
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
TM
Capgemini
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 1

Module 2 – Attacker Perspective

Capgemini

Threat Modeling and Analysis

Capgemini

Agenda

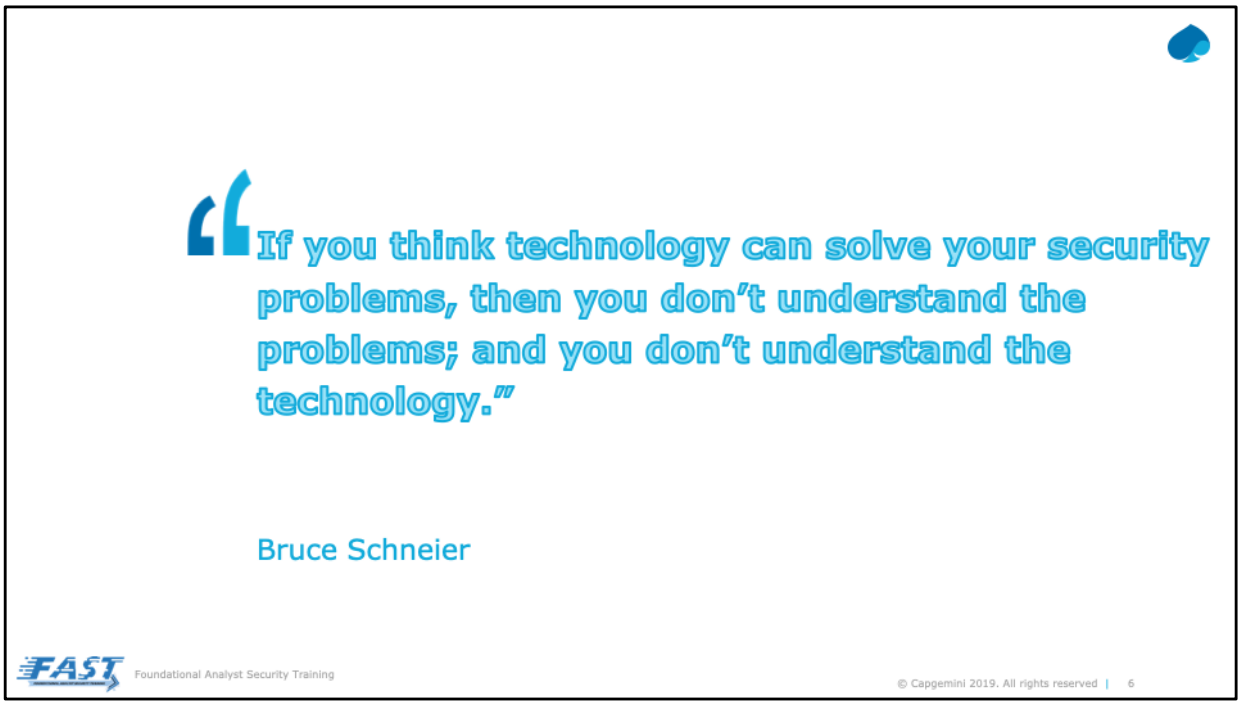
THREATS | THREAT MODELING | THREAT ANALYSIS METHODOLOGY |

During this module, we will talk about how threats are determined, and their possible activities are modeled and analyzed. Understanding how your adversary thinks and acts is essential for defending your networks.

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.



Bruce Schneier (/ˈʃnaɪ.ər/; born December 15, 1952[1]) is an American cryptographer, computer security professional, privacy specialist and writer. He is the author of several books on general security topics, computer security and cryptography. Schneier is a fellow at the Berkman Center for Internet & Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute. He has been working for IBM since they acquired Resilient Systems where Schneier was CTO.[2][3][4] He is also a contributing writer for The Guardian news organization.[5]

From: https://en.wikipedia.org/wiki/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.

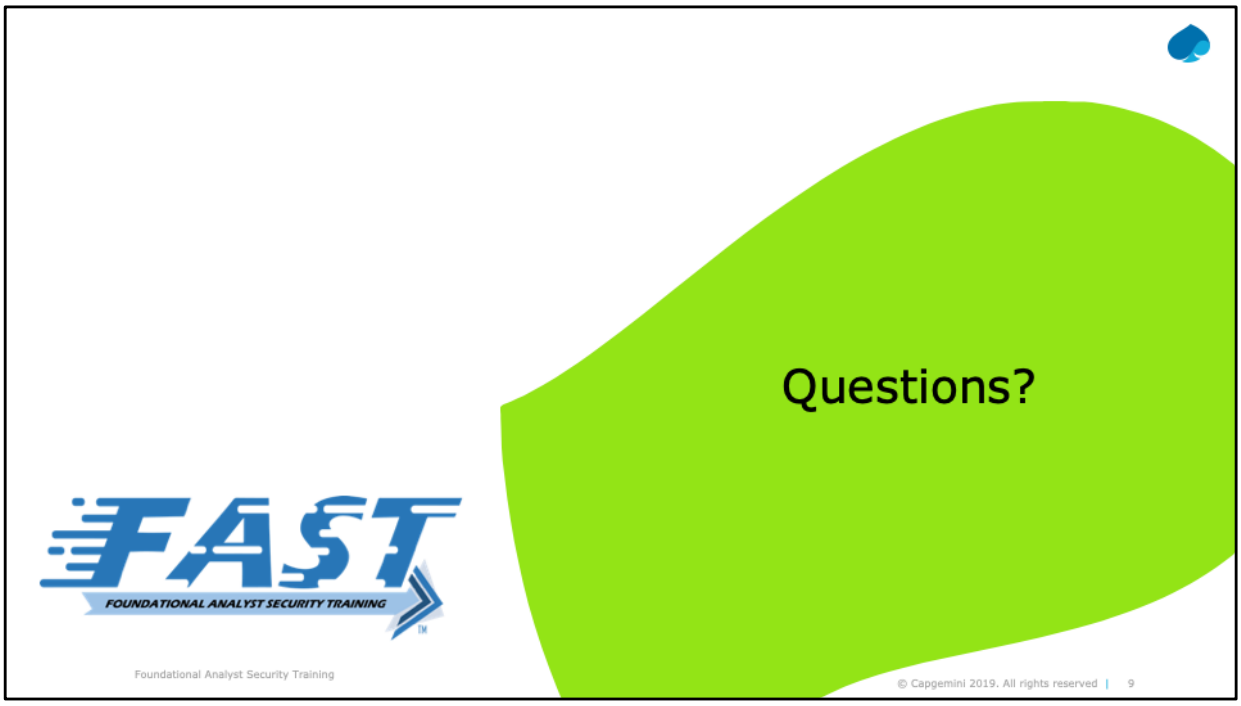
Purpose

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.

FAST Foundational Analyst Security Training

Just as with systems engineering and requirements engineering we must keep the user in mind in order to build the right system, a system that is usable. In building security controls, the threat is our user. If we do not keep the threat in mind, we risk building controls that do not combat real threats and real attacks


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 9

Threat Models

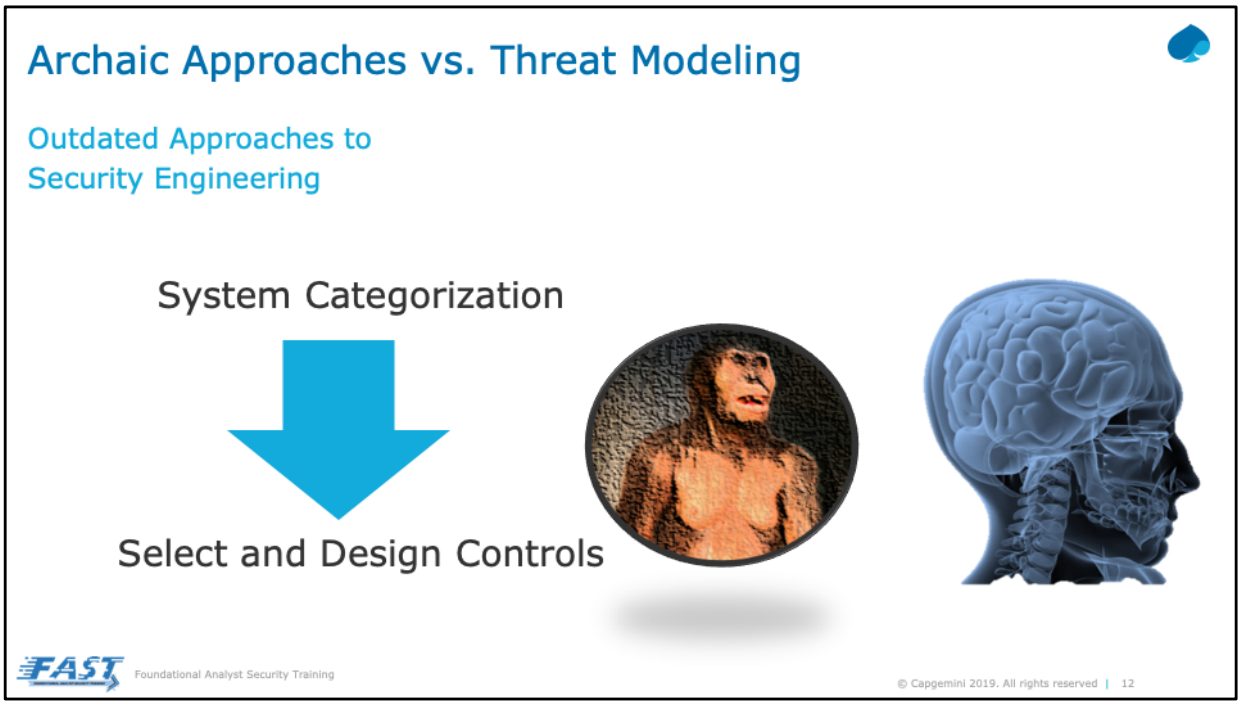
Capgemini

Wise Words…

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

–Neil Rerup

[Build Slide]
Keep this in mind, particularly when we get to decomposing systems



Instructor Notes:

Selecting controls based solely on the categorization of a system takes the thinking out of the process. And what you get is checklist security instead of effective security. Example 1: Do you lock your car in the grocery store parking lot? (yes) Do you lock your car when it's in your garage? (no). Why not? Did you car lose value (lower category) when it's in the garage? No, but there are other compensating controls in place.

Example 2: Encryption at rest requirement. We all have full disk encryption on our laptops. What attack vector does that control mitigate? Physical theft of your hard drive while the computer is turned off. That's it. No help against remote attacks. No help against theft when it's powered on.
Be sure to reinforce the difference of building a system that provides security services – and securing a system that is being built. And you still have to secure the security services – so use case #2 applies to all.

Security Engineering Methodologies

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

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

FAST Foundational Analyst Security Training

Apply a "Threats First" Approach across Architecture, Engineering, and Operations
- Vs. a Controls-First or Vulnerabilities-First Approach

Why?
- Threats are the constant
- Threat agents execute the attacks
- Threats do the damage

Controls-First approach is usually about Compliance

Vulnerabilities-First approach should be IT 101

Security Engineering Methodologies

Controls Driven

Vulnerability Driven

Threat Driven

Select controls from a catalog, based on system criticality.

