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

Module 4 – Networking

Capgemini

Module Learning Objectives

Upon completion of this module, the student should be able to do the following:

- Understand what threat intelligence is and how it can be applied to ensure the safety of networks.
- Understand how threat indicators can be analyzed to obtain information about our adversaries.
- Understand how case analysis can be used to identify Tactics, Techniques, and Procedures (TTPs) of adversaries to inform network defense.
- Understand the Cyber Kill Chain®[1] and how it can be used to analyze and synthesize an attack.
- Understand Unified Enterprise Defense (UED) and how its concepts are used to ensure network integrity.

Introduction to Threat Intelligence

Capgemini

During this module, we will cover the following main topics:

- SOC Organization Structure, Mission, and Responsibilities
- Organizational Maturity
- Security Intelligence and Intelligence Driven Organizations
- Threats and Advanced Persistent Threats

Topic Learning Objectives

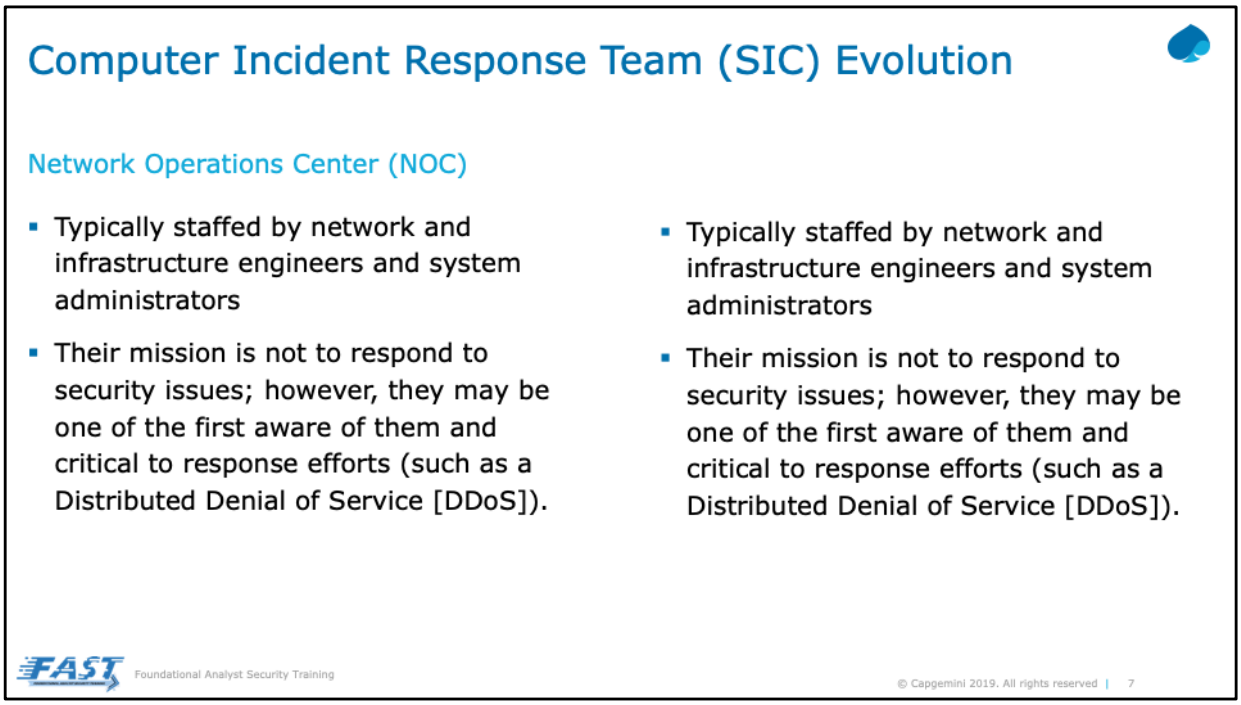
Upon completion of this topic, the student should be able to do the following:

- Describe a SOC organizational structure, mission, and responsibilities.
- Describe a security intelligence and intelligence-driven organizational structure, mission, and responsibilities.
- Explain the different levels of organizational maturity.
- Describe Advanced Persistent Threat (APT) and TTPs.

FAST Foundational Analyst Security Training

Upon successful completion of this module, students will be able to:

- Describe a SOC organizational structure, mission, and responsibilities
- Describe a Security Intelligence and Intelligence Driven organizational structure, mission, and responsibilities
- Explain the different levels of organizational maturity
- Describe Advanced Persistent Threat (APT) and Tactics, Techniques, And Procedures (TTPs)



The SOC has evolved over the years in its organization, structure, and mission. Likewise, a security intelligence center, which is covered on the next slide, does not replace the others mentioned, but enhances the security operations and responsiveness.

A Network Operations Center has the mission to monitor, maintain, and troubleshoot the health, uptime, and performance of network infrastructure (among many other potential network management functions). The NOC performs network management functions (fault management, configuration management, and performance management primarily, but may also performs some levels of accounting and security management). They are typically staffed by network and infrastructure engineers, and system administrators. And, their mission was not necessarily or primarily to respond to security issues, though they likely performed some of those tasks as well.

A Security Operations Center has the mission to provide the security infrastructure and provide Tier 1 detection and triage of cyber security incidents. They are typically staffed with Security Engineers for the different types of security-related equipment and tools supported by the organization. And, their incident response challenge is that they are not typically equipped to detect or investigate targeted attacks and long-term campaigns; again, their primary focus has been at the Tier 1 detection and triage, and not necessarily the long-term analysis and campaign tracking.

Computer Incident Response Team (SIC) Evolution

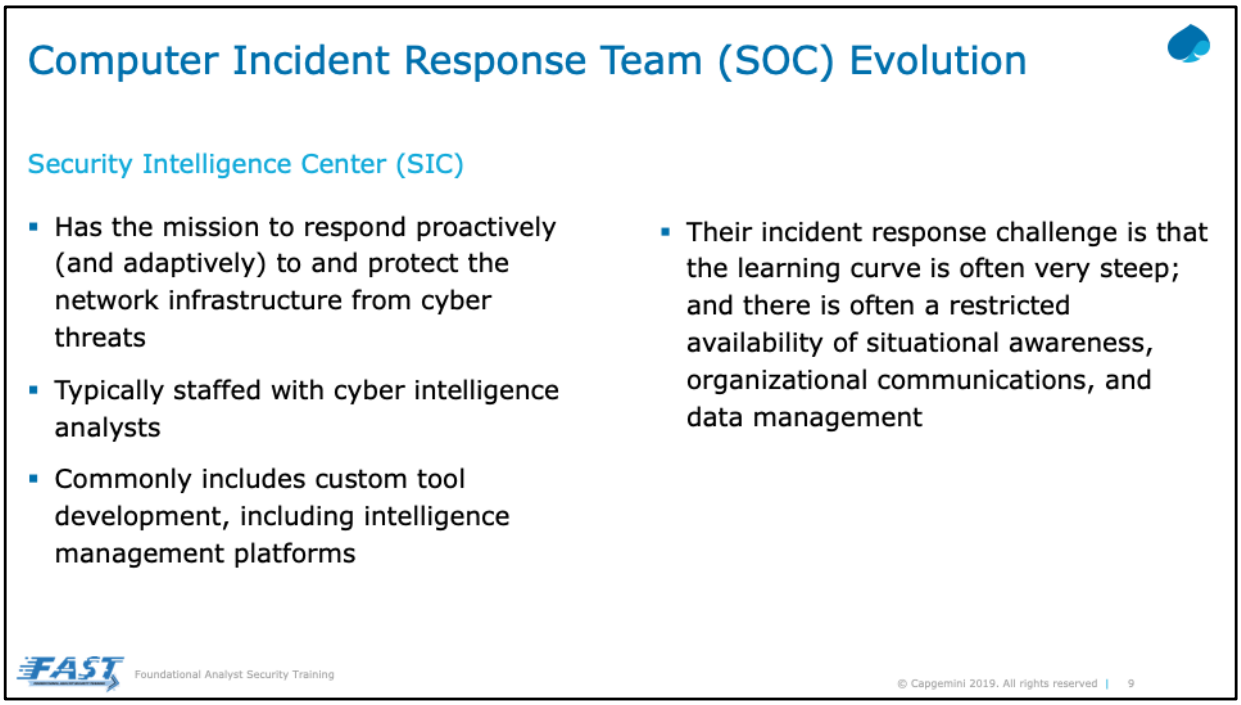
Security Operations Center (SOC)

- Their incident response challenge is that they are not typically equipped to detect or investigate targeted attacks and long-term campaigns.
- SOCs are typically fix and return to operation; intelligence is often not involved.
- Often exist for the purpose of compliance to regulatory policy

- Has the mission to provide the security infrastructure and provide Tier 1 detection and triage of cybersecurity incidents
- Typically staffed with security engineers for the different types of security-related equipment

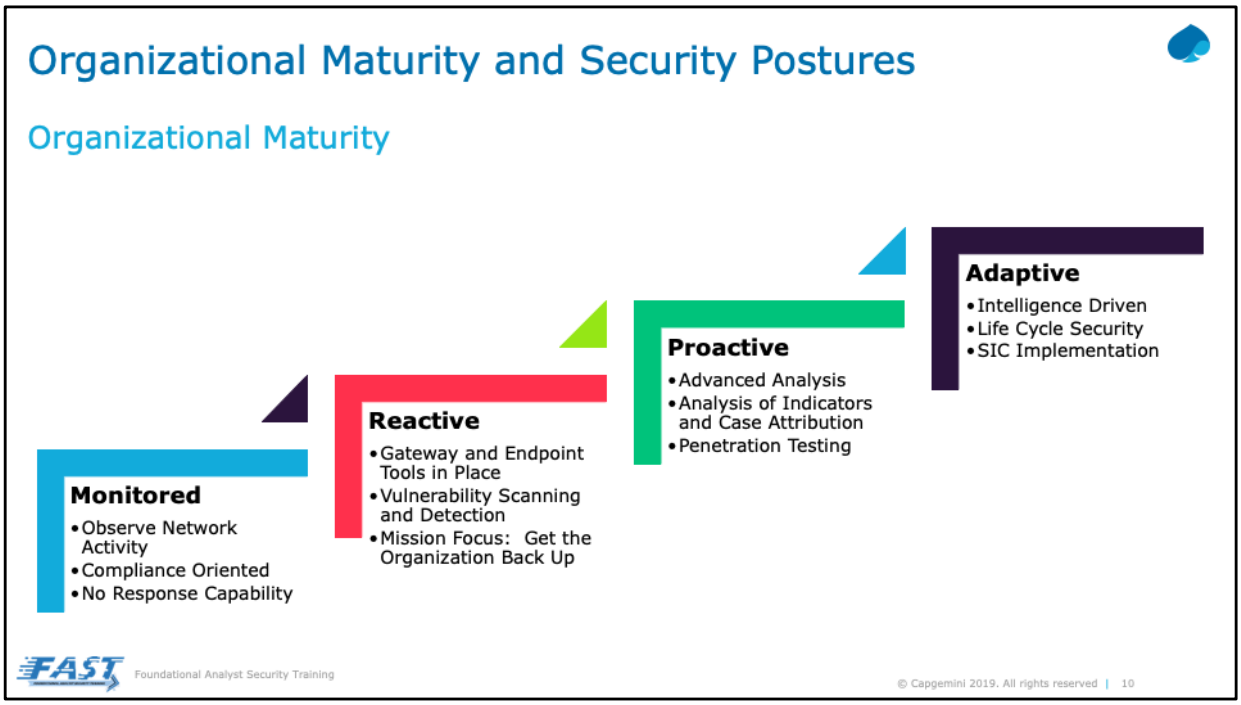
FAST Foundational Analyst Security Training

SOC's are doing things now in most of our customers. DO not want to tell SOC analysts taking the class that they are not good or just there for insurance.



A Security Intelligence Center has the mission to proactively (and adaptively) respond to and protect the network infrastructure from cyber security incidents. They are typically staffed with Cyber Intelligence Analysts and the team commonly includes custom tool development. Their incident response challenge is that the learning curve is often very steep, and there is often a restricted availability of external intelligence, organizational communications, and data management. However, when properly formed and trained, they are able to perform detailed analysis and long-term campaign tracking.

SIC's can implement, they do NOT have the problem of not able to implement. They DO implement. A SIC contains parts of the SOC and NOC. It is the evolution of these into a mature organization.

