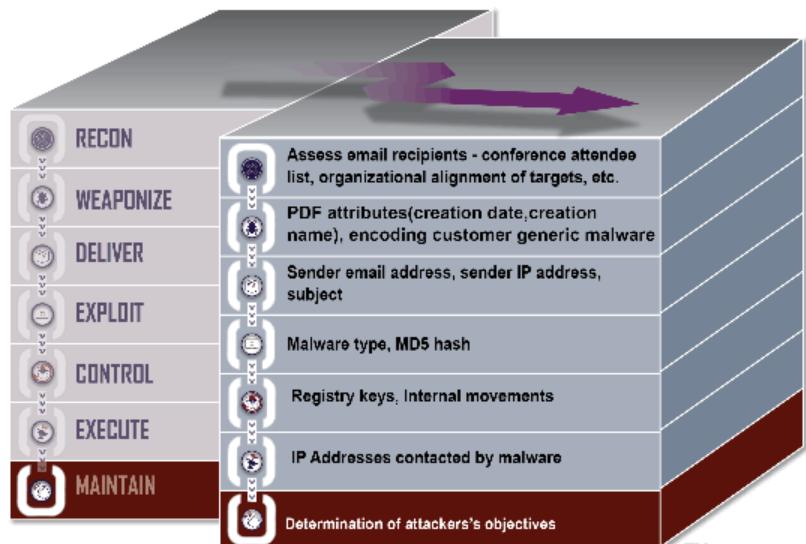
Intelligence from an Attack

Kill Chain Objective: Trojanized attachment with 0-day vulnerability delivered via target phishing email