Castle doctrine, buy all the tech, hide behind it and hope it stops the bad guys.

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.

You will never remove all vulnerabilities, this approach is reactive.

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.

Controls Driven - Concerns

Controls do not actually mitigate specific threats.

Adding more controls is not always effective.

Adds cost and increases complexity.

When you increase complexity, there is a good chance you will introduce more vulns

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.

FAST Foundational Analyst Security Training

Great for compliance

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.

FAST Foundational Analyst Security Training

This picture was actually taken by one of our instructors near his home, it is a hearty gate meant to keep unauthorized people out, however without a fence to pair it with, its effectiveness is mitigated to 0.

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.

FAST Foundational Analyst Security Training

Vulnerability driven approaches means you are constantly chasing security, not being proactive.

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.

FAST Foundational Analyst Security Training

Threat Modeling is not for meeting requirements laid down in generic standards.

Aaron, I sourced this information here https://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf

This is new content…..

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.

FAST Foundational Analyst Security Training

Apply a “Threats First” Approach across Architecture, Engineering, and Operations
- Vs. a Controls-First or Vulnerabilities-First Approach

Why?
- Threats are the constant
- Threat agents execute the attacks
- Threats do the damage

Controls-First approach is usually about Compliance

Vulnerabilities-First approach should be IT 101

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.

FAST Foundational Analyst Security Training

 | 26

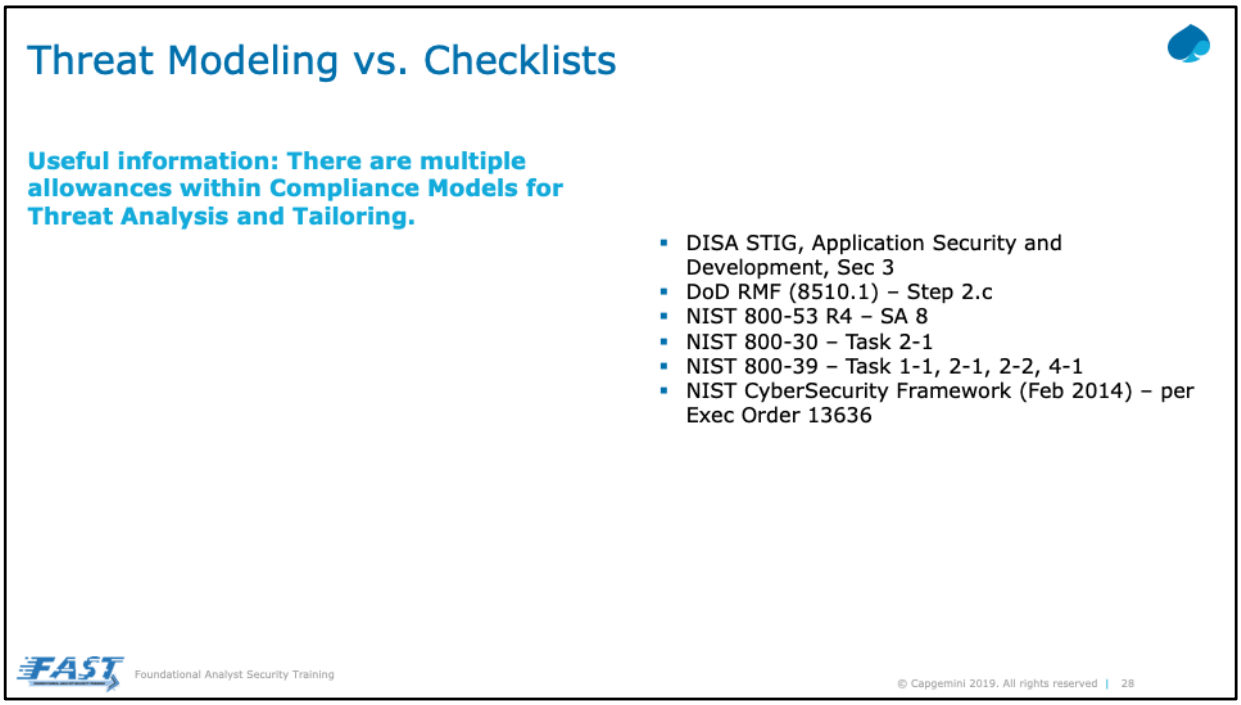
Often threat modeling is neglected, because it is not a direct artifact for compliance. Most audits do not specifically ask for it.

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.



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:

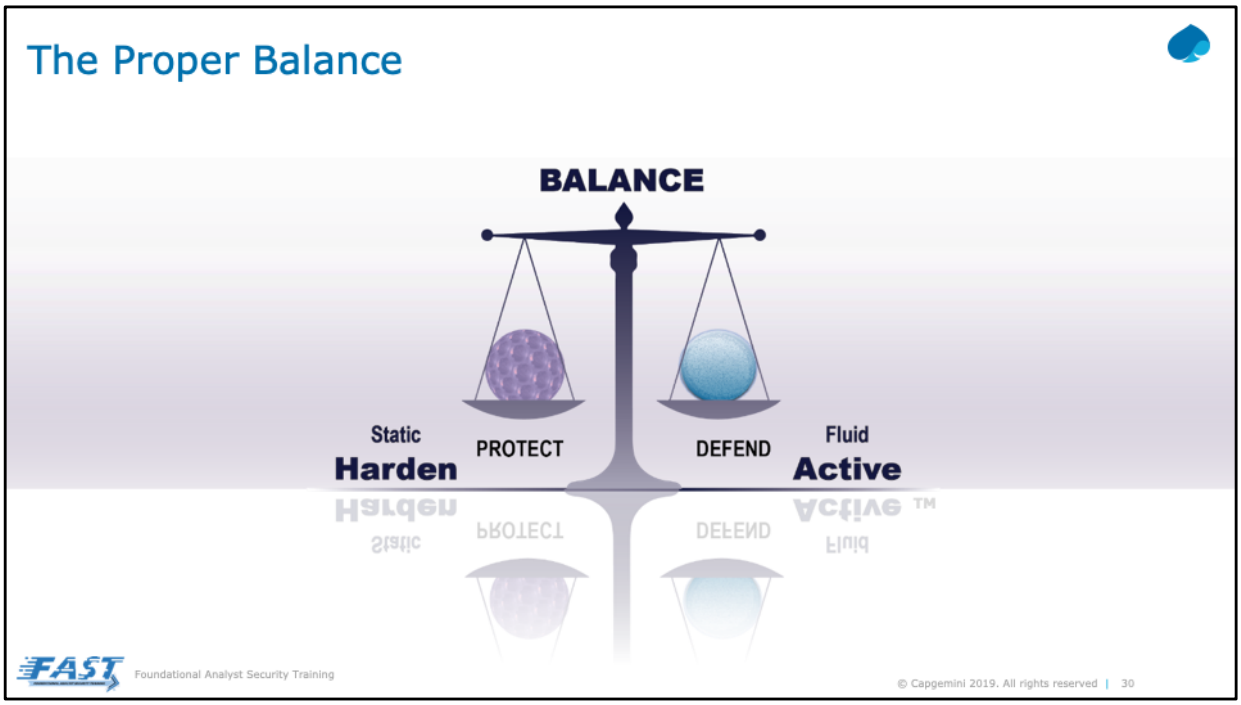
- Select protection and appropriate compensating controls.
- Design the system to be defended while it is built and operated.

FAST Foundational Analyst Security Training

2 key pieces to a threat-driven approach –

Threat Analysis

Threat Intelligence



Any organization must consider both Protect and Defend aspects of cyber security. Typically “Protect” is more aligned to Arch/Engr and Assessments from a role/responsibility perspective – while “Defend” is more aligned to Ops, Incident Response and Intel analysis. Also – “Protect” is relatively static in nature, while “Defend” connotes an active involvement.

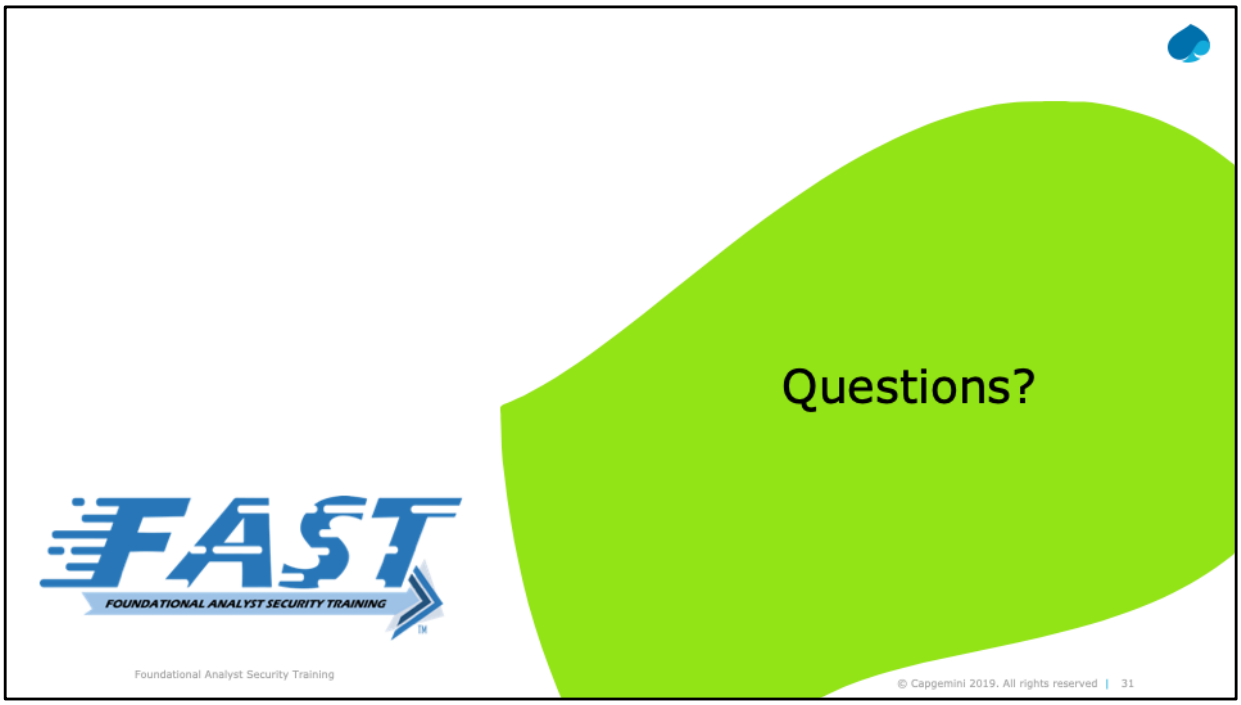
An organization that focuses too much on either side will have large gaps in its cyber security posture.