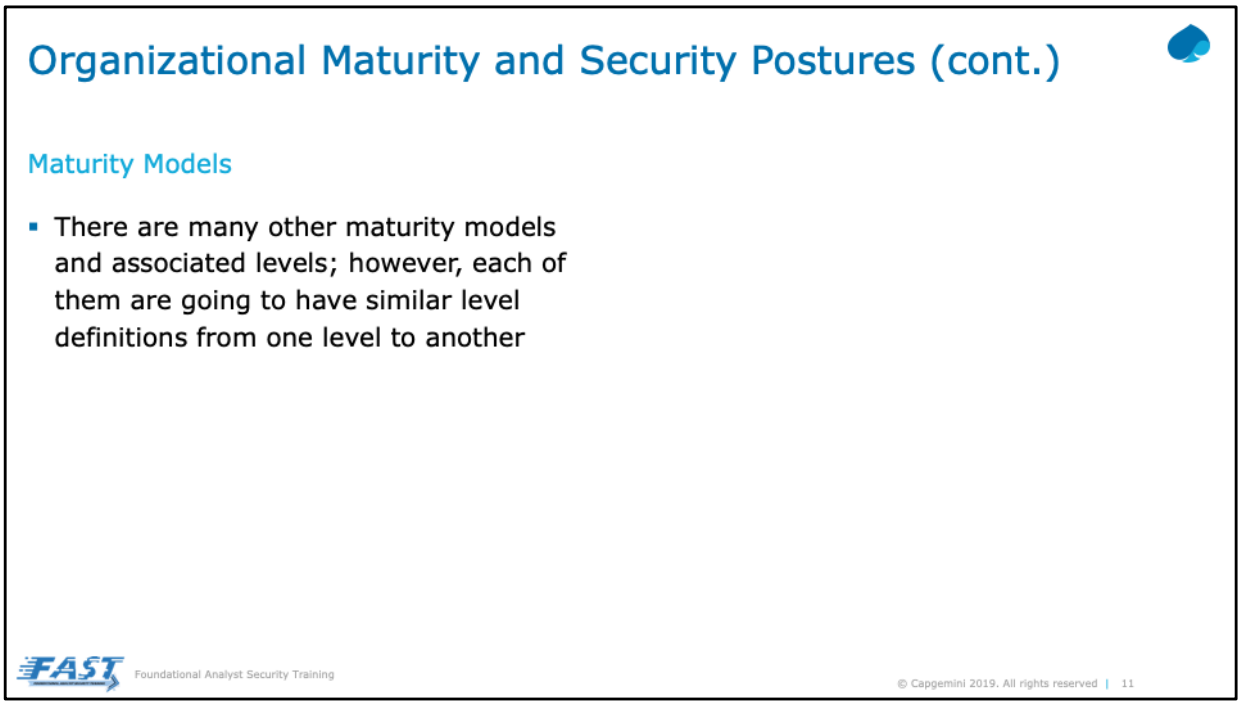


An attack from a sophisticated adversary, such as a nation-state adversary, can happen to your Enterprise. You need to be ready for such attacks. You need to be able to produce the intelligence that mitigates the risk and anticipates the adversary's next move. You need well-trained personnel in your SOC team, you need to develop custom detection capabilities that complement and depend on the traditional security solutions, and you need to take actions to evolve the Enterprise infrastructure, guided by the demands of increasing situational awareness and insight into our enterprise.

Security Intelligence Centers are intentionally named "Intelligence" as that is very important. Organizations will go through a maturity process as they develop new capabilities, including security-related capabilities.

While there are many different maturity models and frameworks, following is a common maturity level description:

- Monitored means that the organization monitors network activity, but does not have the people, processes, or technology in place to respond to or adapt to evolving security threats.
- Reactive means that they have the security gateway and endpoint tools in place and they can conduct vulnerability scanning and detection. However, they are reactive – meaning that they are waiting until there is an incident or an alert before they can take action.
- Proactive means that they have advanced analytics, analyzing indicators, they can conduct a Case Analysis, and they test their network security posture with methods such as Red Team / Blue Team drills.
- Adaptive is the highest level and means that they are tracking threats based on a full lifecycle analysis, such as the Cyber Kill Chain, they implement security throughout the lifecycle, they have well-established Security Information Centers and Security Intelligence Centers and Analysis processes in place.



There are many other maturity models and associated levels; however, each of them are going to have similar level definitions from one level to another.

For example, in the Capability Maturity Model (CMM), there are five maturity levels:

- Initial, where processes are characterized by being unpredictable, poorly controlled, and reactive.
- Managed, where projects of the organization have ensured that requirements are managed and that processes are planned, performed, measured, and controlled; but they still tend to be reactive.
- Defined, where processes are well characterized and understood, and are described in standards, procedures, tools, and methods by the organization. They are proactive.
- Quantitatively Managed, processes are measured and controlled by defined qualitative measures and standards within the organization.
- Optimizing, where the organization focuses on continual process improvement.

Capability Maturity Model (CMM)

For example, in the Capability Maturity Model (CMM), there are five maturity levels:

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimizing

Capability Maturity Model (CMM)

For example, in the Capability Maturity Model (CMM), there are five maturity levels:

1. **Initial**
2. Repeatable
3. Defined
4. Managed
5. Optimizing

- Processes are usually ad hoc and the organization usually does not provide a stable environment.
- Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes.

FAST Foundational Analyst Security Training

Processes are usually ad hoc and the organization usually does not provide a stable environment. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes.

In spite of this ad hoc, chaotic environment, maturity level 1 organizations often produce products and services that work; however, they frequently exceed the budget and schedule of their projects.

Organizations are characterized by a tendency to over commit, abandon processes in the time of crisis, and not be able to repeat their past successes again.

Software project success depends on having quality people.

Capability Maturity Model (CMM)

For example, in the Capability Maturity Model (CMM), there are five maturity levels:

1. Initial
2. **Repeatable**
3. Defined
4. Managed
5. Optimizing

- Software development successes are repeatable.
- The processes may not repeat for all the projects in the organization.
- The organization may use some basic project management to track cost and schedule.

FAST Foundational Analyst Security Training

Process discipline helps ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans.

Project status and the delivery of services are visible to management at defined points (for example, at major milestones and at the completion of major tasks).

Basic project management processes are established to track cost, schedule, and functionality. The minimum process discipline is in place to repeat earlier successes on projects with similar applications and scope. There is still a significant risk of exceeding cost and time estimate.

Capability Maturity Model (CMM)

For example, in the Capability Maturity Model (CMM), there are five maturity levels:

1. Initial
2. Repeatable
3. **Defined**
4. Managed
5. Optimizing

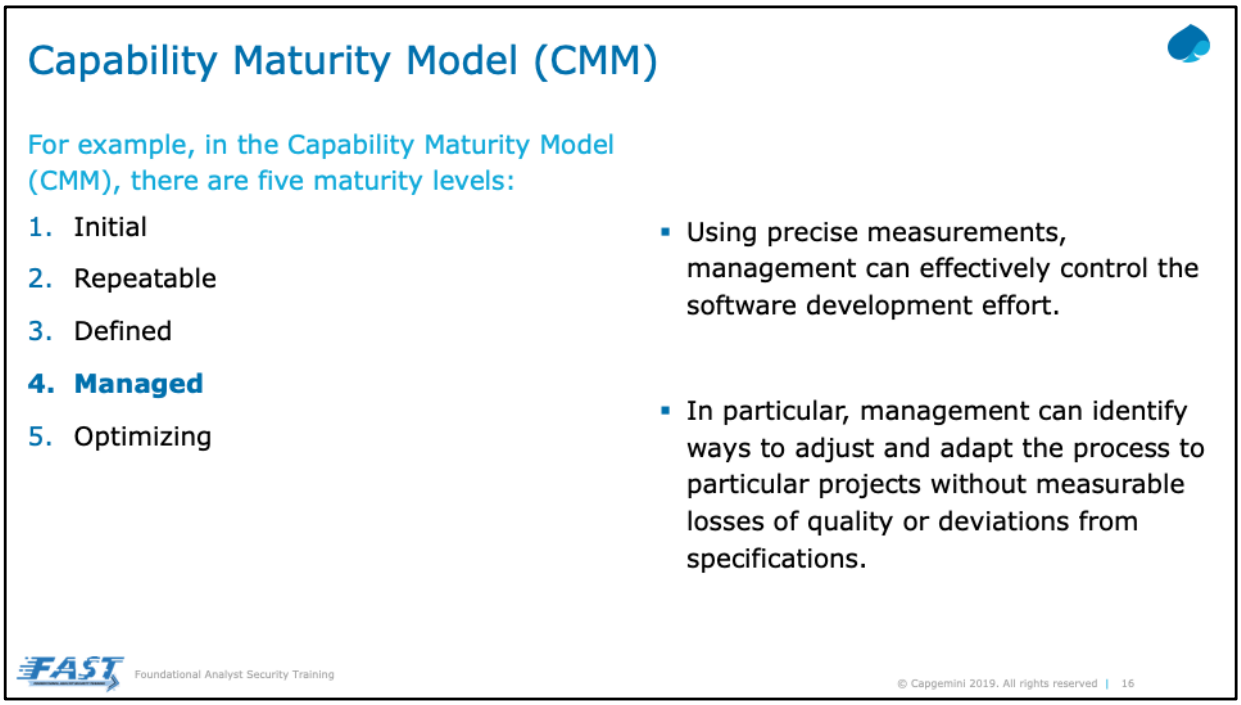
- The organization's set of standard processes, which is the basis for level 3, is established and improved over time.
- These standard processes are used to establish consistency across the organization.

FAST Foundational Analyst Security Training

Projects establish their defined processes by the organization's set of standard processes according to tailoring guidelines.

The organization's management establishes process objectives based on the organization's set of standard processes and ensures that these objectives are appropriately addressed.

A critical distinction between level 2 and level 3 is the scope of standards, process descriptions, and procedures. At level 2, the standards, process descriptions, and procedures may be quite different in each specific instance of the process (for example, on a particular project). At level 3, the standards, process descriptions, and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit.



At this level organization set a quantitative quality goal for both software process and software maintenance.

Subprocesses are selected that significantly contribute to overall process performance. These selected subprocesses are controlled using statistical and other quantitative techniques.

A critical distinction between maturity level 3 and maturity level 4 is the predictability of process performance. At maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques, and is quantitatively predictable. At maturity level 3, processes are only qualitatively predictable.

Capability Maturity Model (CMM)

For example, in the Capability Maturity Model (CMM), there are five maturity levels:

1. Initial
2. Repeatable
3. Defined
4. Managed
5. **Optimizing**

- Focusing on continually improving process performance through both incremental and innovative technological improvements.
- Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives

The effects of deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities.

Security Intelligence

Security Intelligence IS NOT the following:

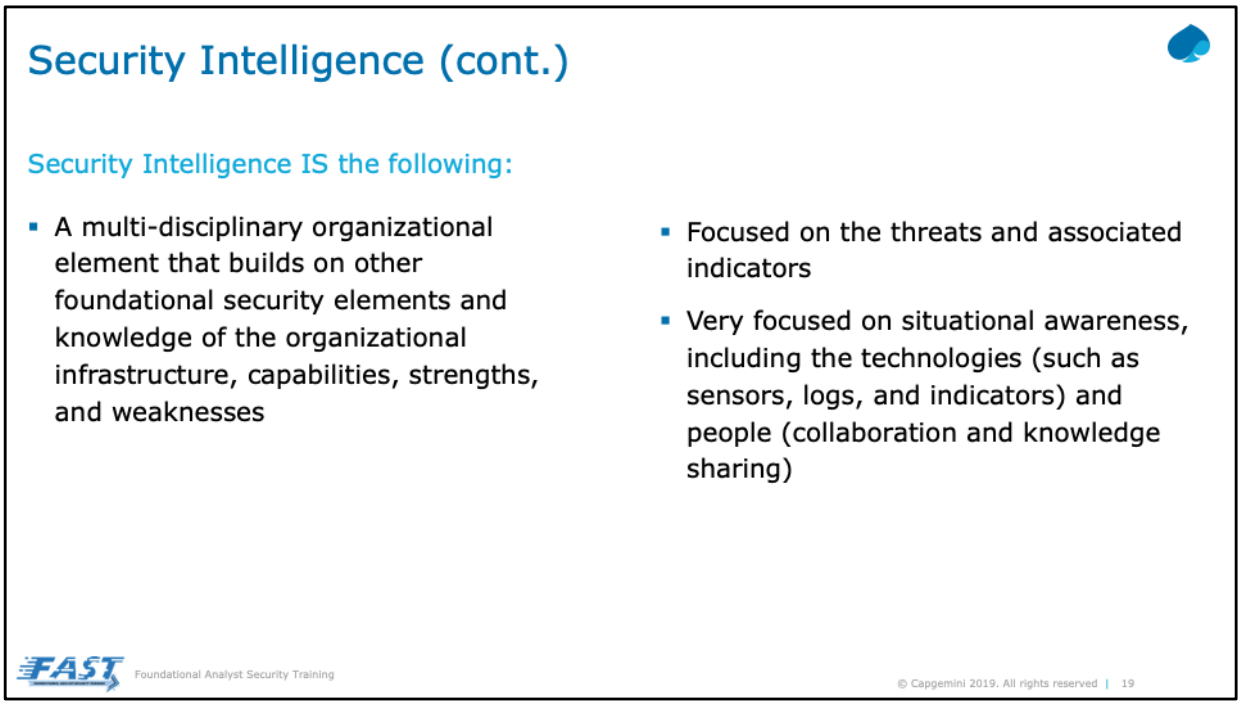
- A replacement for the NOC or SOC elements
- Based on, or dependent on, pre-canned alerts, alarms, and signatures
- Restricted to traditional security tools, controls, and technologies

FAST Foundational Analyst Security Training

In order to talk about what security intelligence is, it is important to address what it is not.