Lateral Movement

Password Extraction and Cracking

File Exfiltration



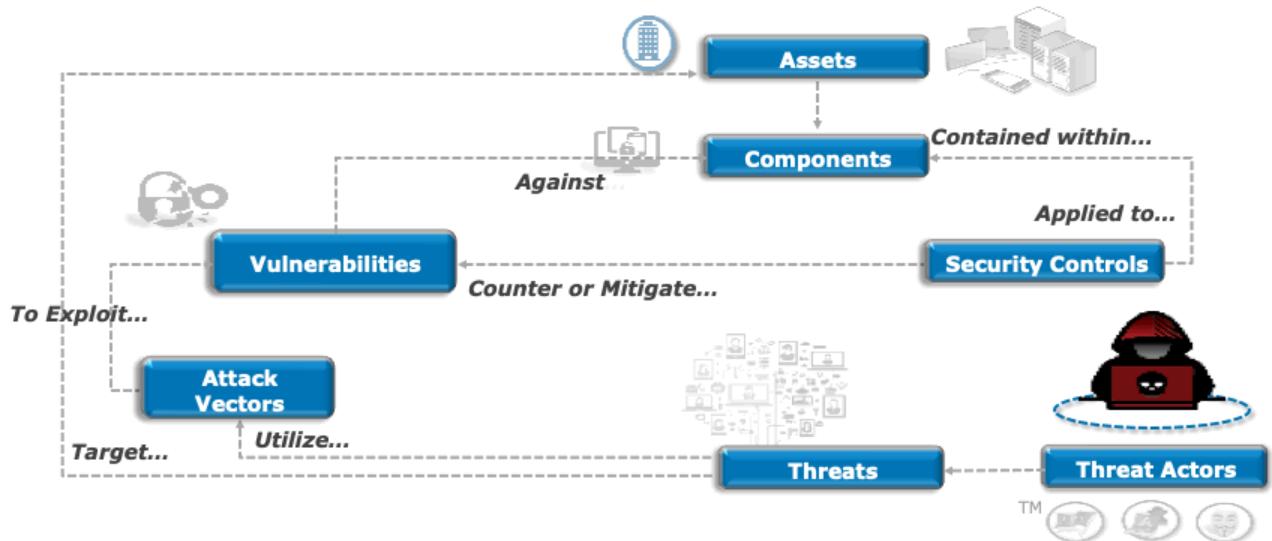
Selecting and Implementing Controls

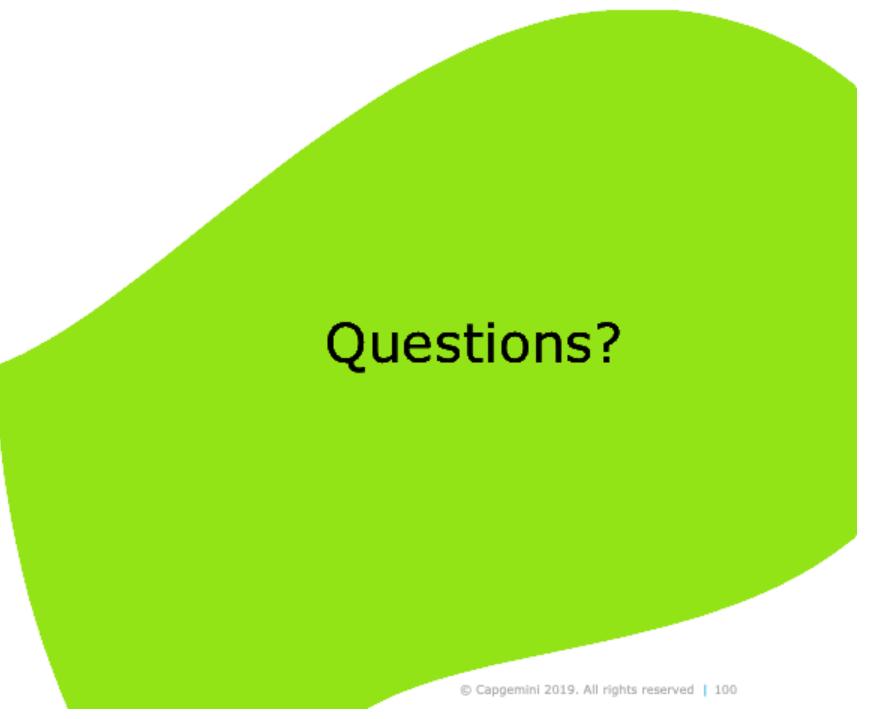


Selecting and implementing controls is the purpose of creating threat models.