Examples:

- Too heavy on “Protect” leads to an extremely reactive operational security environment (i.e. “whack a mole”), and prevents an organization from learning and adapting over time based on its defensive capabilities and historical analysis
- Too heavy on “Defend” leads to large gaps in both preventative measures and also prevents maturity in the infrastructure and systems architectures. Additionally – without a solid Protect baseline – defenders waste valuable time on individual vulns and incidents vs. building an intelligence base and identifying patterns

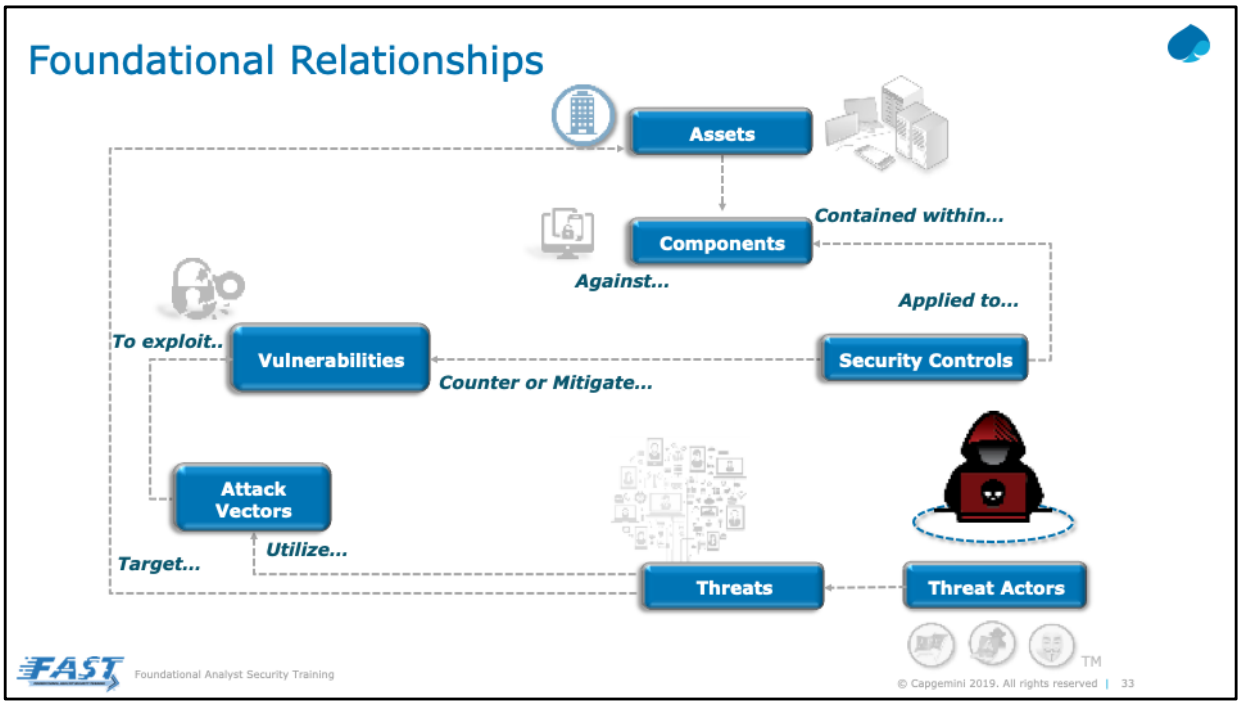
The better you get at “Protect” - the easier it is for the Defenders. This is why it is critical to have two-way, continuous communications and interactions between the teams/groups that provide these functions.

Question to the group: where do you think AEP is currently at ? (answer: LM has the scale tipped more on the “Defend” side of the scale. This workshop is designed to help properly align the Protect side of the scale.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 31

Defining Threat Concepts

Capgemini

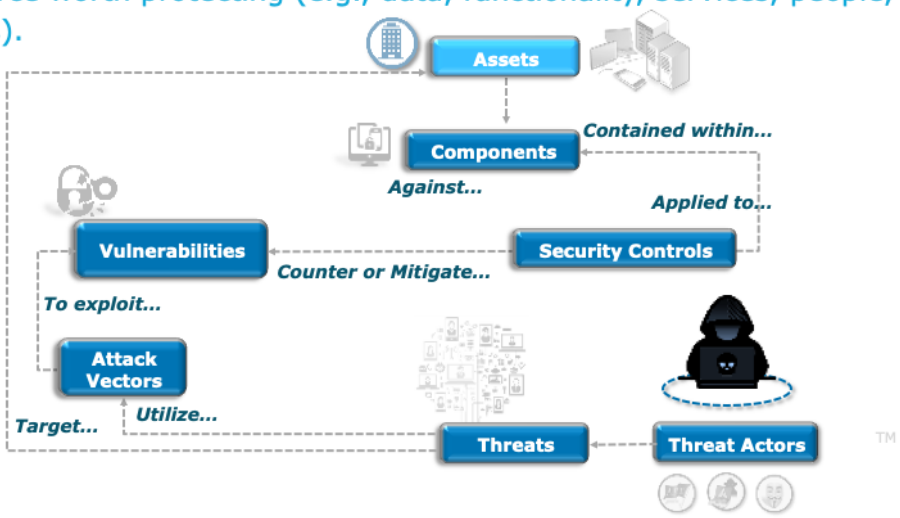


Instructor Notes:

In order to accomplish threat modeling these are the basic building blocks required to build a threat model.

Important Vocabulary

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



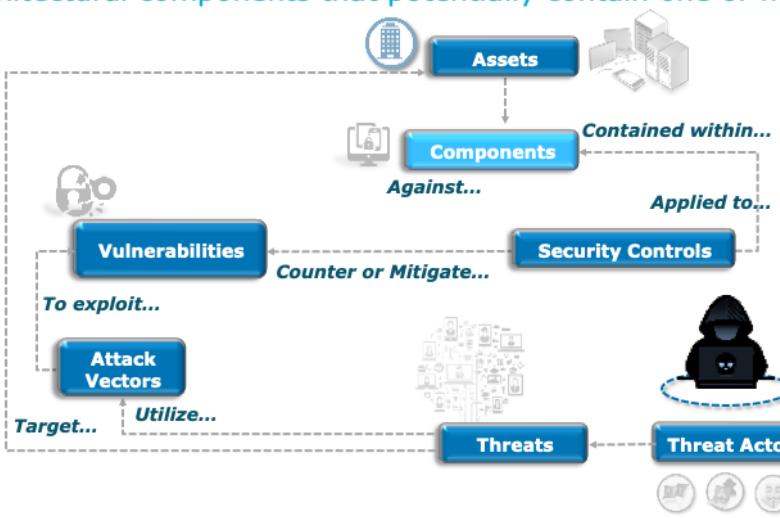
FAST Foundational Analyst Security Training

 | 34

Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.

Important Vocabulary

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

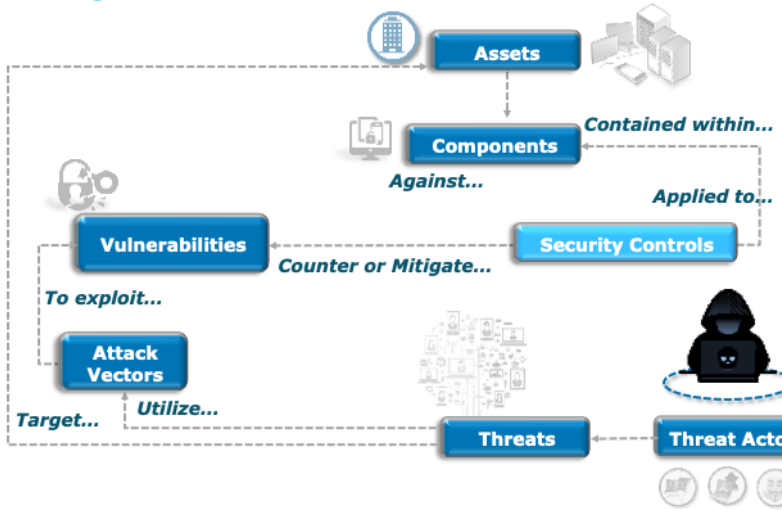


FAST Foundational Analyst Security Training

Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.

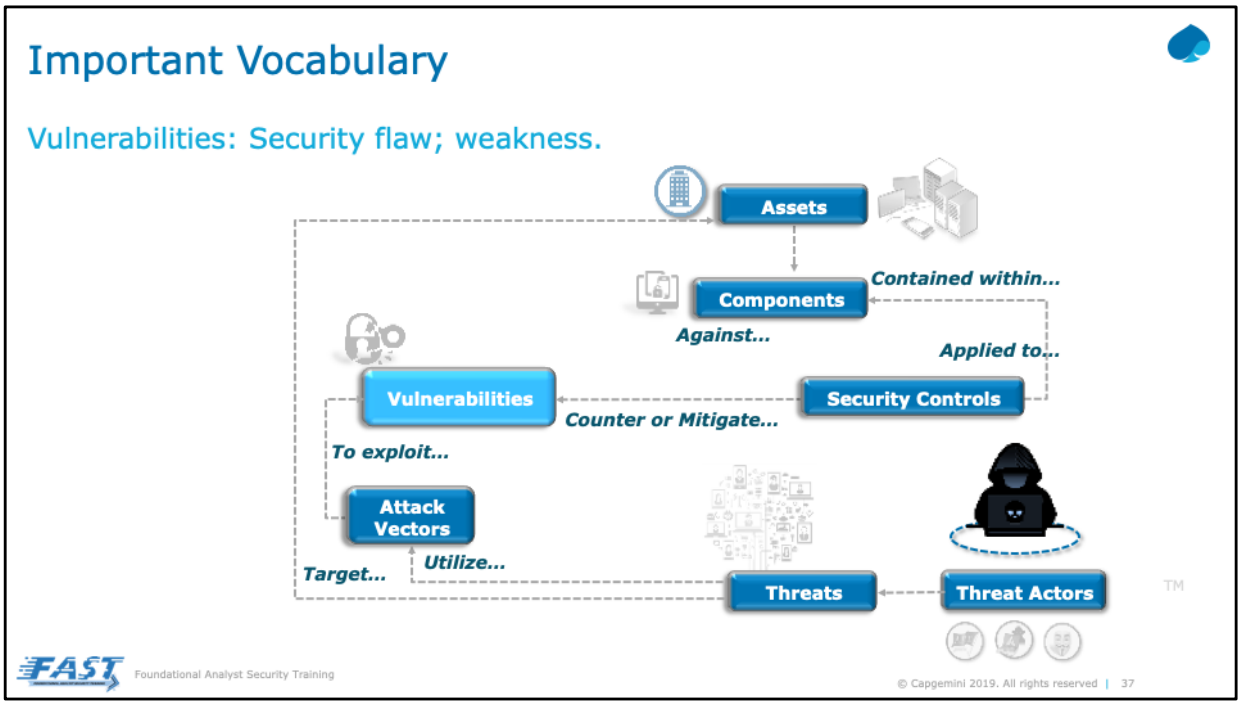
Important Vocabulary

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



FAST Foundational Analyst Security Training

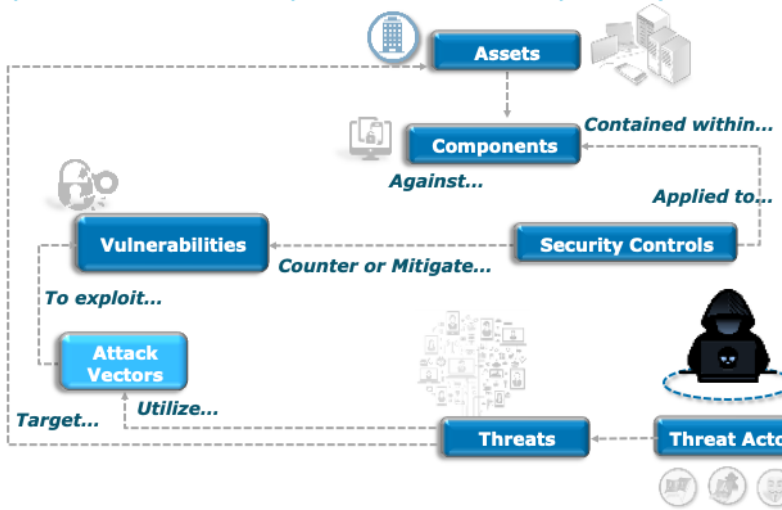
Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.



Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.

Important Vocabulary

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



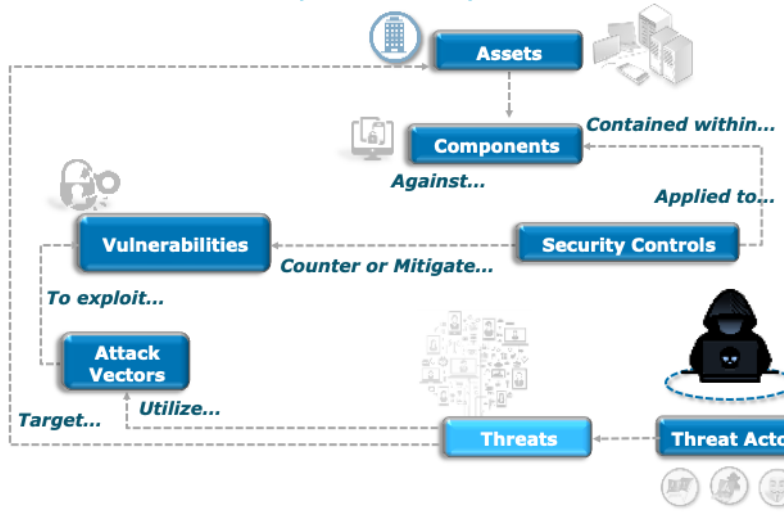
FAST Foundational Analyst Security Training

 | 38

Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.

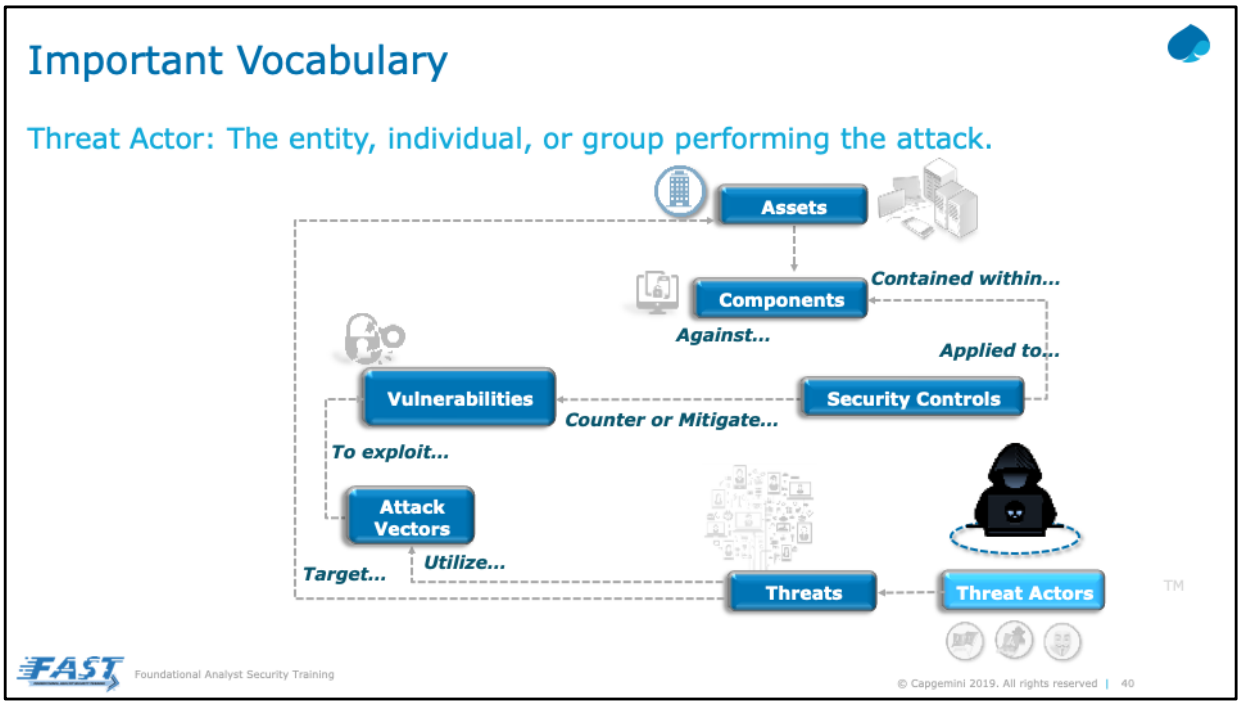
Important Vocabulary

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

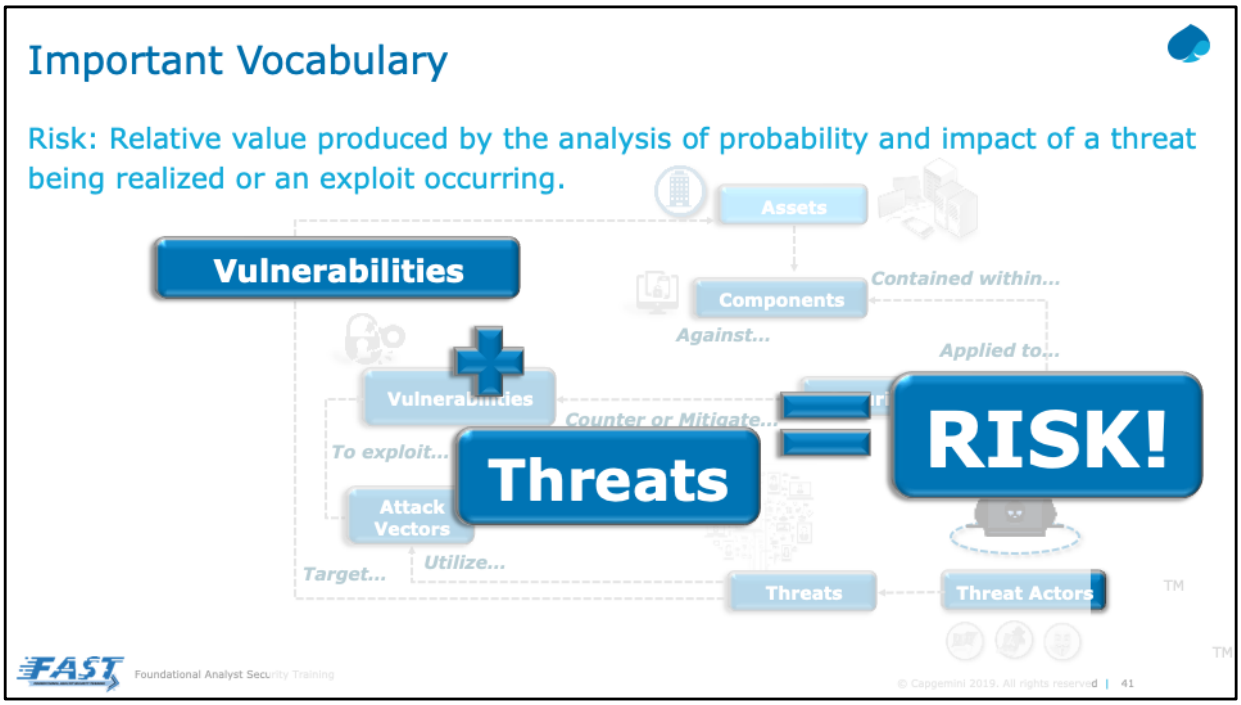


FAST Foundational Analyst Security Training

Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.



Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.



Note: Some communities (e.g., CIRT / DIB) use “threat” to refer to an actor. This is an artifact of history and perspective. The important part is to be aware of the meaning in your context. For this class, we use the definitions on this slide.

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.

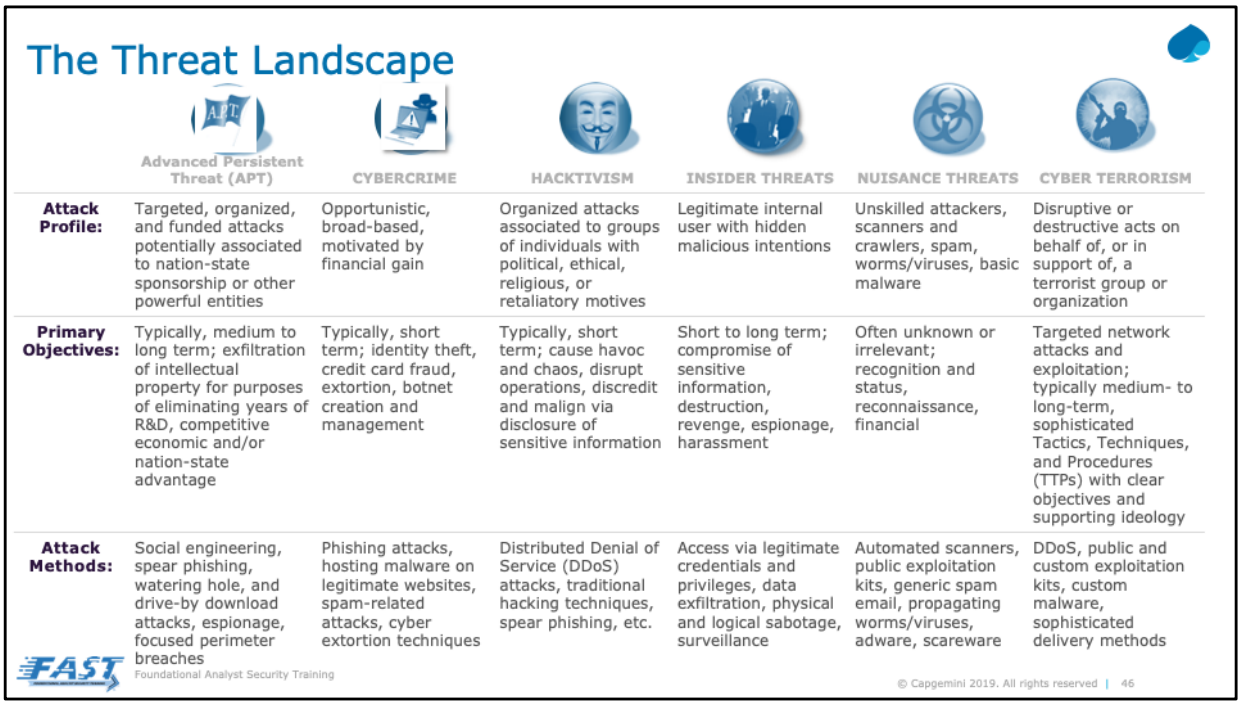
Threat vs. Risk – A House in the City

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?