Security Intelligence IS NOT a replacement for the NOC or SOC elements, it is not based on or dependent on pre-canned alerts, alarms, and signatures, and it is not restricted to traditional security tools, controls, and technologies.

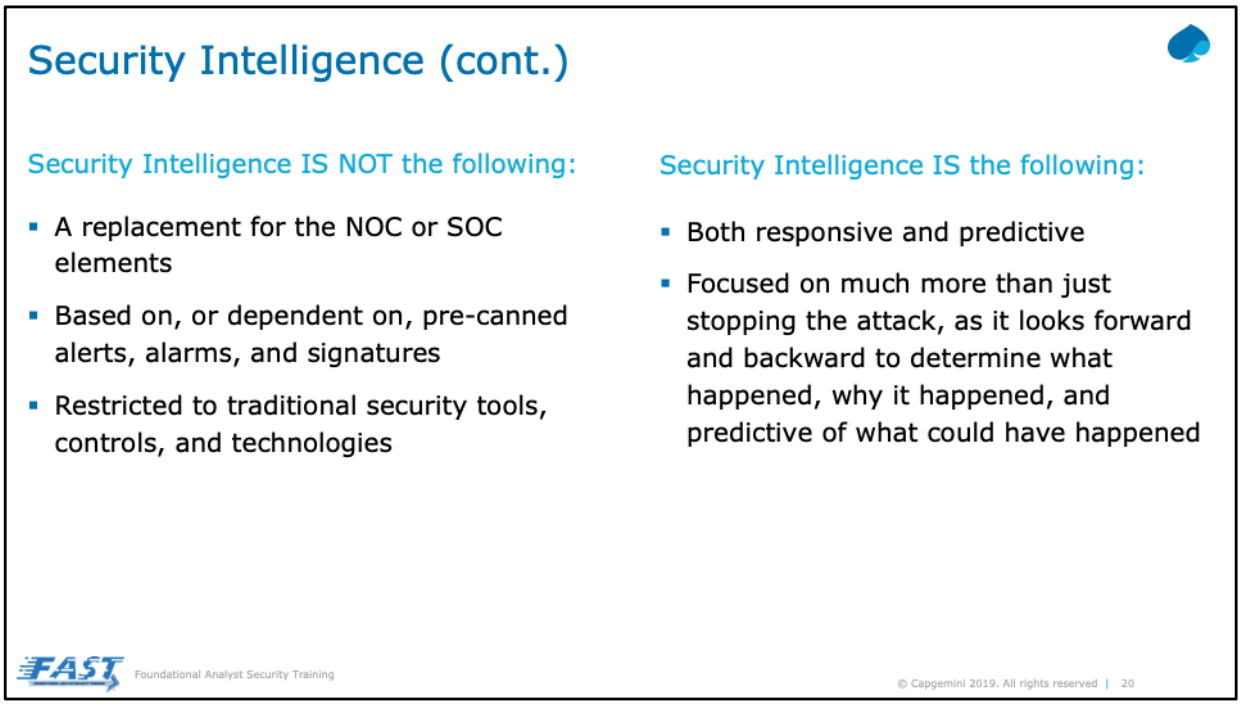
Security Intelligence IS a multi-disciplinary organizational element that builds on other foundational security elements and knowledge of the organizational infrastructure, capabilities, strengths, and weaknesses (where security intelligence requires many different skills and expertise through the organization), it is focused on the threat and associated indicators (including Case Analysis and tracking as previously mentioned), it is very focused on situational awareness, including the technologies (such as sensors, logs, and indicators); and people (collaboration and knowledge sharing), it includes elements that are both responsive and predictive, and it is focused on much more than just stopping the attack, as it looks forward and backward to determine what happened, why it happened, and predictive of what could have happened (which enables an organization get to the level where they become predictive).



In order to talk about what security intelligence is, it is important to address what it is not.

Security Intelligence IS NOT a replacement for the NOC or SOC elements, it is not based on or dependent on pre-canned alerts, alarms, and signatures, and it is not restricted to traditional security tools, controls, and technologies.

Security Intelligence IS a multi-disciplinary organizational element that builds on other foundational security elements and knowledge of the organizational infrastructure, capabilities, strengths, and weaknesses (where security intelligence requires many different skills and expertise through the organization), it is focused on the threat and associated indicators (including Case Analysis and tracking as previously mentioned), it is very focused on situational awareness, including the technologies (such as sensors, logs, and indicators); and people (collaboration and knowledge sharing), it includes elements that are both responsive and predictive, and it is focused on much more than just stopping the attack, as it looks forward and backward to determine what happened, why it happened, and predictive of what could have happened (which enables an organization get to the level where they become predictive).



In order to talk about what security intelligence is, it is important to address what it is not.

Security Intelligence IS NOT a replacement for the NOC or SOC elements, it is not based on or dependent on pre-canned alerts, alarms, and signatures, and it is not restricted to traditional security tools, controls, and technologies.

Security Intelligence IS a multi-disciplinary organizational element that builds on other foundational security elements and knowledge of the organizational infrastructure, capabilities, strengths, and weaknesses (where security intelligence requires many different skills and expertise through the organization), it is focused on the threat and associated indicators (including Case Analysis and tracking as previously mentioned), it is very focused on situational awareness, including the technologies (such as sensors, logs, and indicators); and people (collaboration and knowledge sharing), it includes elements that are both responsive and predictive, and it is focused on much more than just stopping the attack, as it looks forward and backward to determine what happened, why it happened, and predictive of what could have happened (which enables an organization get to the level where they become predictive).

Unified Enterprise Defense (UED)

UED Life Cycle

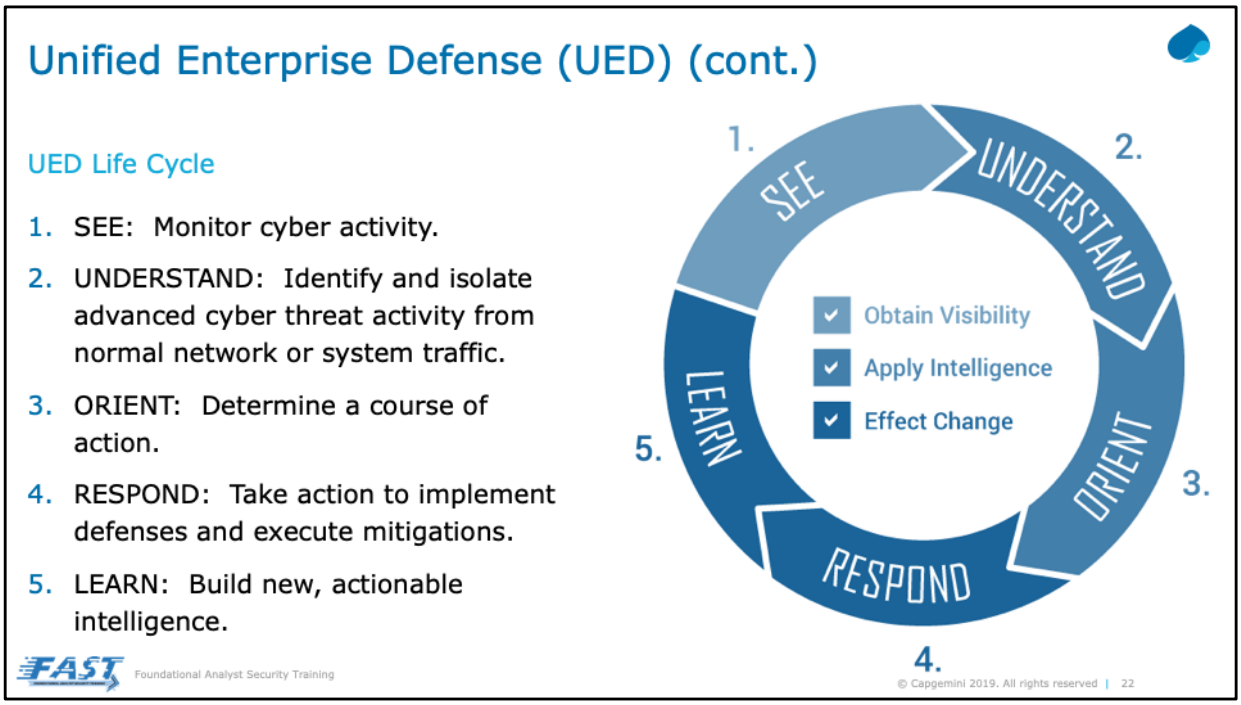
- Services, solutions, and products
- Adaptive defense strategy
- Sustainable threat protection
- Mature security posture

FAST Foundational Analyst Security Training

A Unified Enterprise Defense provides services, solutions and products that ensure an adaptive defense strategy, sustainable threat protection, and a mature security posture.

The Unified Enterprise Defense Pillars are:
SEE, which monitors cyber activity across the organization.
UNDERSTAND, which identifies and isolates advanced cyber threat activity from normal network or system traffic.
ORIENT, which is focused on determining a course of action.
RESPOND, which takes action to implement defenses and executes mitigations.
LEARN, which builds new, actionable intelligence.

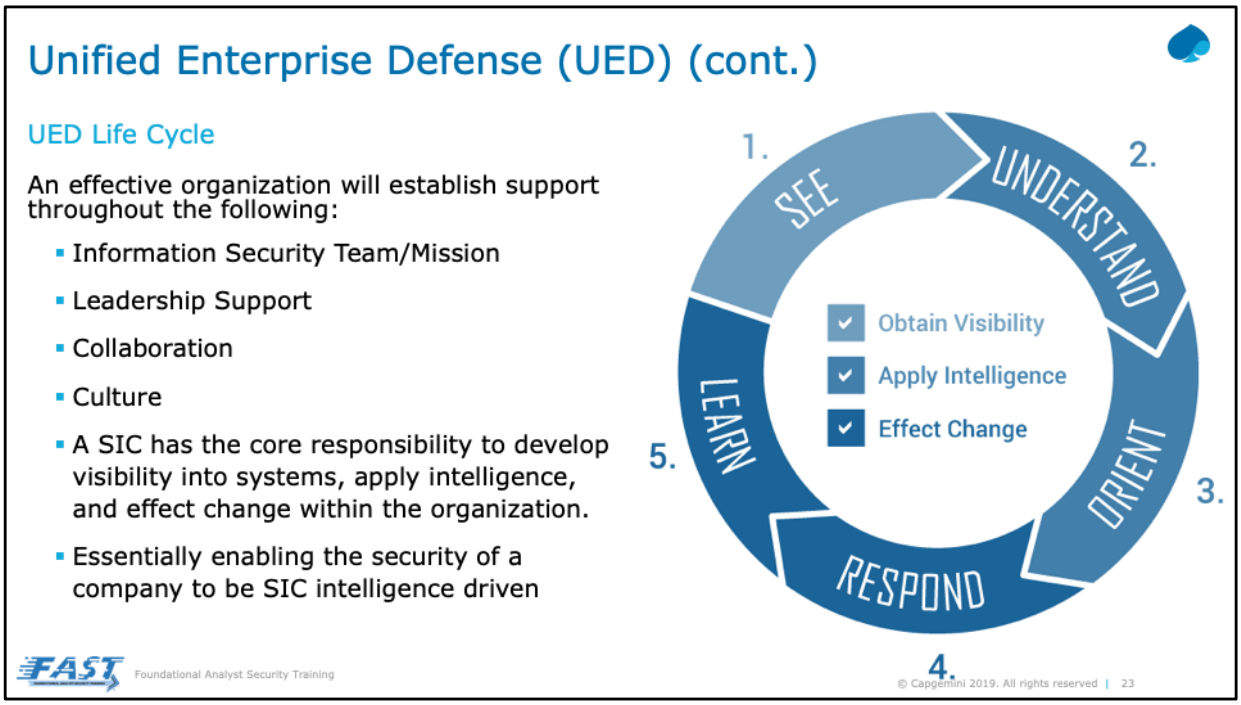
An effective organization will establish support throughout the organization, including well-defined and supported Information Security Team/Mission, having Leadership Support, encouraging Collaboration through the organization, and establishing a company Culture that is conducive to those elements previously discussed.