Selecting Controls





Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 100

Security Controls



Capgemini

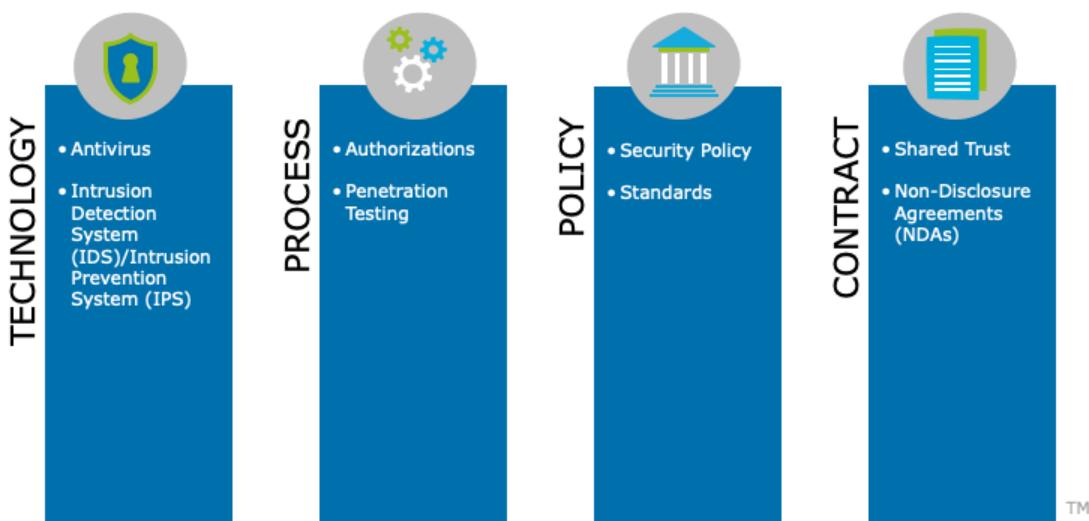
Foundational Analyst Security Training



Common Attack Characteristics

Attack or Vulnerability	Examples or Related Concepts	Cyber Kill Chain® Steps	Attack Surfaces/ Vectors	Targets	Primary Threat Types
Social Engineering	Email phishing, phone calls, identity spoofing, etc.	Steps 1 - 5	Telephones, Email, Social Media, Google	Human Trust	Typically Information Disclosure and Spoofing
Lateral Movement	<ul style="list-style-type: none"> • Pass-the-Hash Kit • WCE • Mimikatz • Gdump 	<ul style="list-style-type: none"> • Installation • Actions on Objectives 	<ul style="list-style-type: none"> • Windows > NT4 • Local Security Authority (LSA) Application Program Interfaces (APIs) and Memory Structures 	<ul style="list-style-type: none"> • Administrator Accounts • Privileged Accounts • Domain Service Accounts 	<ul style="list-style-type: none"> • Information Disclosure • Privilege Escalation • Lateral Movement
Web Application Attacks	Related: <ul style="list-style-type: none"> • Cross-Site Scripting • Lightweight Directory Access Protocol (LDAP) and Extensible Markup Language (XML) Injection 	<ul style="list-style-type: none"> • Exploitation • Command and Control (C2) • Actions on Objectives (AoO) 	<ul style="list-style-type: none"> • Hypertext Transfer Protocol (HTTP) GET/POST • Hypertext Markup Language (HTML) Forms • Web Services 	Web Applications with Relational Database	<ul style="list-style-type: none"> • Information Disclosure • Elevation of Privilege
Memory Corruption/ Remote Code Execution (RCE)	<ul style="list-style-type: none"> • Buffer Overflow • Heap Spray • Heap Overflow • ROP 	<ul style="list-style-type: none"> • Weaponize • Exploitation 	Any Code Written in C/C++ that can be User Manipulated		Initial Compromise/ Establish Foothold

Security Controls



Security Controls



There are challenges to working with security controls:

- Evaluate effectiveness objectively.
- Categorize and give context for the purpose.

Security Control Levels



The levels of security controls are as follows:

- Built in to infrastructure.
- Security services to integrate.
- Security functions that network will have to implement individually.

Controls Effectiveness



Causes:

- Misaligned Controls
 - Inadequate system understanding
 - Inadequate Controls
 - Inadequate threat analysis
 - Inappropriate Controls
- Misaligned Control of threat model
 - Inconsistent Controls
 - Lack of policies/enforcement of threat model

Examples of Security Controls



Securing the Operating System (OS)

Securing Applications

Layered Security

Endpoint Mitigations



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 107

Security Controls Effectiveness



Capgemini

Foundational Analyst Security Training

Reducing OS Attack Surface



An Attack Surface is the total of possible attack vectors that a threat can deploy against a network to infiltrate or exfiltrate data.

Reducing OS Attack Surface



Hardening the OS is the first step in protecting your system and reducing the Attack Surface.

Reducing Application Attack Surface



After securing the OS, installed applications must be protected, as they too contribute to the Attack Surface.

Reducing Application Attack Surface



Remove software that is no longer useful or is no longer being updated, including the following:

- Older versions of Flash and Java.
- Users installing their own software.
- “Default” software being included with legitimate software.

Reducing Application Attack Surface



Mitigating controls for more vulnerable systems include the following:

- Whitelisting vulnerable external servers.
- Firewalls for web applications.
- Extra care should be taken to fine tune endpoint security controls for users and assets on the network.

Layered Security



Layered security is the process of implementing multiple types of security at all levels of the organization, allowing the controls to intercept threats at multiple points.

Layered Security



There are multiple types of controls that can be created:

- Software (Firewalls, IDS, etc.)
- Physical (Gates, Locks, etc.)
- Hardware (Encryption)
- Authentication (Multi-Factor Authentication [MFA])
- Personnel (Separation of Duties)
- Many more...

Endpoint Mitigations



Antivirus

- Helps protect against broad-based attacks.
- Should be deployed to all supported endpoints.
- Features, such as Potentially Unwanted Programs, can help detect and remove tools that can leverage attacks.