Combine these two by talking about each actor on a separate slide,

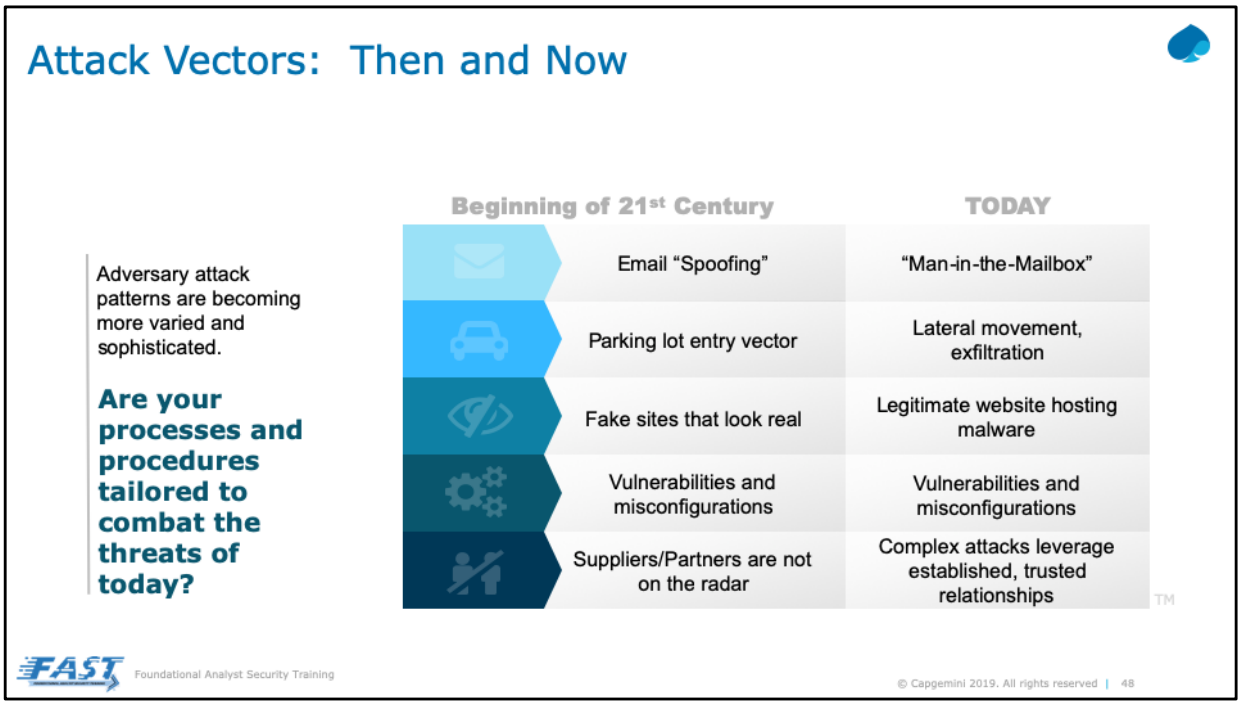
Threat Actors (aka Attack Agents)

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
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

FAST Foundational Analyst Security Training

This is not a comprehensive list, and it is broken up by “class” or “category” of threat actor. But it does cover the most well-known classes of threat actors.

Combine these two by talking about each actor on a separate slide,

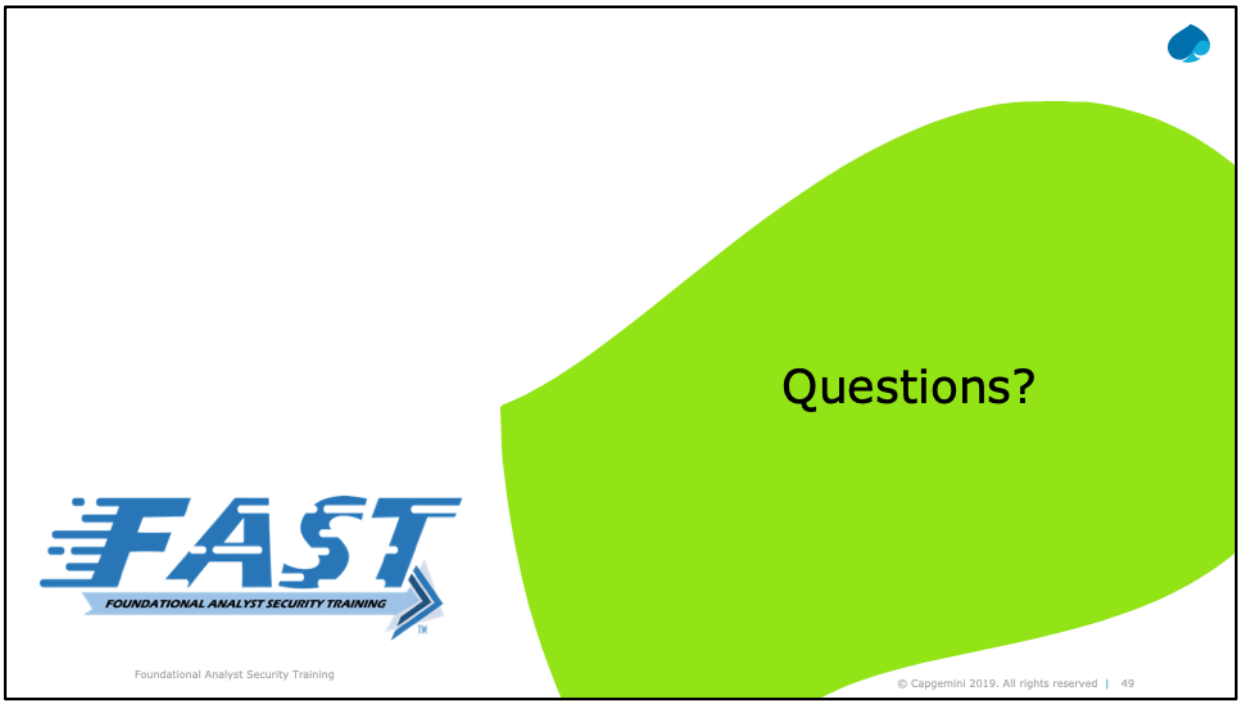


Instructor Note:
Its not what you are doing today, but knowing that threat's attacks evolve year to year, and even day to day.

How dated are your response procedures?

Compare and contrast – the threat is greater
Most orgs have trained to the threats of 2006 but the new kids on the block are escalating the threat

- Email vector
- Portable media
- Website vector
- Server vector – some things never change – still something the industry is struggling with – resignation that patching and system configuration and web server hardening are basic tenants that still need to be managed
- Partner vector


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 49


Why is this Important?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Capgemini
Foundational Analyst Security Training

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.

FAST Foundational Analyst Security Training

Instructor Notes:

Threat Modeling is an evolving process, it is constantly evolving to combat new threats.

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

FAST Foundational Analyst Security Training

 | 52

Remember the value of these resources is relative.

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 perform outside of specifications?"

Instructyo

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…

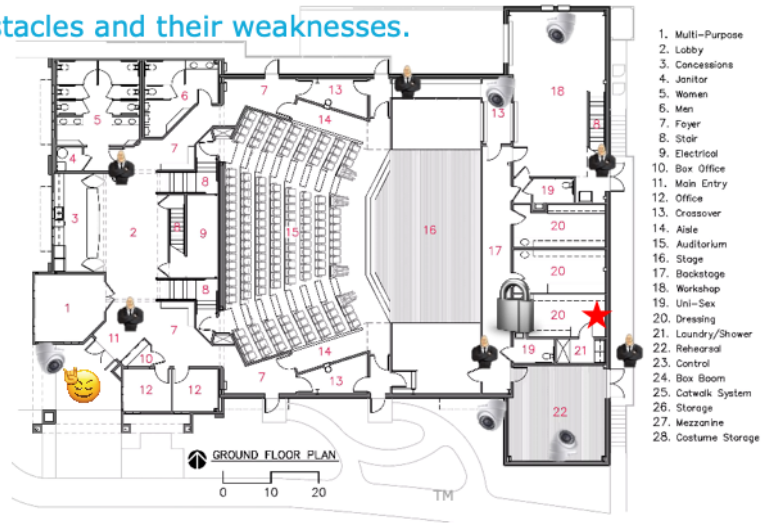
*So, how would **YOU** do it… ???*

FAST Foundational Analyst Security Training

Lets step out of the IT and Security realms, and do it in another arena, literally….

Mindset

Consider the current obstacles and their weaknesses.



FAST Foundational Analyst Security Training

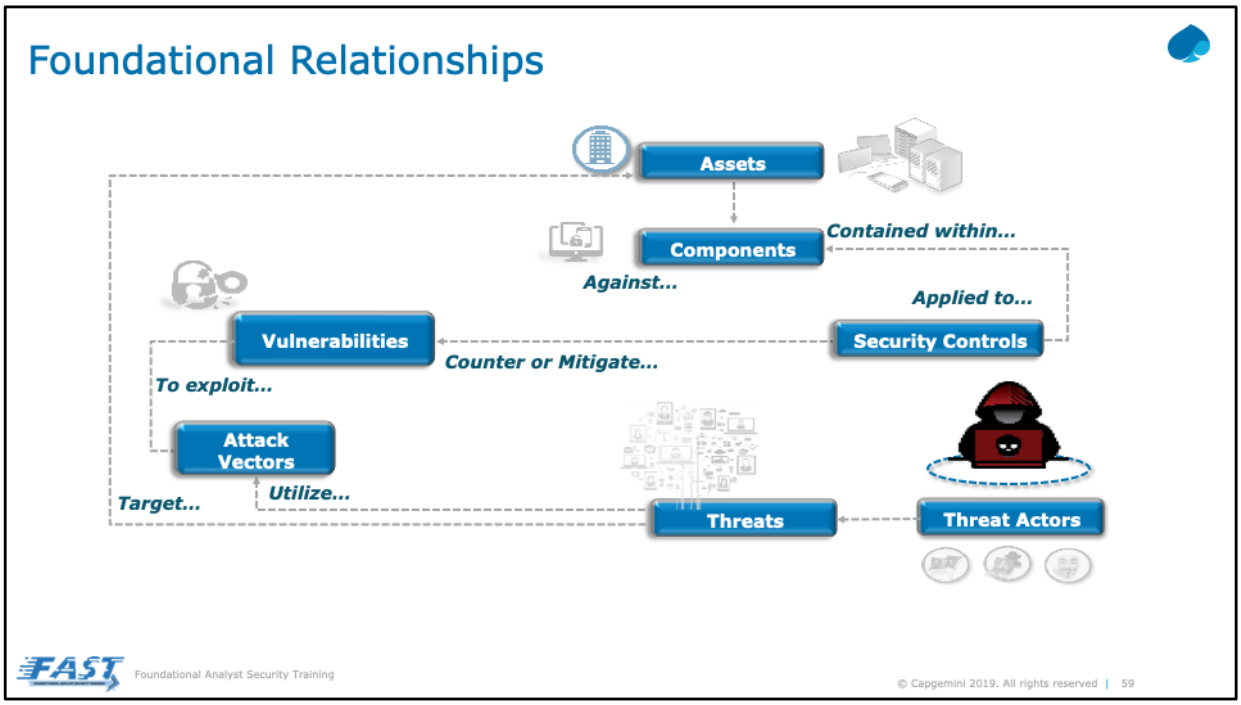
[Build Slide]
Discussion points:

- What are the assets? (Stick with physical for this example)
- Is the money the most valuable thing in the bank? Do the assets from the bank's view and the attacker's view differ?
- How would you go about getting the money (or other asset)?
- What do you need to know to pull it off? Remember, you want to get away with it, and make it worthwhile!
- Would you do it alone? If not, how and who would you recruit?