A Unified Enterprise Defense provides services, solutions and products that ensure an adaptive defense strategy, sustainable threat protection, and a mature security posture.

The Unified Enterprise Defense Pillars are:
SEE, which monitors cyber activity across the organization.
UNDERSTAND, which identifies and isolates advanced cyber threat activity from normal network or system traffic.
ORIENT, which is focused on determining a course of action.
RESPOND, which takes action to implement defenses and executes mitigations.
LEARN, which builds new, actionable intelligence.

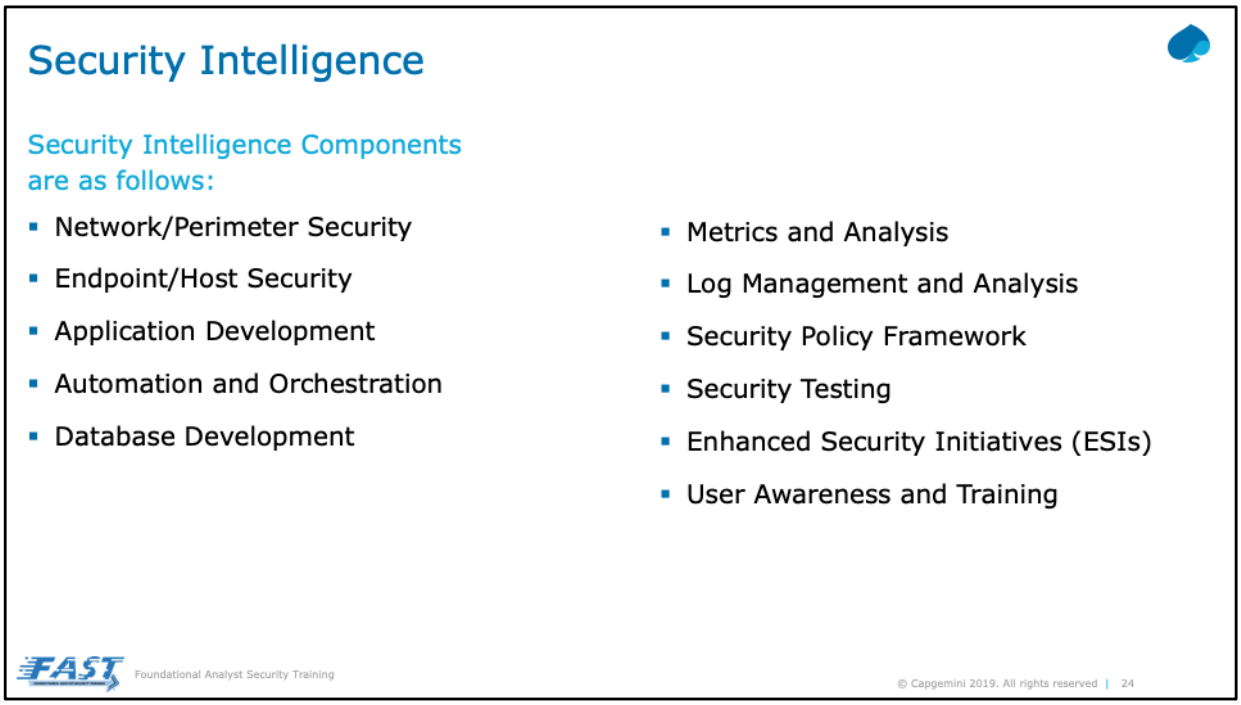
An effective organization will establish support throughout the organization, including well-defined and supported Information Security Team/Mission, having Leadership Support, encouraging Collaboration through the organization, and establishing a company Culture that is conducive to those elements previously discussed.



A Unified Enterprise Defense provides services, solutions and products that ensure an adaptive defense strategy, sustainable threat protection, and a mature security posture.

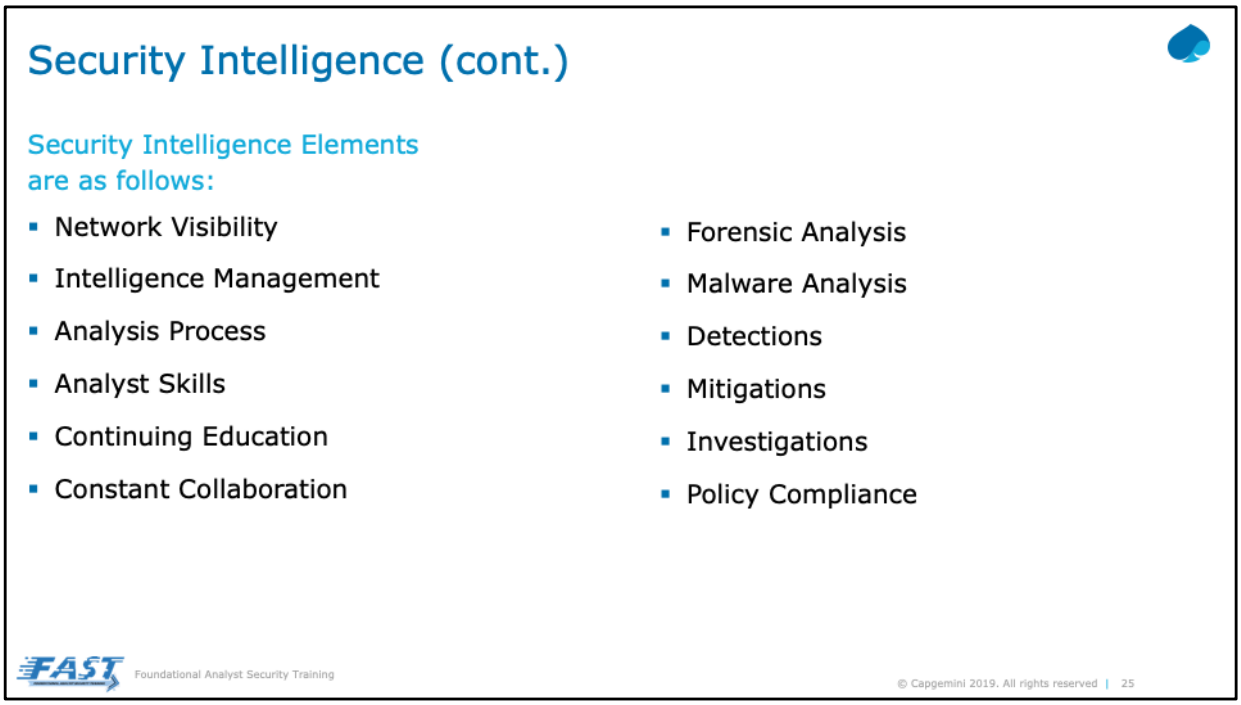
The Unified Enterprise Defense Pillars are:
SEE, which monitors cyber activity across the organization.
UNDERSTAND, which identifies and isolates advanced cyber threat activity from normal network or system traffic.
ORIENT, which is focused on determining a course of action.
RESPOND, which takes action to implement defenses and executes mitigations.
LEARN, which builds new, actionable intelligence.

An effective organization will establish support throughout the organization, including well-defined and supported Information Security Team/Mission, having Leadership Support, encouraging Collaboration through the organization, and establishing a company Culture that is conducive to those elements previously discussed.



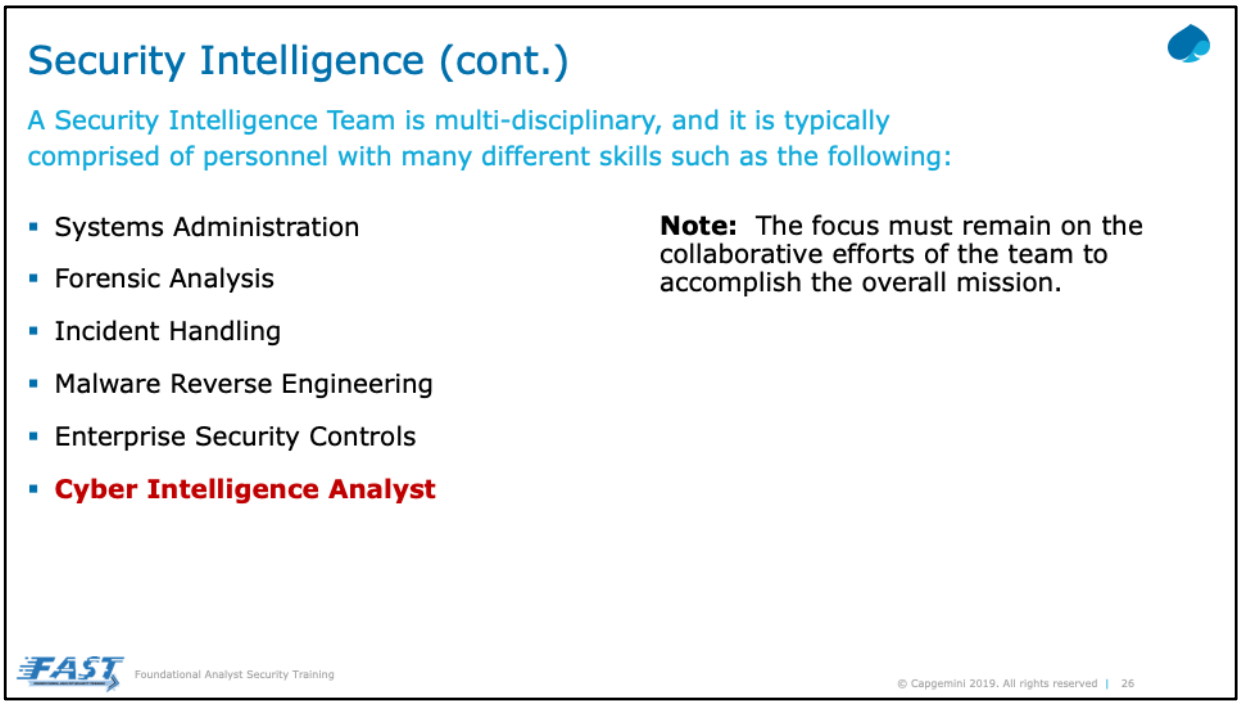
Security Intelligence includes many different and supporting components, including, but not limited to:

- Network/Perimeter Security
- Endpoint/Host Security
- Application Development
- Application Code
- Database Development
- Metrics and Analysis
- Log Management and Analysis
- Security Policy Framework
- Security Testing
- Enhanced Security Initiatives (ESI)
- User Awareness and Training



Likewise, there are many different elements that comprise Security Intelligence, including:

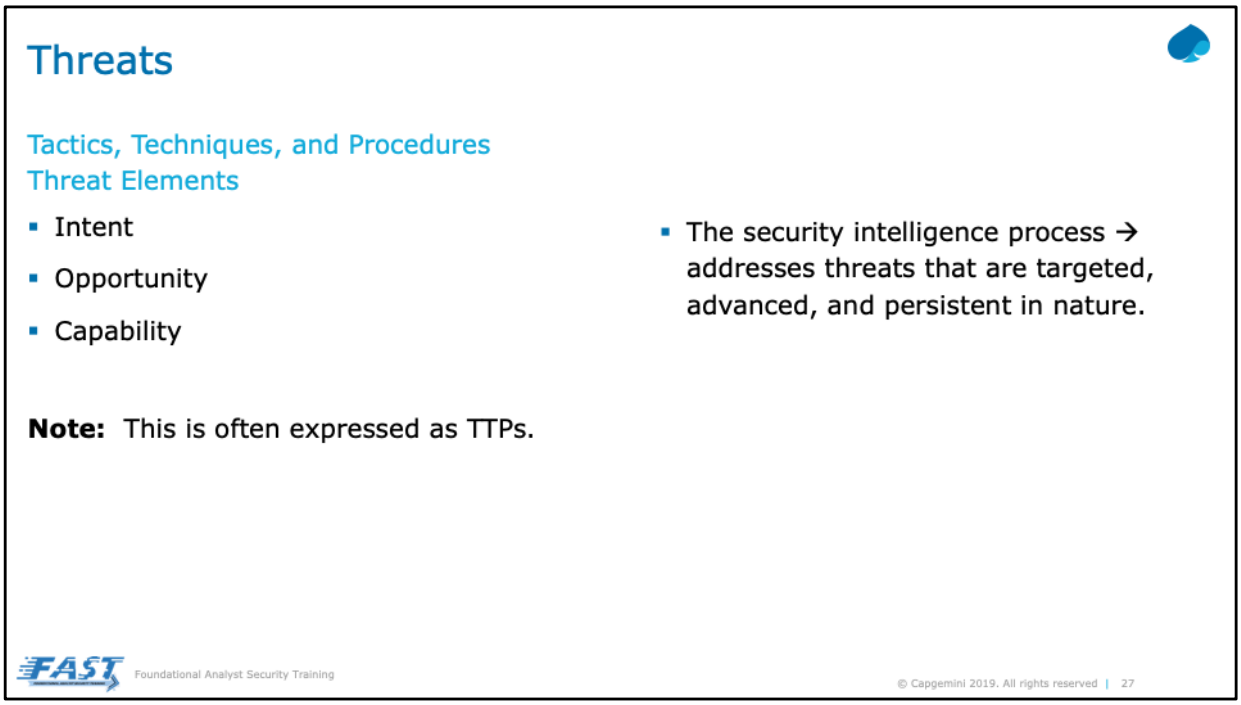
- Network Visibility
- Intelligence Management
- Analysis Process
- Analyst Skills
- Forensic Analysis
- Malware Analysis
- Detections
- Mitigations
- Investigations
- Policy Compliance



As previously mentioned, a Security Intelligence Team is a multi-disciplinary team that succeeds with strong team work and collaboration. The Security Intelligence Team is typically comprised of personnel with many different skills, including:

- Systems Administration
- Forensic Analysis
- Incident Handling
- Malware Reverse Engineering
- Enterprise Security Controls
- Cyber Intelligence Analysis

Note that the focus must remain on team work and on the collaborative efforts of the team to accomplish the overall mission.



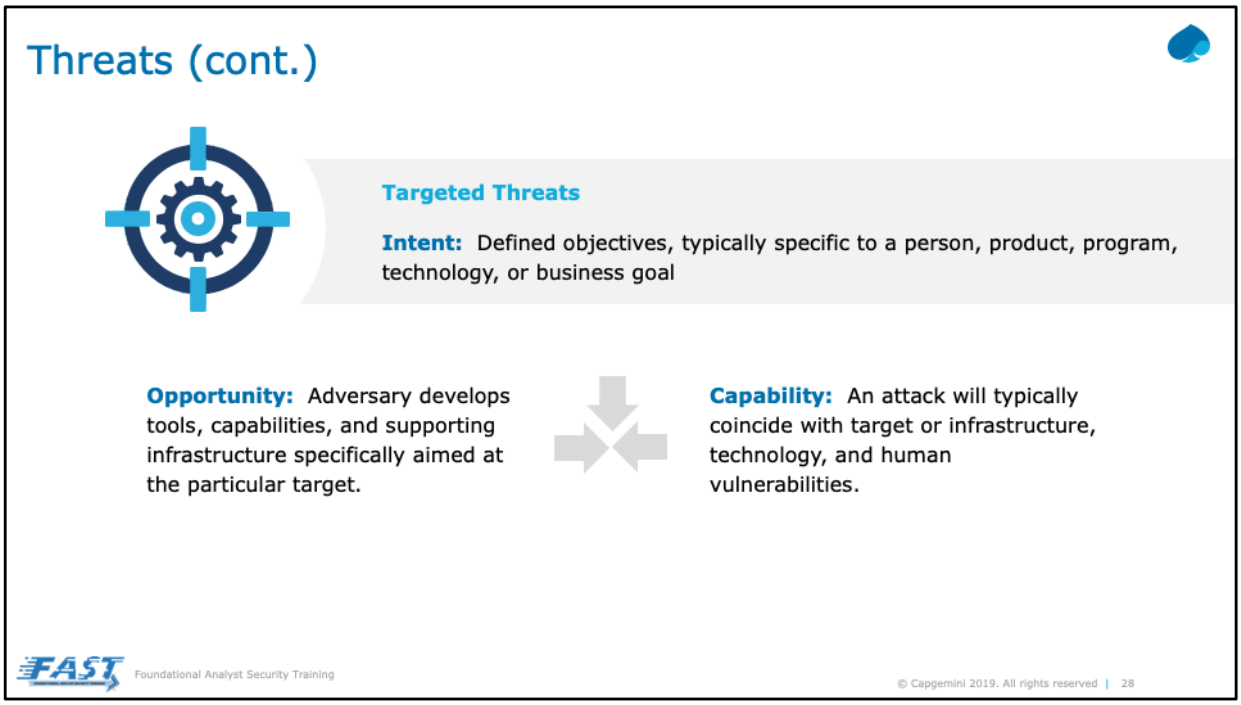
The threat includes people who will reuse familiar technologies, techniques, and procedures; and develop their own tools and capabilities for malicious intent. This is evident by how many phishing attempts are seen each year that use both old methods and new tactics.

A threat (or malicious activity) is comprised of 3 main elements:

- Intent, which is the desire to do something.
- Opportunity, which is the opening or vulnerability that exists within the organization.
- Capability, which means having the skills and/or tools to be able to perform the malicious activity.

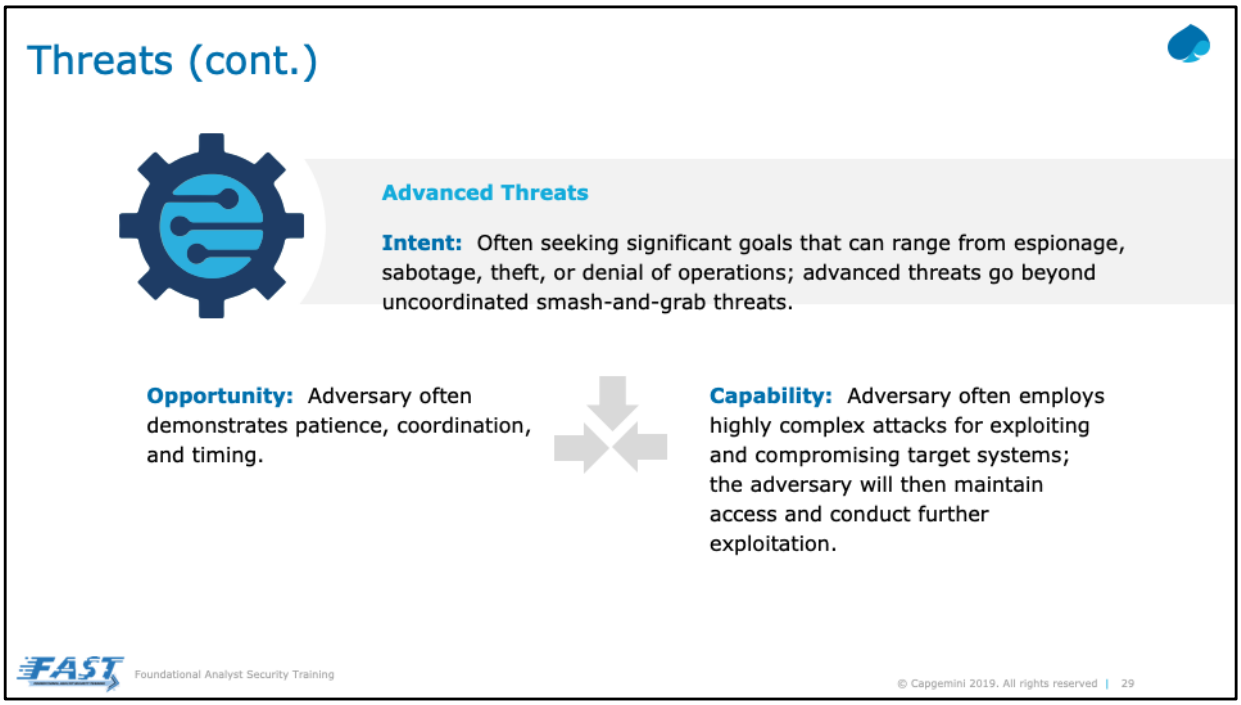
Note: you will often hear this expressed as Means, Opportunities, and Motives.

The security intelligence process is specifically designed to address threats that are targeted, advanced, and persistent in nature.



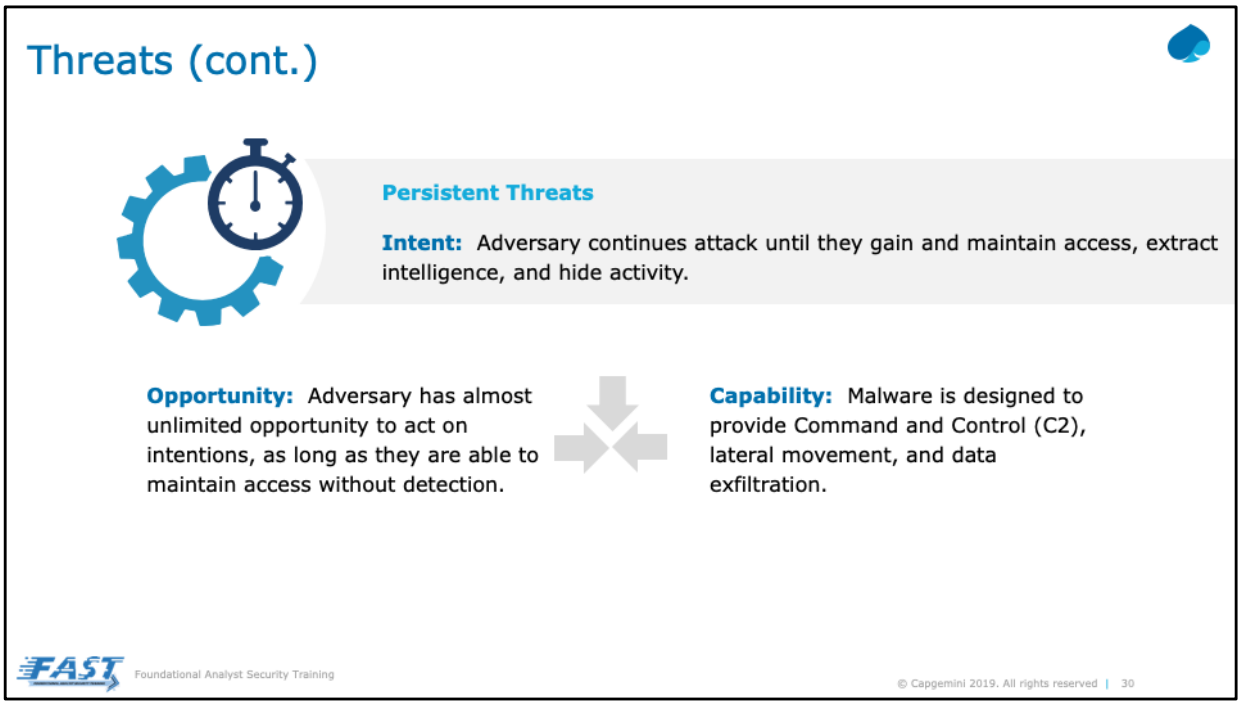
The Intent, Opportunity, and Capability characteristics of Targeted Threats include:

- Intent, which has defined objectives, typically specific to a person, product, program, technology, or business goal.
- Opportunity, where the attack will typically coincides with target or infrastructure vulnerabilities.
- Capability, where the adversary develops tools, capabilities, and supporting infrastructure specifically aimed at the particular target.