Endpoint Mitigations



Host Intrusion Prevention System (HIPS) Software

- Expands the ability to watch executables.
- Can block the execution of software based on actions.

Endpoint Mitigations



Firewall

- Block known bad ports inbound or outbound.
- Enables the Security Intelligence Center (SIC) to log network traffic at the endpoint.
- Lock down endpoints when not on the corporate network.

Endpoint Mitigations



Application Whitelisting

- Extremely difficult to manage in a diverse enterprise.
- Whitelisting should be focused on critical systems.
- Advanced attacks almost always touch critical systems, including Domain Controllers, two-factor authentication systems, document repositories, etc.

Endpoint Mitigations



Endpoint Detection and Response (EDR)

- Allows for live querying of endpoint properties.
- Some allow for advanced response capabilities.

Endpoint Mitigations



Behavioral Analysis Tools

- Identify outliers that indicate malicious activity.
- Can look at different systems across the enterprise to identify anomalies within the environment.
- Provide logging around system activity that benefits post-intrusion analysis.

Endpoint Mitigations



Sandboxing

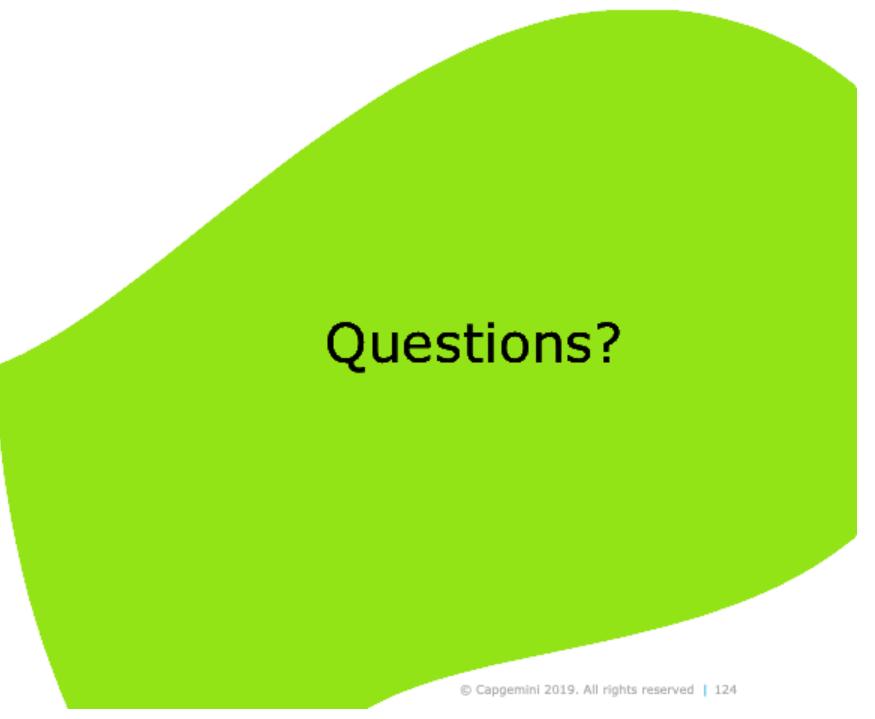
- Spin up micro-malware analysis sandboxes when new applications are launched.
- Monitor behavioral characteristics and terminate malicious malware.
- Can be challenging to configure in dynamic environments and should focus efforts on static environments, such as Active Directory or Domain Controllers.

Endpoint Mitigations



Data Loss Prevention (DLP)

- Focus on identifying sensitive information and logging.
- Analyst can leverage solution to gain additional visibility into endpoint activity.
- Prevent unauthorized transmission of company sensitive data.



Questions?



Foundational Analyst Security Training

© Capgemini 2019. All rights reserved | 124



People matter, results count.

This presentation contains information that may be privileged or confidential
and is the property of the CapGemini Group.
Copyright © 2019 CapGemini. All rights reserved.

About CapGemini

A global leader in consulting, technology services and digital transformation, CapGemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, CapGemini enables organizations to realize their business ambitions through an array of services from strategy to operations. CapGemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Learn more about us at
www.capgemini.com