- Guidelines, you cant blow anything up, NO NUKES, and you cant kill anyone, remember we want to have fun and meet our favorite artist, not go to prison for the rest of our lives.

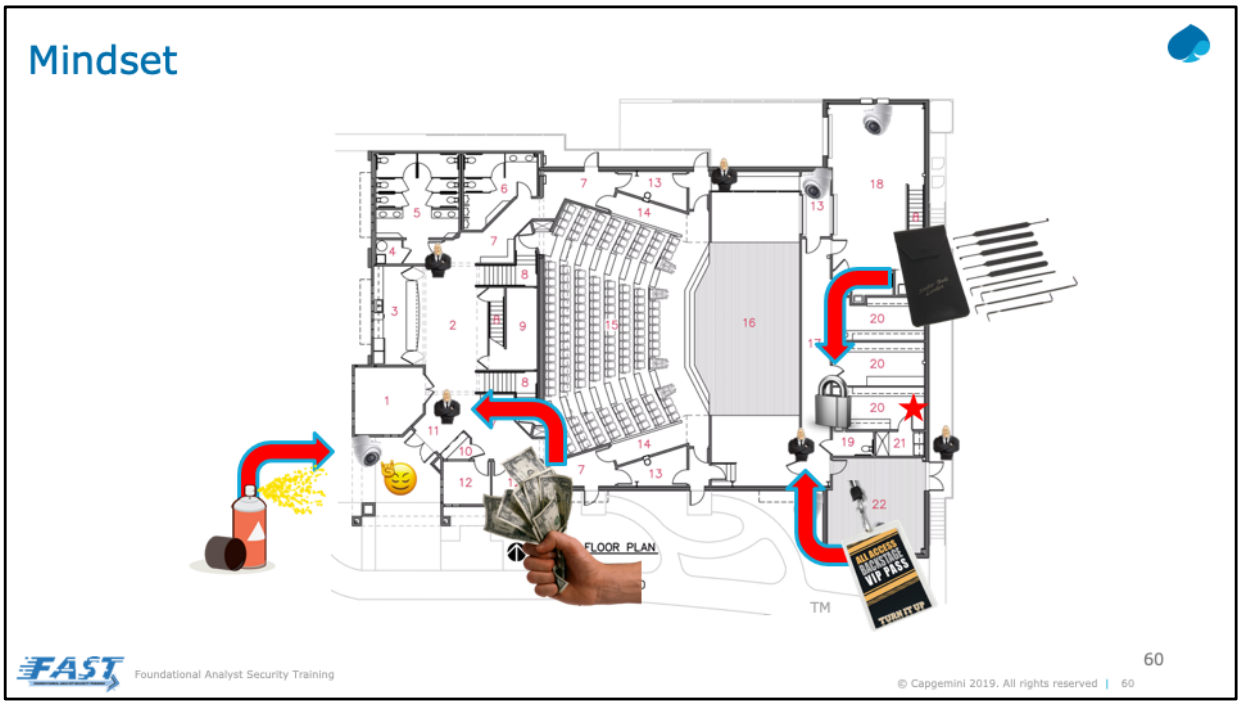
- This explains relative value, meeting a pop star may be worth a night in jail for trespassing to you, but not to me, but life in prison would only be worth it for a sociopath….

- Value is not determined by you, it is determined by the attacker.

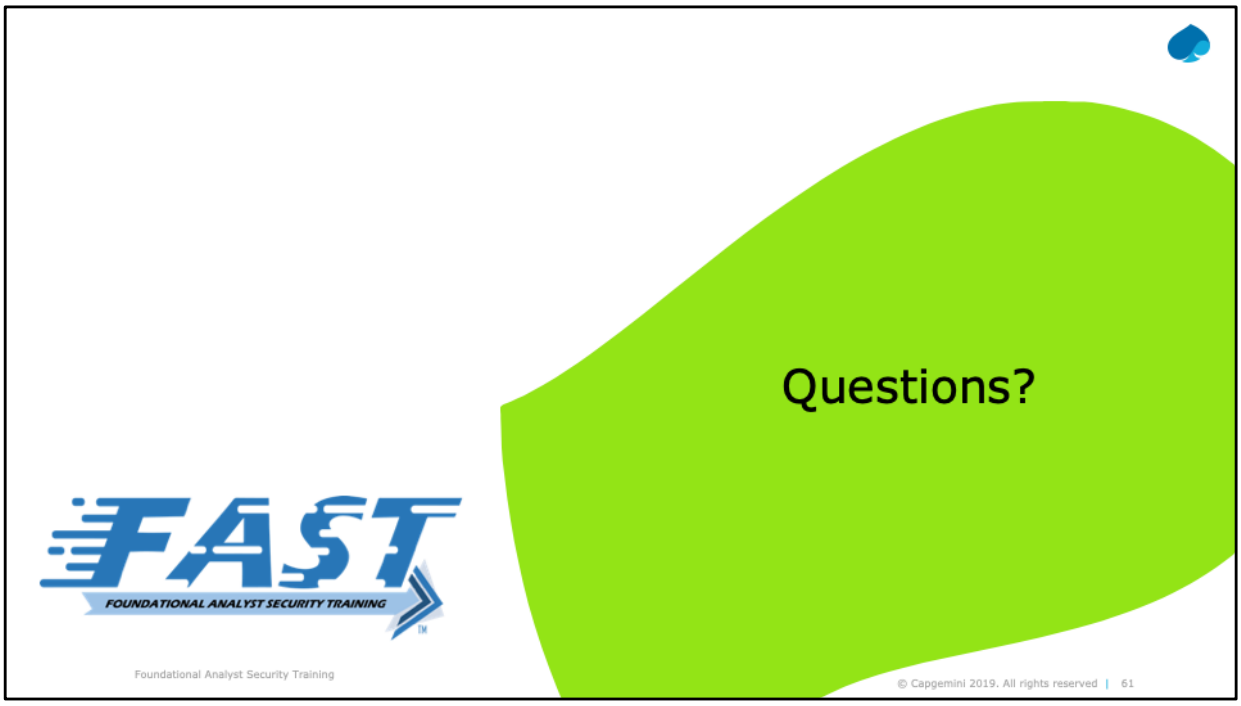


Instructor Notes:

In order to accomplish threat modeling these are the basic building blocks required to build a threat model.


Mindset
FLOOR PLAN
ALL ACCESS BACKSTAGE VIP PASS
TURN IT UP
FAST
Foundational Analyst Security Training
60
© Capgemini 2019. All rights reserved | 60

[Build Slide]


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 61

Threat Models: Analysis

Capgemini

Disclaimer

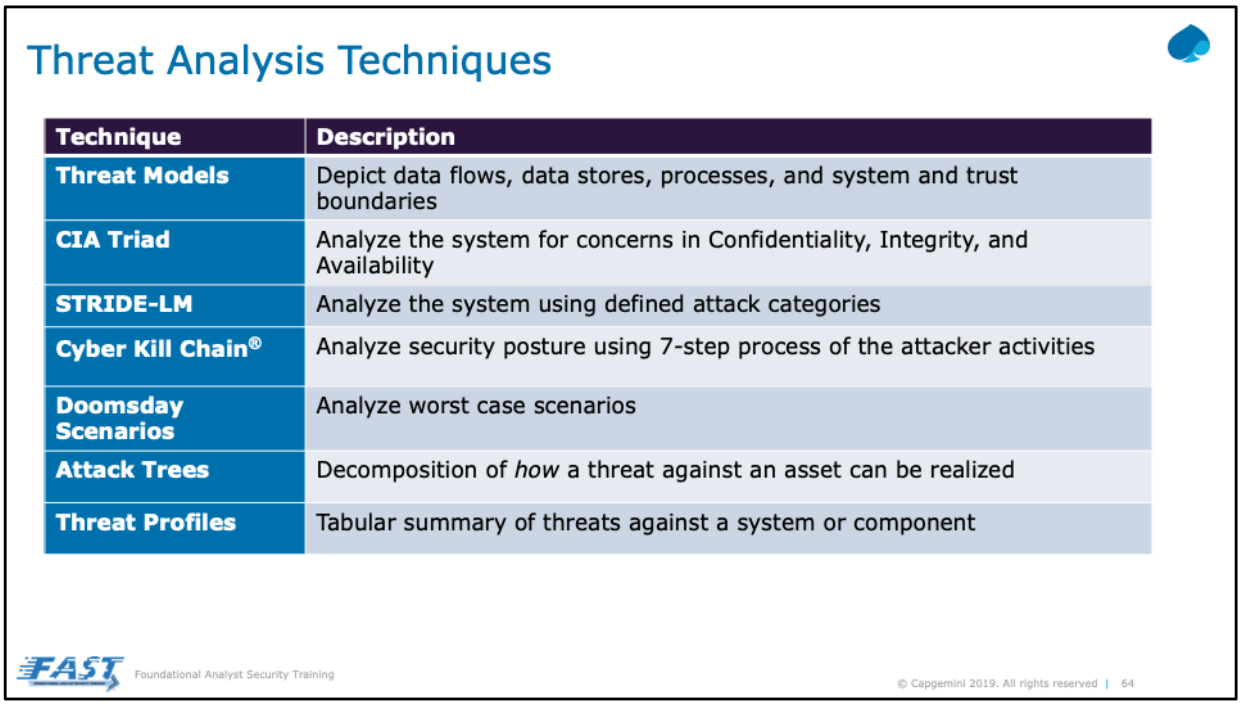
This section presents tools that can be used to perform attack analysis.

- 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.



Use what makes sense for your system, analysis needs, and communications goals.

These techniques are not mutually exclusive
Mix/match and combine usage of them as needed

Common Techniques:

- Confidentiality, Integrity, and Availability (CIA)
- STRIDE LM
- Lockheed Martin Cyber Kill Chain® (CKC)
- Misuse and Abuse Cases
- Doomsday Scenarios

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.

FAST Foundational Analyst Security Training

In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Interesting note if it seems applicable….