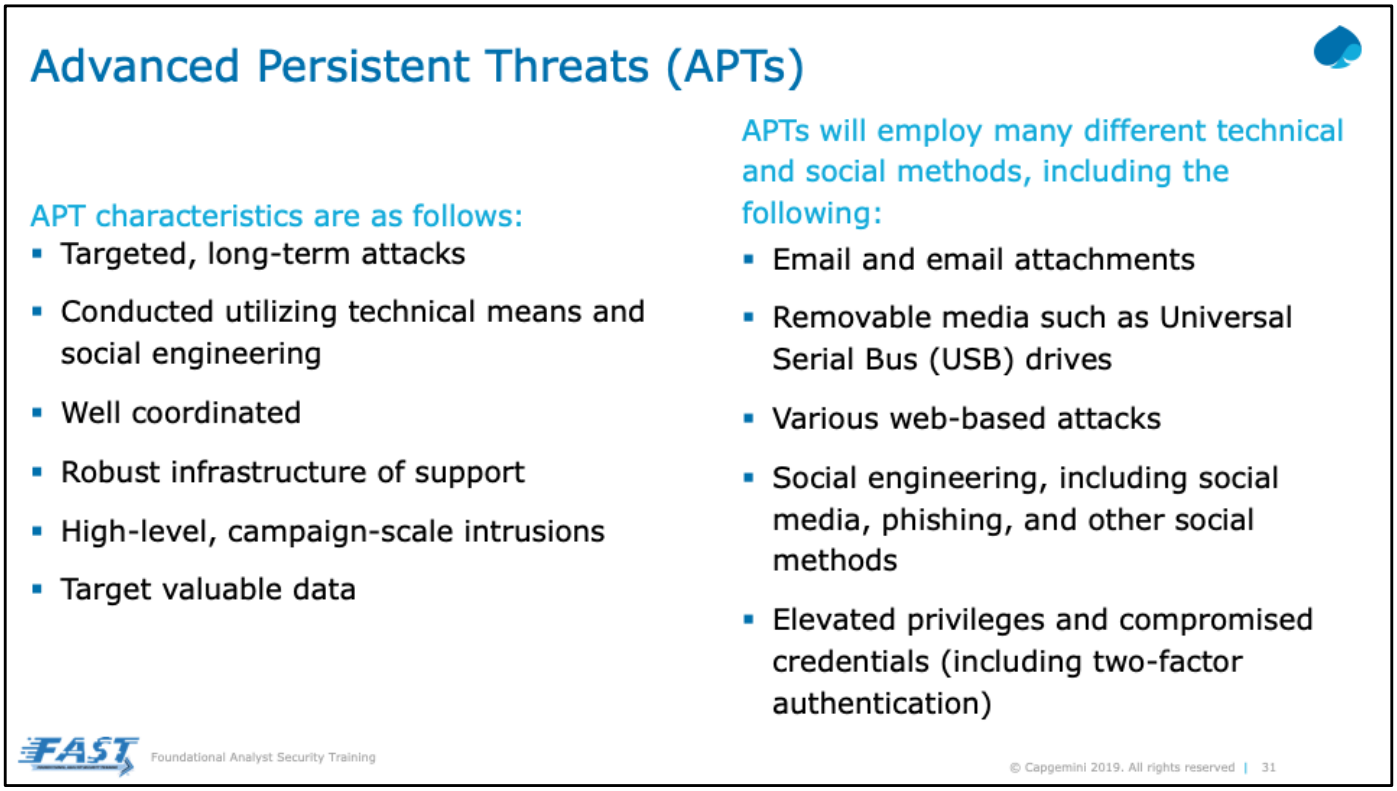
The Intent, Opportunity, and Capability characteristics of Advanced Threats include:

- Intent, where the adversary performs extensive target reconnaissance.
- Opportunity, where the adversary often demonstrates patience, coordination, and timing in the conduct of their attack.
- Capability, where the adversary often employs highly complex attacks for exploiting and compromising target systems; the adversary will then maintain access and conduct further exploitation while trying to remain undetected.



The Intent, Opportunity, and Capability characteristics of Persistent Threats include:

- Intent, where the adversary continues attack until they gain and maintain access, extract intelligence, and hide activity.
- Opportunity, where the adversary has almost unlimited opportunity to act on intentions, as long as they are able to maintain access without detection.
- Capability, where malware is designed to provide command and control, lateral movement, and data exfiltration.

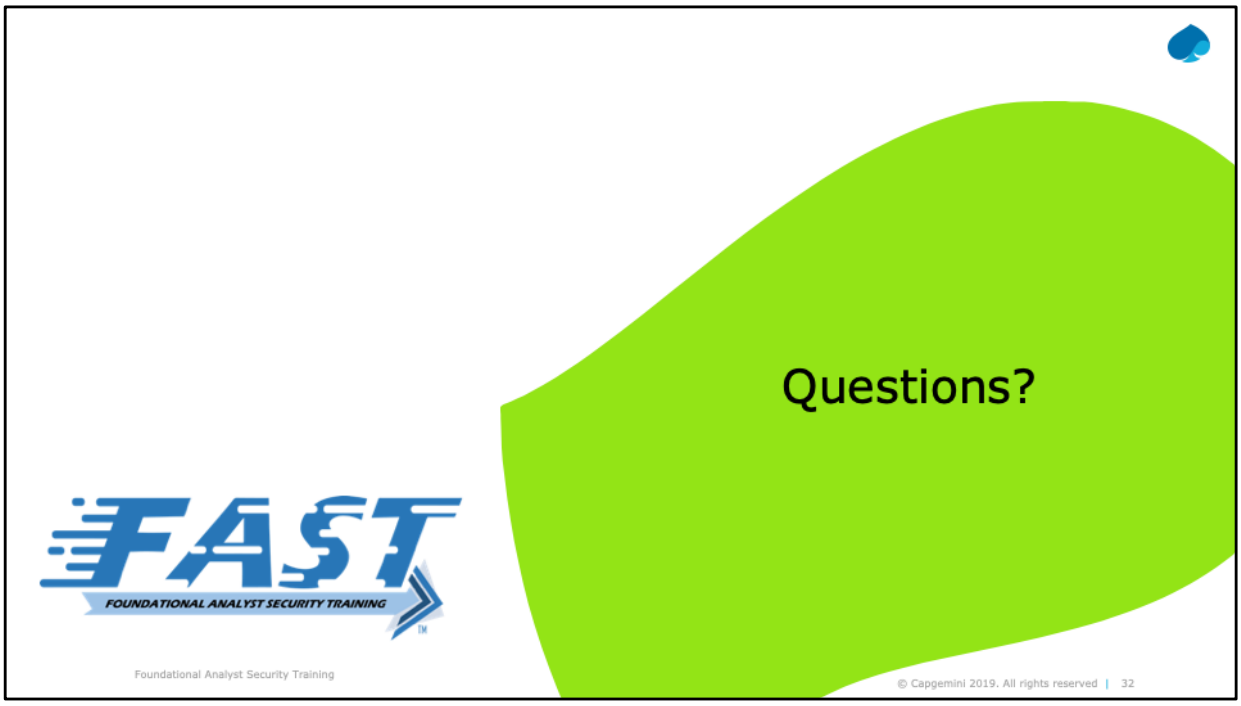


Advanced Persistent Threats are characterized by a targeted, long-term attacks conducted utilizing technical means and social engineering.

APTs are typically well coordinated, they develop a robust infrastructure of support, they are often high-level, campaign-scale intrusions, and they target valuable data.

APTs will employ many different technical and social methods, including:

- Email and email attachments
- Removable media, such as USB drives
- Various Web-based attacks
- Social engineering, including social media, phishing, and other social methods
- Elevated privileges and compromising credentials (including two-factor authentication)


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 32

Cyber Kill Chain®

Capgemini

Agenda

WHAT IS THE CYBER KILL CHAIN®? | PHASES OF THE CYBER KILL CHAIN®

Topic Learning Objectives

- Upon completion of this topic, the student should be able to do the following:
  - Understand the concept of the Cyber Kill Chain® and how it is utilized.
  - Describe where information for the Cyber Kill Chain® comes from and how it is used to protect an organization.
  - List the seven phases of the Cyber Kill Chain®, including Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives (AoO).

FAST Foundational Analyst Security Training

Upon successful completion of this module, students will be able to:

- Describe a SOC organizational structure, mission, and responsibilities
- Describe a Security Intelligence and Intelligence Driven organizational structure, mission, and responsibilities
- Explain the different levels of organizational maturity
- Describe Advanced Persistent Threat (APT) and Tactics, Techniques, And Procedures (TTPs)

The Cyber Kill Chain®

What it is…

The Cyber Kill Chain® is a seven-phase framework depicting the actions adversaries or actors take against a specific target.

FAST Foundational Analyst Security Training

 | 36

Script:

{pause}

Lockheed Martin's Cyber Kill Chain is a seven phase framework depicting the actions adversaries or actors must take against a specific target(s).

The Cyber Kill Chain® (cont.)

What it is…

Using this framework, analysis can be done to assess the defenses of an organization.

FAST Foundational Analyst Security Training

 | 37

Script:

{pause}

Using this framework, analysis can be done to assess the defenses of any organization. That the Cyber Kill Chain, while it is 7 phases, it is a framework and adding phases to meet your organization's needs is encouraged, if you feel you need more or less for different tasks. Such as email with a link vs with a doc or web attack.

The Cyber Kill Chain® (cont.)

What it is…

The Cyber Kill Chain® framework tracks the phases that an attacker must complete successfully to achieve their desired objectives.

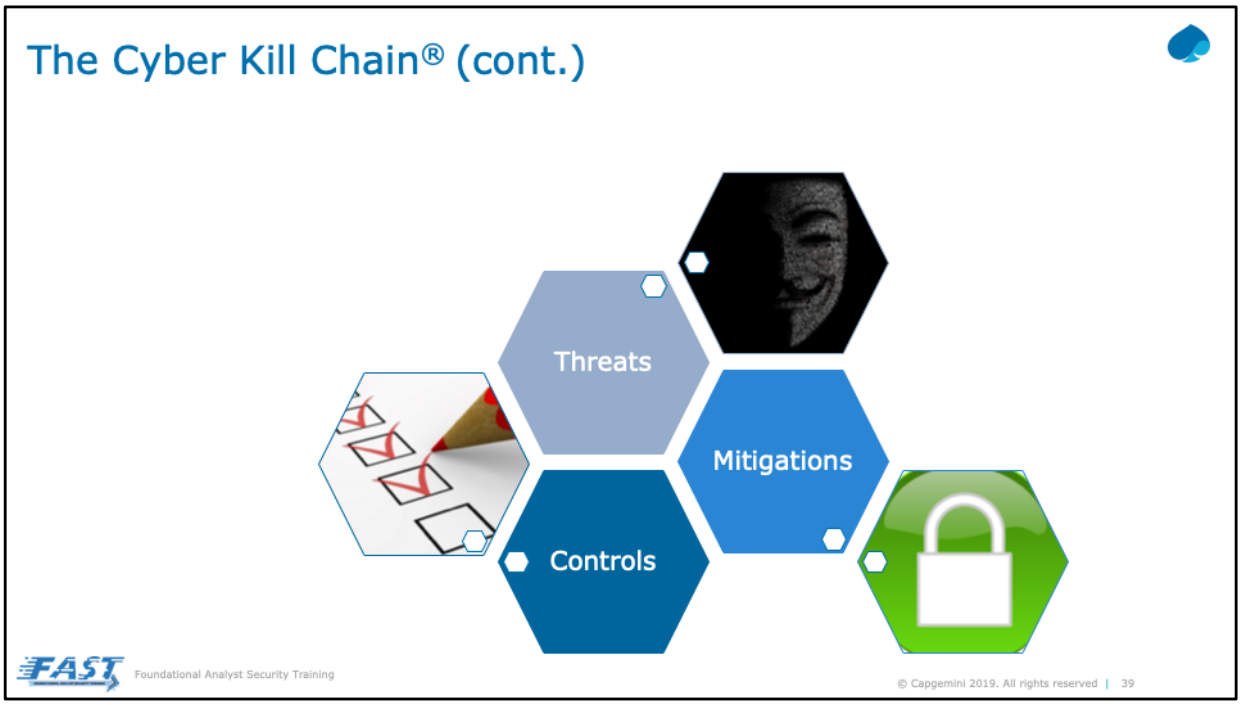
FAST Foundational Analyst Security Training

 | 38

Script:

{pause}

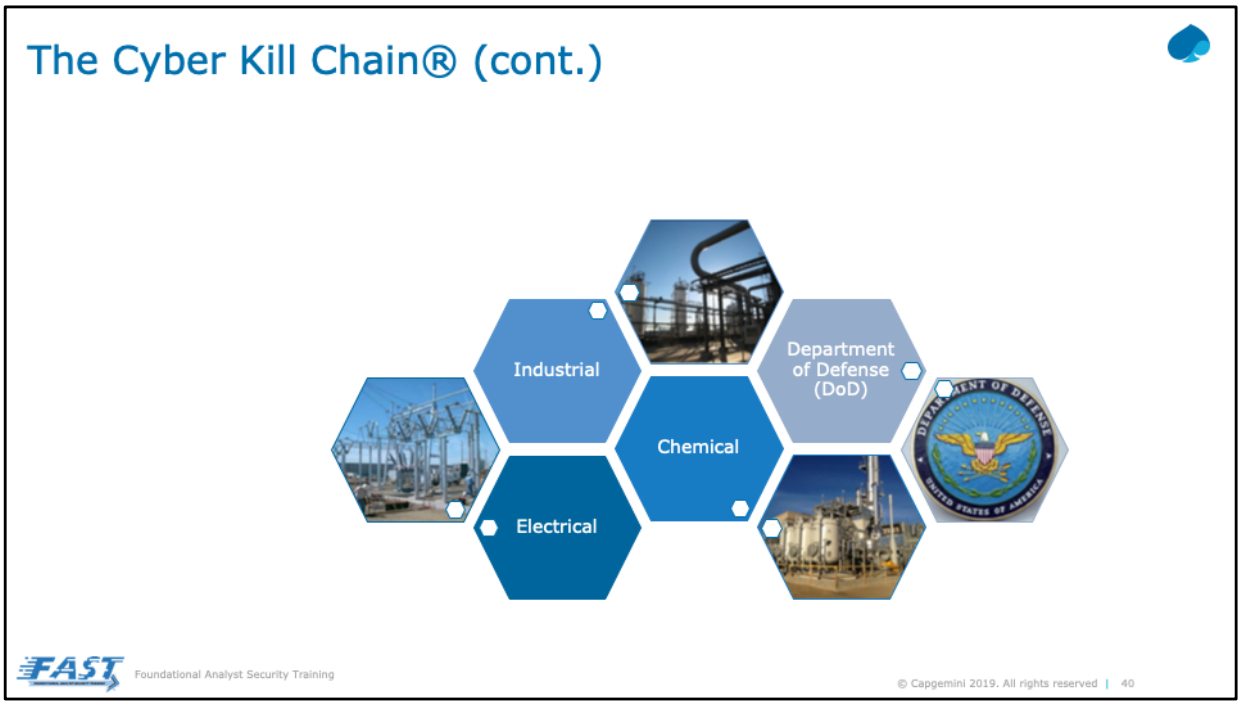
The Kill Chain framework tracks the phases that an attacker must complete successfully to achieve their desired objectives.



Script:

{pause}

The Kill Chain Allows an organization to align controls and mitigations with threats to the organization and is used across multiple industries and multiple network types for network defense.



Script:

{pause}

In fact the Kill Chain has been adopted as the industry standard for pre-attack mitigation, incident response, active attack mitigation, and resolution across many different industries.

What it is…

Through the Cyber Kill Chain®, an aggressor must identify and target a perceived weakness in an organization.

FAST Foundational Analyst Security Training

 | 41

Script:

{pause}

Through the Kill Chain an aggressor must identify and target a perceived weakness in an organization.

What it is… (cont.)

The Cyber Kill Chain® uses a standardized lexicon to describe the milestones an attacker must complete to progress to the next stage of exploiting that weakness.

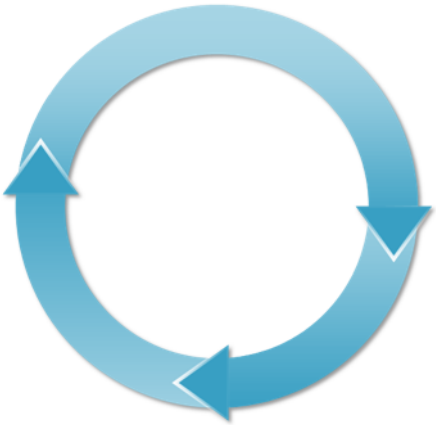
Script:

{pause}

Although these phases are a representation of the actions an attacker must take to be successful, we man not discover them in the order in which they happen, the goal is to detect and end the attack as early as possible.

What it is… (cont.)

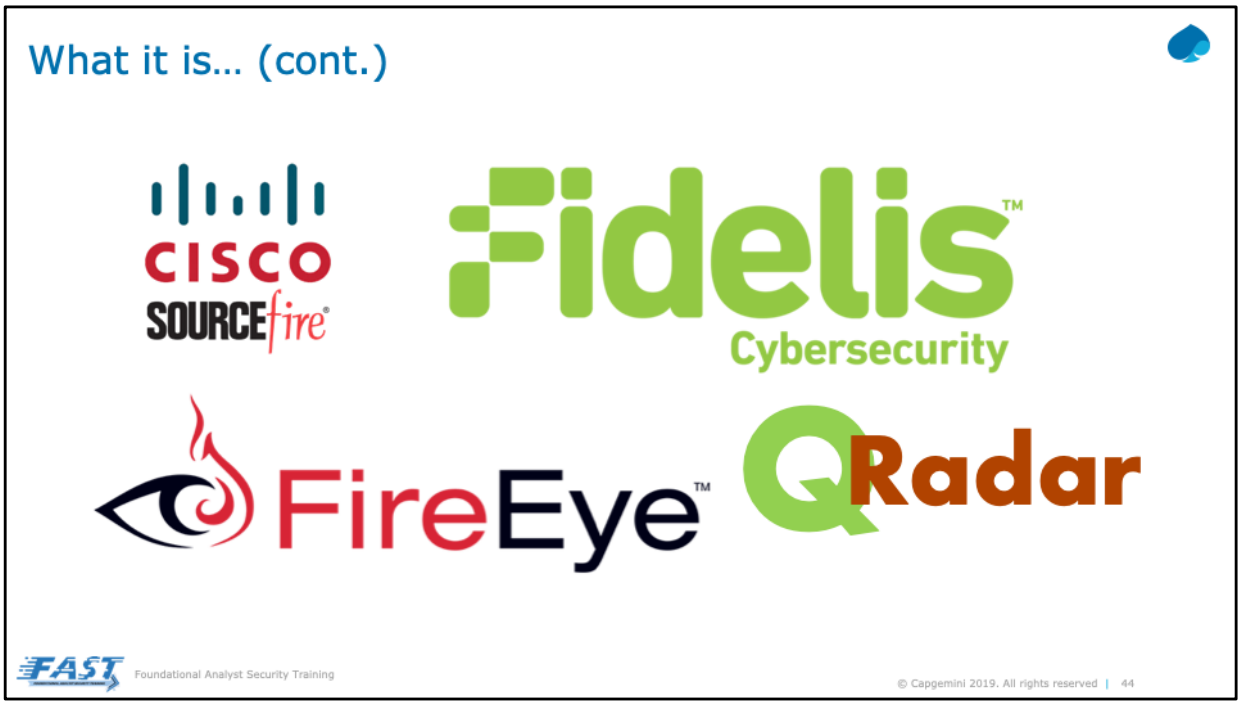
These phases are a representation of the actions an attacker must take to be successful.



FAST Foundational Analyst Security Training

 | 43

You will have to work backwards and forwards in the kill chain to stop the attack and develop threat intelligence.

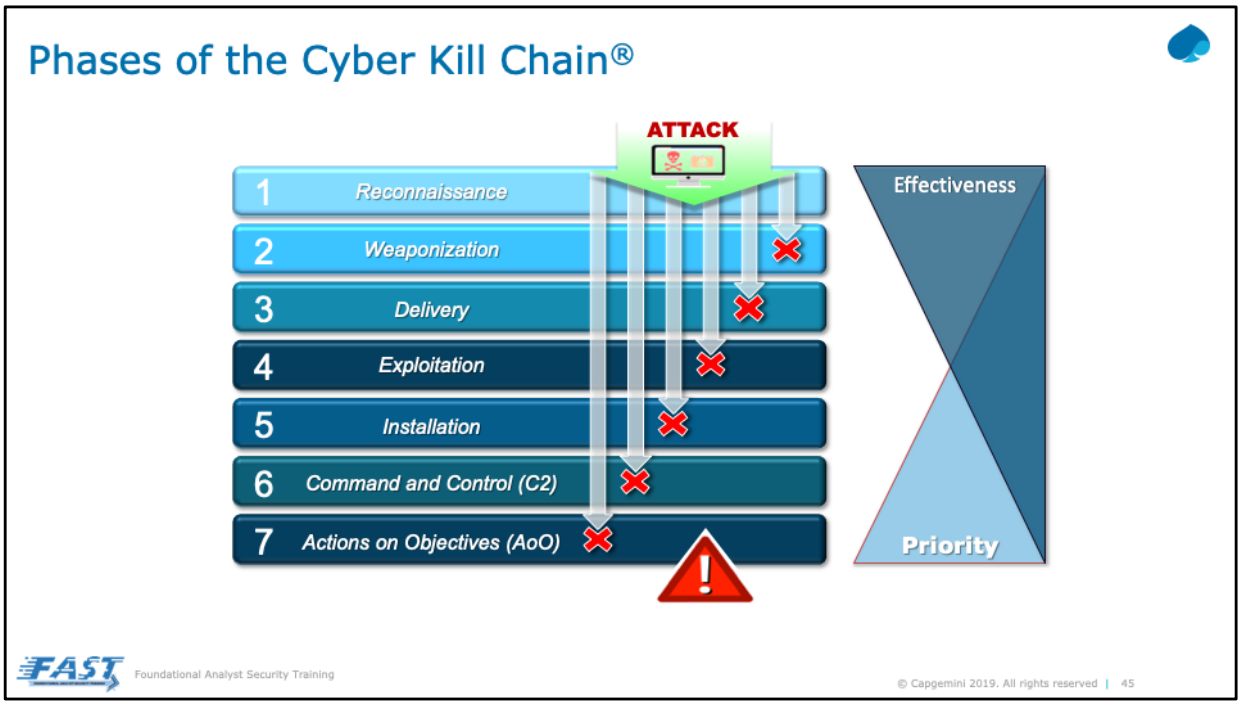


Script:

{pause}

The cornerstone of applying and leveraging the value of the Kill Chain is the availability of real-time and historical data.

As such, a robust Data Analytics model is imperative to consolidate, correlate, and leverage holistic data sets for analysis. This goal can be achieved through strategic integration of SIEM and Big Data platforms.

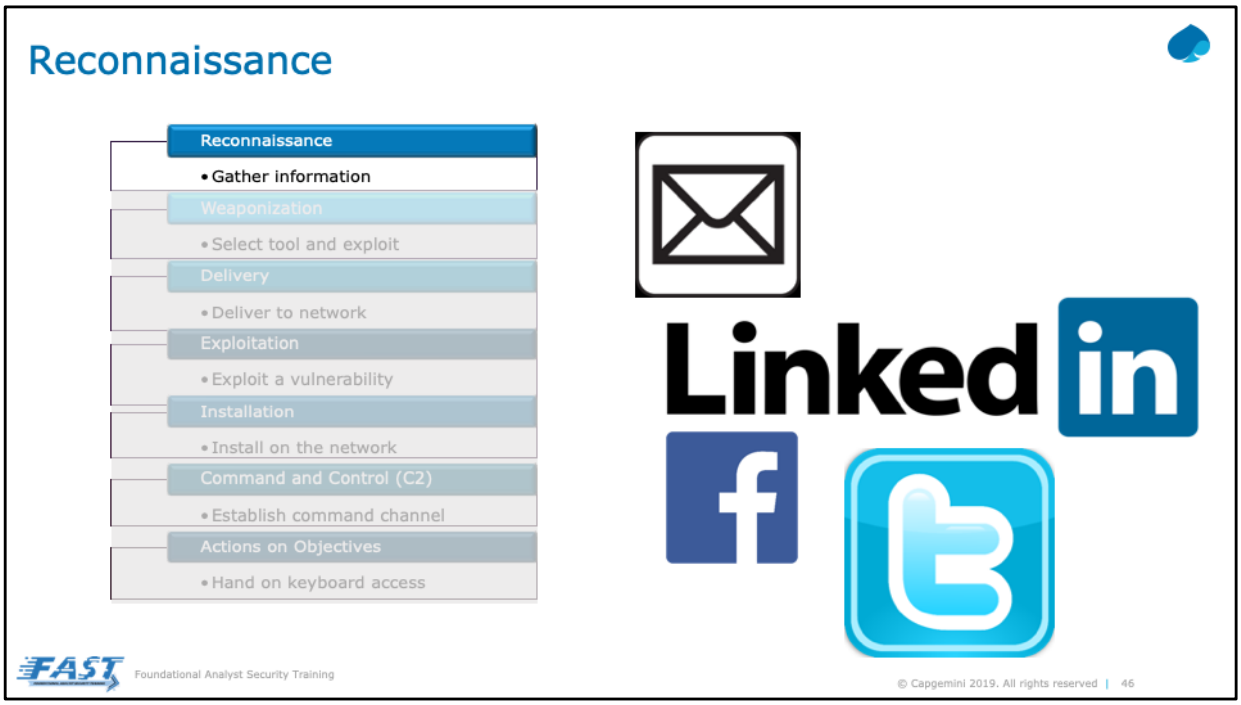


Script:

{pause}

As an attacker moves through the kill chain during an attack, the defenders response will increase in Priority. Likewise mitigations increase in effectiveness the earlier they are implemented.