While CIA is the standard for most IT networks, in the OT environment, it is actually AIC, because up time is king….. Everything is relative to priorities…

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

Foundational Analyst Security Training

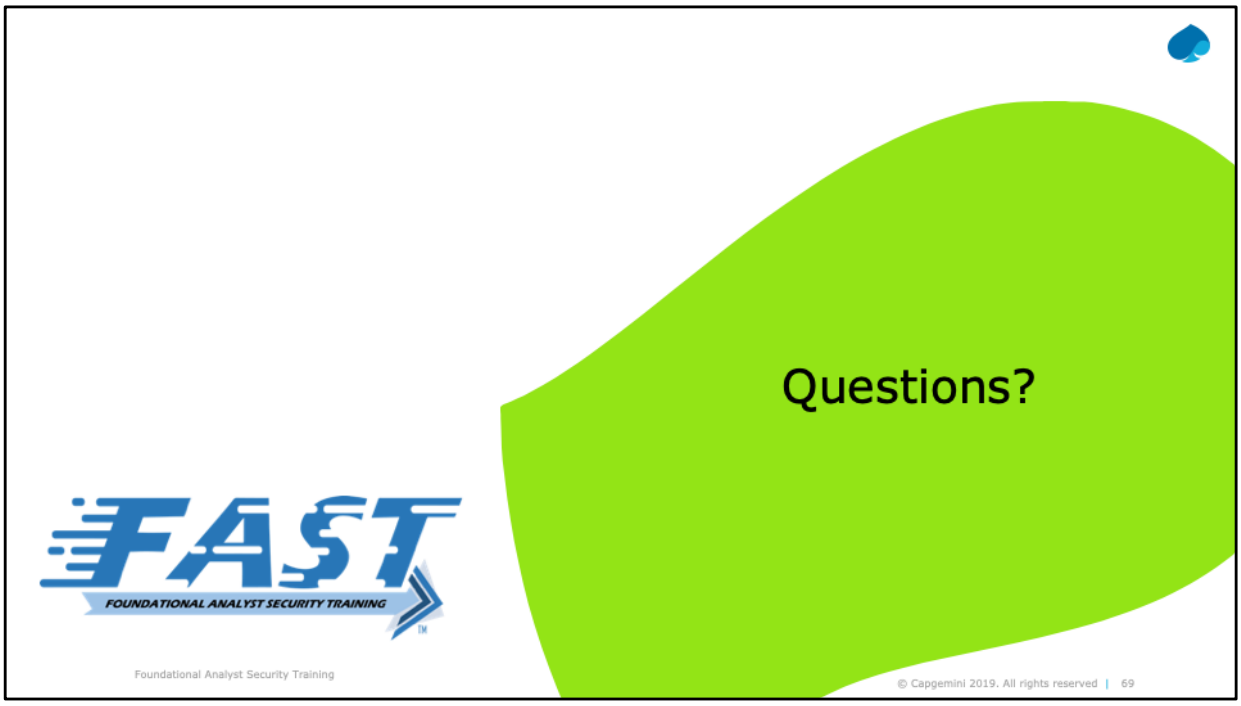
STRIDE-LM and the CIA Triad

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

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

STRIDE-LM and the CIA Triad

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


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
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	• Spoofing • Tampering • Repudiation • Information Disclosure • Elevation of Privilege	• Unauthorized Data Access and Modification	• Database Server • Web Service • Web Application	• Hardening • Secure Coding • Least Privilege
TimeExpense Data	• Spoofing • Tampering • Repudiation • Information Disclosure • Elevation of Privilege	• Unauthorized Data Access and Modification	• Mainframe • Web Application	• Hardening • Secure Coding
PassTicket	• Spoofing	• Unauthorized Access to Mainframe	• Web Service • PassTicket Generation Service	• Least Privilege • Restricted Access

FAST Foundational Analyst Security Training

An example of a Threat Profile for a smart card system assessment. FYI – this profile is taken from the threat model/assessment presented on Slide 57 in the Threat Model section (smart card ecosystem)

It is not necessary to walk through this entire slide. Reinforce the reasoning for the structure of the profile (i.e. rows and columns) and the importance of aligning assets <-> threats <-> attack surface <-> controls.

But do discuss the Controls for the SmartCard OS asset… some very good discussion points here.

- Code Audits: Yes, this is a good control. However, is it practical to audit the code on every card received? No – so only periodic audits are performed and this is essentially a Risk Acceptance item.
- Contract language: Not all controls are technical or procedural
- What control is not on here (that many folks think should be…) ? Code signing. Why is code signing not a viable control for this threat/attack vector? Because the code has been tampered with at the source. So all you get is a verified non-tampered malicious code ☺

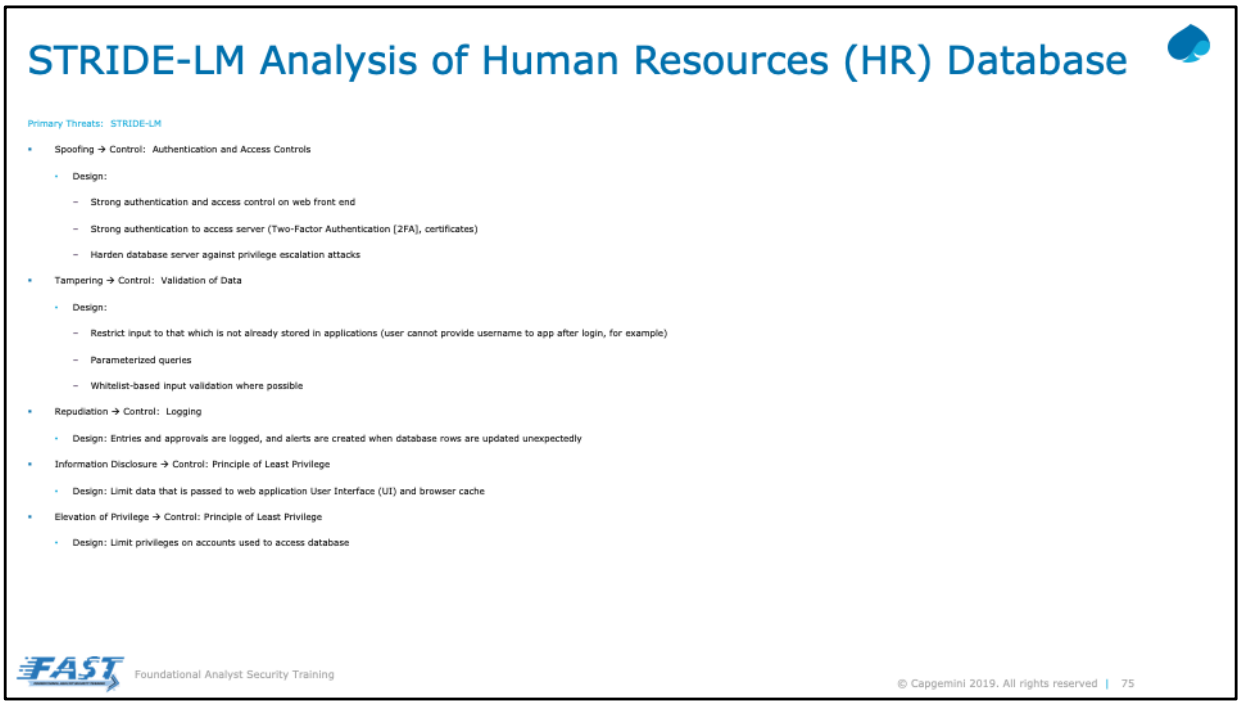
Threat Profile Example

Technique	Description
Asset	HR Database
Threat Types(s) STRIDE-LM	Spoofing Identity, Tampering, Repudiation, Information Disclosure, Elevation of Privilege
Attack Surface	• Database files on the server • Database server itself • Web service that interacts with HR database • Backup servers and services
Attack Vector	• Gain access to database server and download database files • 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
Threat Agents	• Malicious insider/corporate espionage • Threat actor looking for financial gain • Disgruntled employee
Compromise Result	• 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

FAST Foundational Analyst Security Training

Actual example filled in. Note that this was performed at the ConOps Phase of work.

Q: Why do we define all of the components in the attack surface?
A: To assist in the identification of attack vectors; To determine which locations controls can be allocated.



Primary Threats: STRIDE

Spoofing: Users attempt to become other users

Tampering: Users manipulate data sent to clients

Repudiation: Users change data after the fact with no

Information Disclosure: Browsers may leak data

Elevation of Privilege: User may try to access other data

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.

FAST Foundational Analyst Security Training

 | 76

- Good for validating gaps after a ”successful” incident

Threat Profile Lessons Learned

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

Summary of Threat Analysis Techniques

Technique	Description	Best Used For
Threat Models	Depict data flows, data stores, processes, and system and trust boundaries	• 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	• Basic security analysis • High level brainstorming • Defining security goals
STRIDE-LM	Method of analyzing system using defined attack categories	• Analyzing threats to system assets
Cyber Kill Chain®	Seven-step process of attacker activities	• Understanding adversary TTPs • Evaluating controls • Framework for threat intelligence

FAST Foundational Analyst Security Training

Use what makes sense for your system, analysis needs, and communications goals.

These techniques are not mutually exclusive
Mix/match and combine usage of them as needed

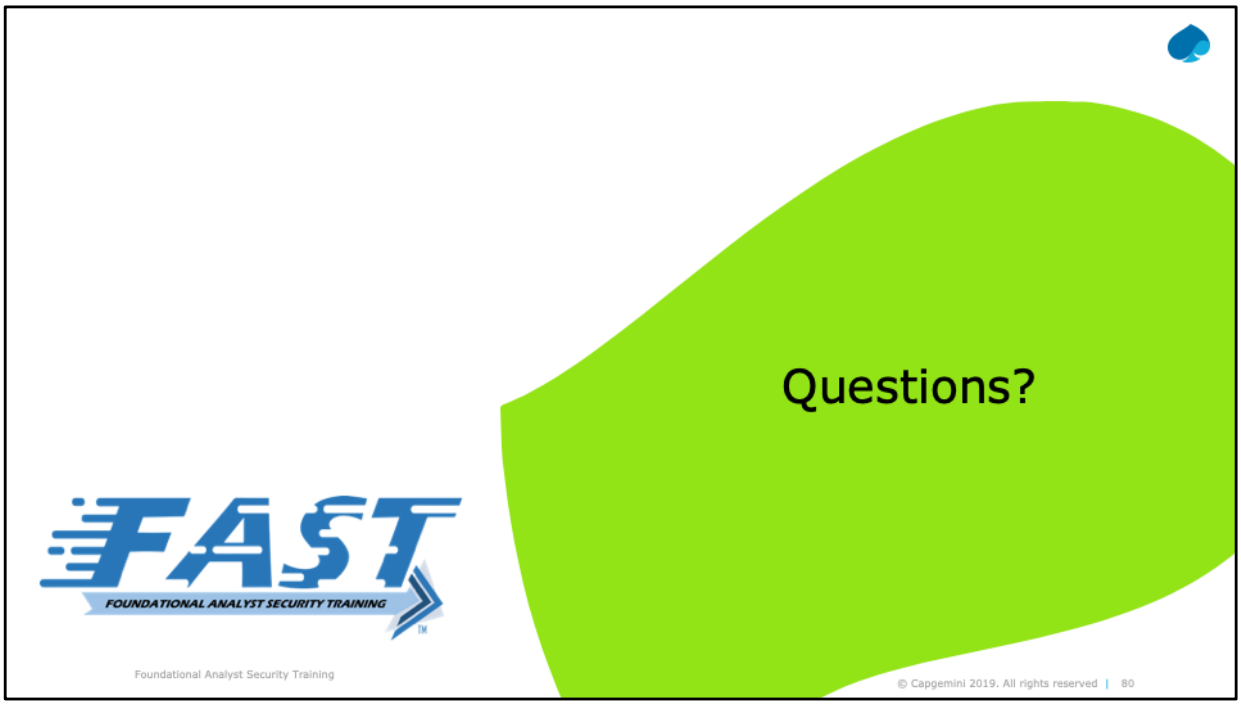
Summary of Threat Analysis Techniques

Technique	Description	Best Used For
Doomsday	Analysis of worst-case scenarios	• Identifying critical business threats
Attack Trees	Decomposition of *how* a threat against an asset can be realized	• Detailed analysis of specific attacks • Generally narrow in scope
Threat Profiles	Tabular summary of threats against a system or component	• Communications • Decision-making • Cause and effect documented

FAST Foundational Analyst Security Training

Use what makes sense for your system, analysis needs, and communications goals.

These techniques are not mutually exclusive
Mix/match and combine usage of them as needed


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
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.

FAST Foundational Analyst Security Training

In order to combat threats, one must understand how threats attack systems

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.**

FAST Foundational Analyst Security Training

Everyday users are the weakest link in the security chain
Attackers tempt users online, or in person to violate network policies.
Compromised user account are responsible for over 90% of malware installation.
Attackers can escalate their access to a user account to an administrative account.
Although this does leave a log trail for post-incident review.

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.

Talk about admins not using admin accounts for routine use.

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

Security Controls

Capgemini

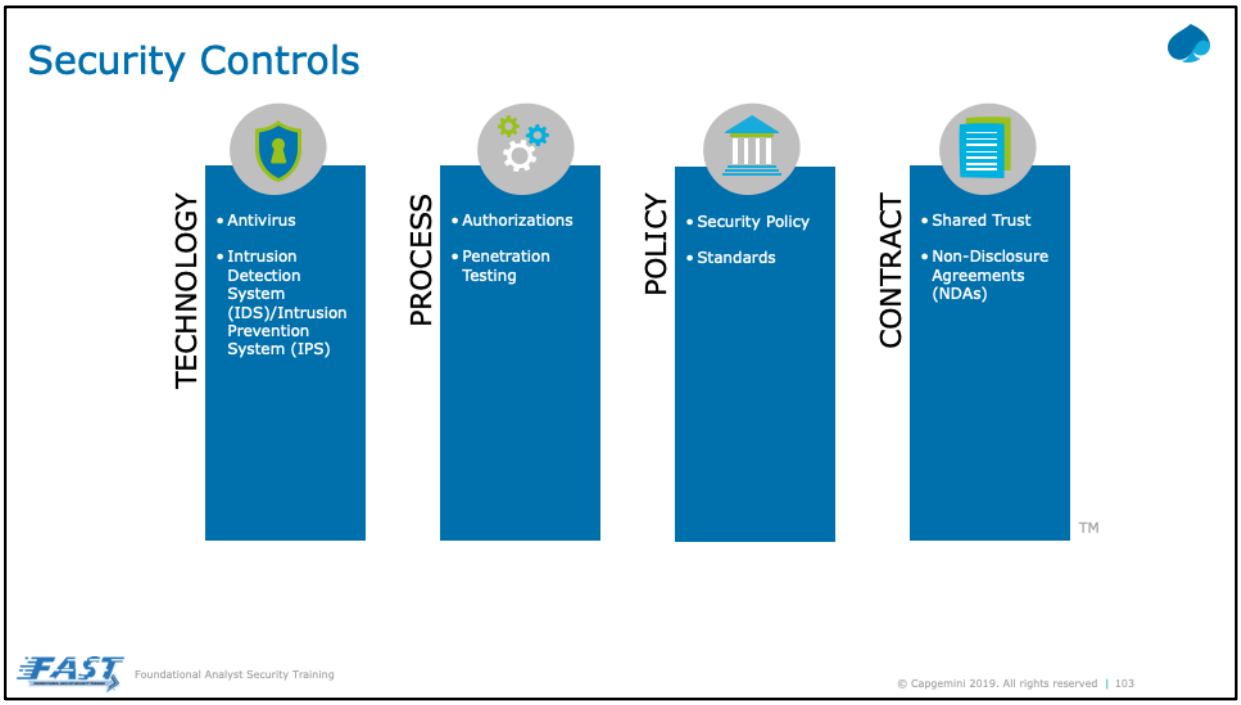
Common Attack Characteristics

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	• Pass-the-Hash Kit • WCE • Mimikatz • Gdump	• Installation • Actions on Objectives	• Windows > NT4 • Local Security Authority (LSA) Application Program Interfaces (APIs) and Memory Structures	• Administrator Accounts • Privileged Accounts • Domain Service Accounts	• Information Disclosure • Privilege Escalation • Lateral Movement
Web Application Attacks	Related: • Cross-Site Scripting • Lightweight Directory Access Protocol (LDAP) and Extensible Markup Language (XML) Injection	• Exploitation • Command and Control (C2) • Actions on Objectives (AoO)	• Hypertext Transfer Protocol (HTTP) GET/POST • Hypertext Markup Language (HTML) Forms • Web Services	Web Applications with Relational Database	• Information Disclosure • Elevation of Privilege
Memory Corruption/ Remote Code Execution (RCE)	• Buffer Overflow • Heap Spray • Heap Overflow • ROP	• Weaponize • Exploitation	Any Code Written in C/C++ that can be User Manipulated		Initial Compromise/ Establish Foothold

We can implement controls in order to mitigate specific attacker TTP's or capabilities. Some of these common attacks are displayed here….

Key Points:
- PTH is the primary mechanism for lateral movement in corporate networks
- Memory Corruption and SQLi – the root cause of each is poor input validation (coding practice) – even though the target and results are very different

Controls:
- PTH - as long as Windows user credentials are stored in memory this threat will remain…
  - However – Knowing what specific APIs are used (i.e. "decompose") can lead to custom HIPS rules (what we did with McAfee HIPS)
  - Restricting administrative access accounts and paths (a-* accounts; Jumpboxes, Captive Portal, 2Factor AuthN)
  - Reduce the number and scope of domain service accounts that have elevated privileges
  - Windows has some new technology that is supposed to mitigate this; the jury is still out, however
    - https://www.rsaconference.com/events/us15/agenda/sessions/1620/pass-the-hash-ii-the-wrath-of-hardware?versioned_session_id=2437
- Memory Corruption
  - Primary controls are secure coding practices and endpoint protections tuned for these attacks
  - Microsoft EMET has been most effective control on Windows – even more than AV/HIPS
  - Linux has some equivalents to EMET, such as StackGuard, PAX, grsecurity
- SQL Injection
  - Primary controls are secure coding practices, proper permissions on db connection string accounts and a *properly configured* WAF (note the "properly configured" accent)
- Social Engineering
  - The best control is continuous User Awareness and Education (think I-Campaign)



There are different types of security controls, implemented or installed at different periods of the software and hardware lifecycles.

Security controls fall into these general categories:

- Technology
- Process
- Policy
- Contract

Technology: Firewall, AV, EMET, StackGuard, ASLR, IDS/IPS
Process: Authorization, Pen-Testing, Provisioning
Policy: Security Engineering engagements
Contract: Supply Chain scenarios, NDAs, Shared-Trust (Cloud)

Security Controls

There are challenges to working with security controls:

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

FAST Foundational Analyst Security Training

Security Controls accomplish a specific purpose, or function.
You must be careful not to use a ‘controls first’ perspective when the threats have not been analyzed.

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.

FAST Foundational Analyst Security Training

All controls must be implemented properly and tested.

Technology: Firewall, AV, EMET, StackGuard, ASLR, IDS/IPS
Process: Authorization, Pen-Testing, Provisioning
Policy: Security Engineering engagements
Contract: Supply Chain scenarios, NDAs, Shared-Trust (Cloud)

Capabilities Matrix / Mitigation Scorecard

Controls Effectiveness

Causes:

- Inadequate system understanding
- Inadequate threat analysis
- Miscommunication of threat model
- Lack of policies/enforcement of threat model

Missing Controls
Inadequate Controls
Inappropriate Controls
Unworkable Controls
Inconsistent Controls

Examples of Security Controls

Securing the Operating System (OS)
Securing Applications
Layered Security
Endpoint Mitigations

Security Controls Effectiveness

Capgemini

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.

Should give the ability of the Security Intelligence Center (SIC) to deploy custom detections

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

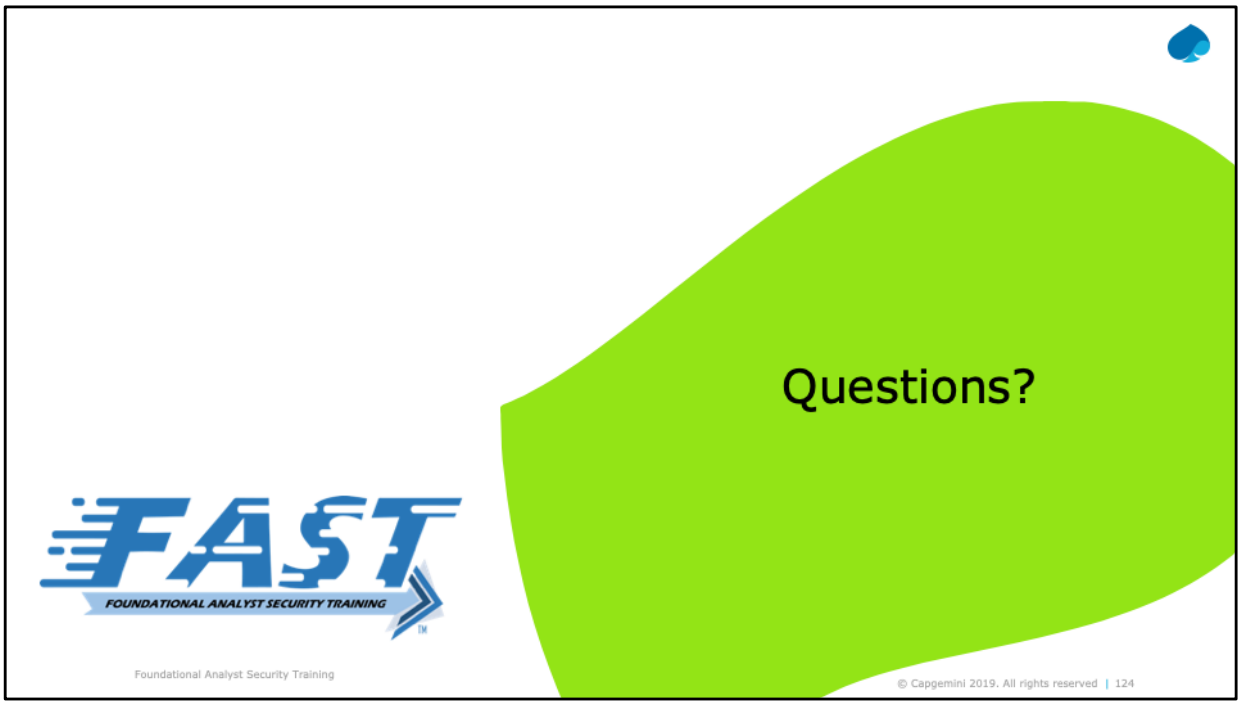
Sandboxing

- 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?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 124


FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
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