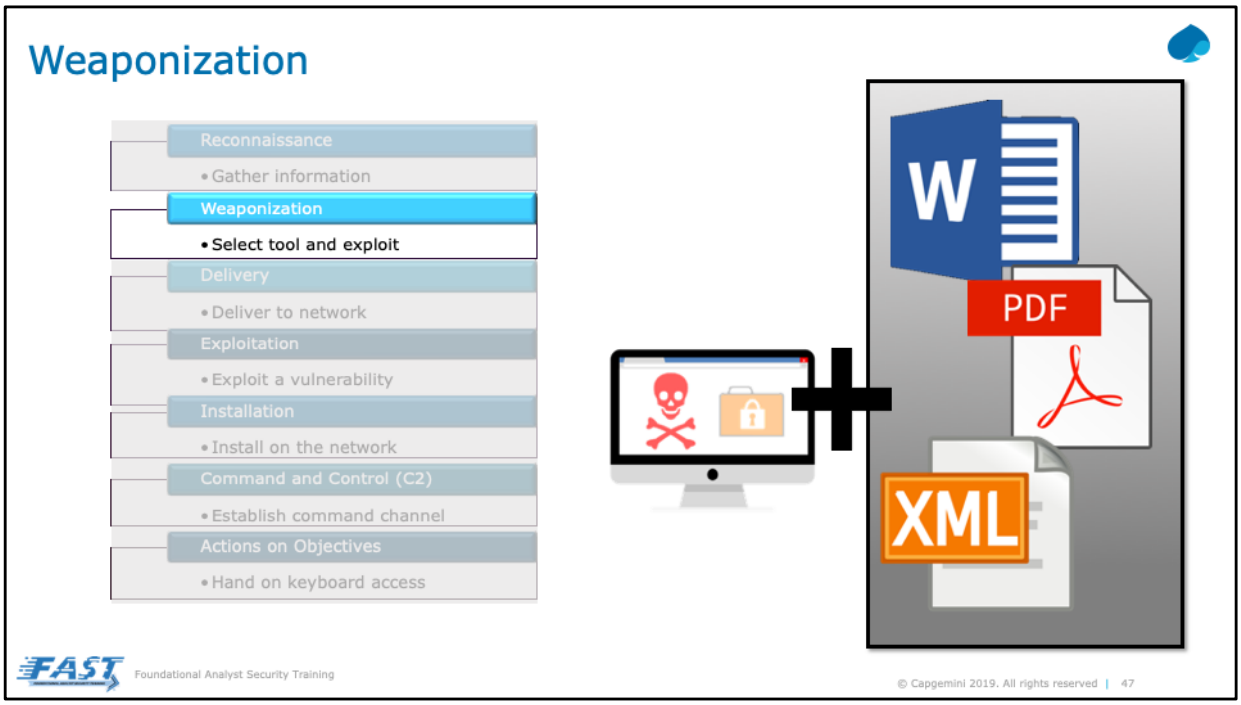
An attacker must get through every step in the kill chain in order to be successful, while the defender only has to trip them up once, this gives your organization the advantage in defending our networks.



Script:

{pause}

Reconnaissance - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.



Script:

{pause}

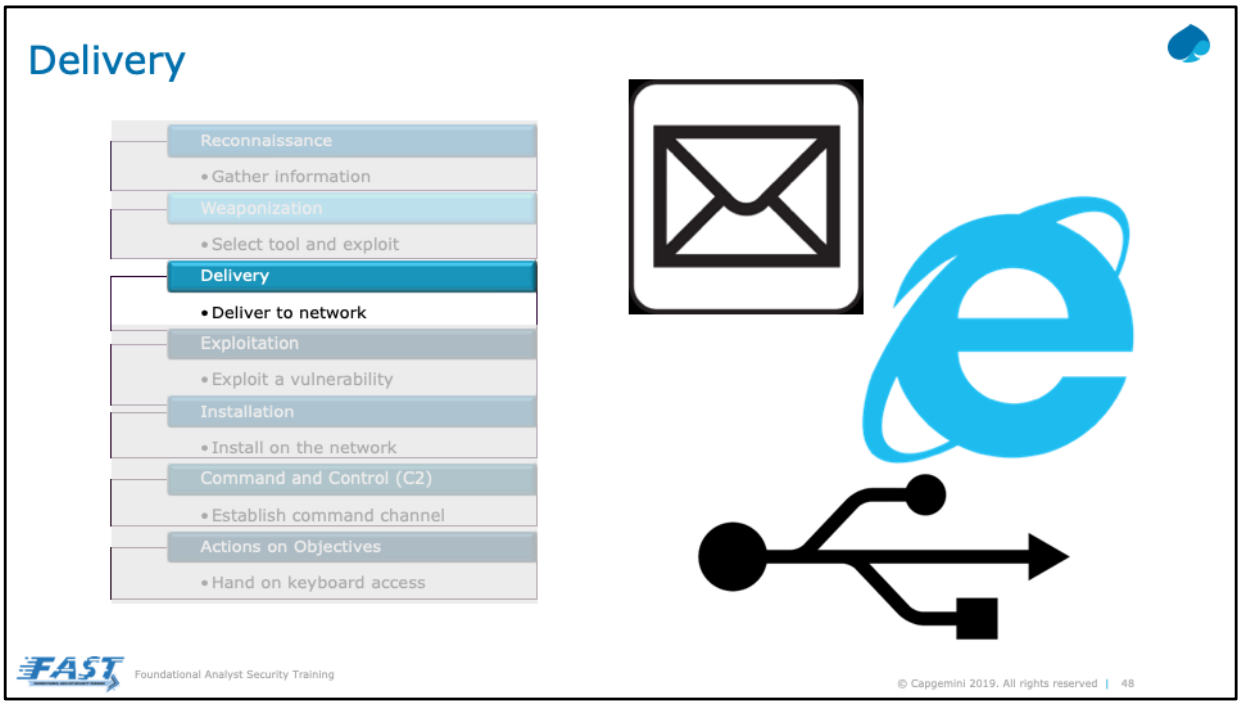
Weaponization – During this phase the attacker creates the weapon to leverage the security weakness that has been identified in the target environment. Weapons typically consist of a malicious payload and a benign container to transport the weapon to the target.

{pause}

For example, coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer).

{pause}

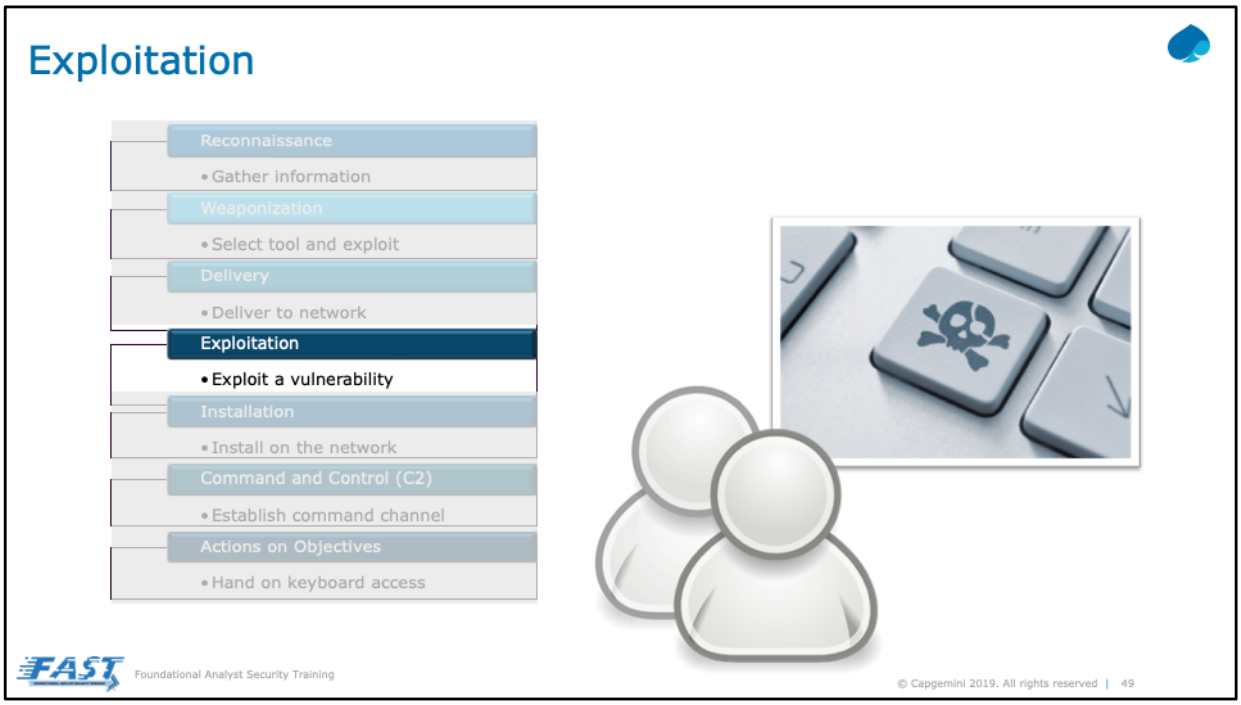
Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.



Script:

{pause}

Delivery – This Is the Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by threat actors, are email attachments, websites, and USB removable media. However, email and web traffic are often the primary concerns.



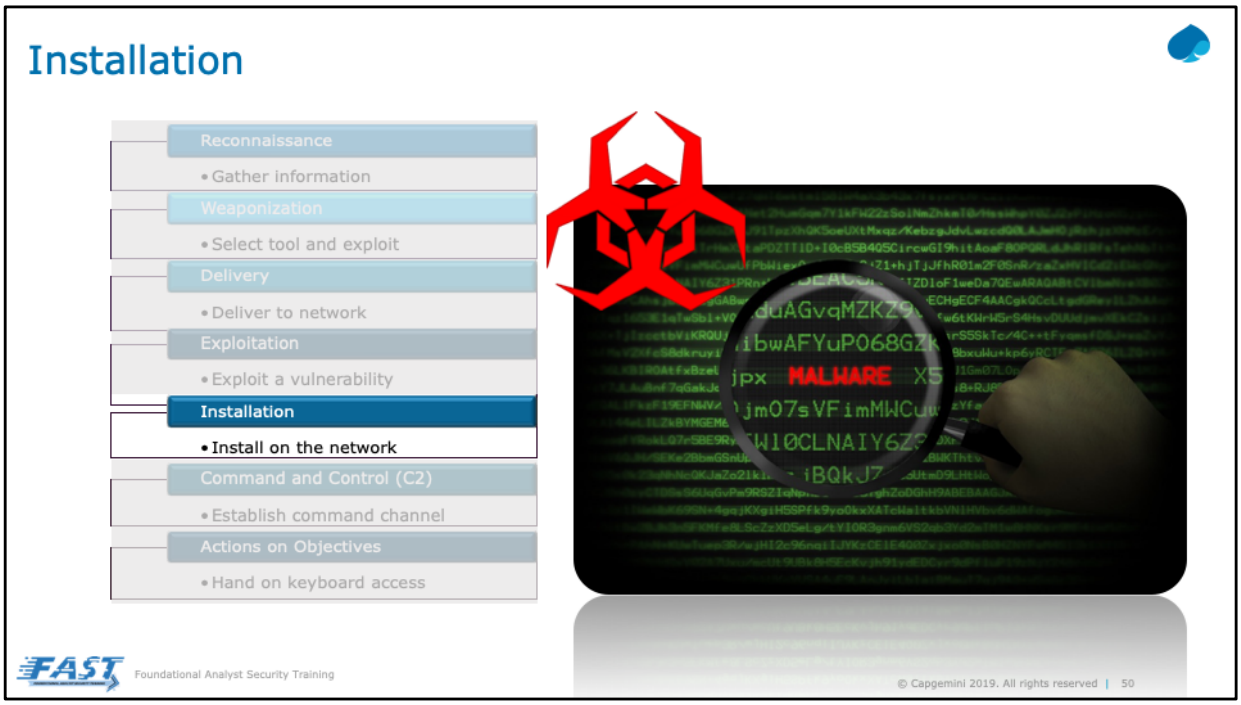
Script:

{pause}

Exploitation - After the weapon is delivered to victim host, exploitation triggers an intruders' code.

Most often, an exploitation targets an application or operating system vulnerability,

However it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

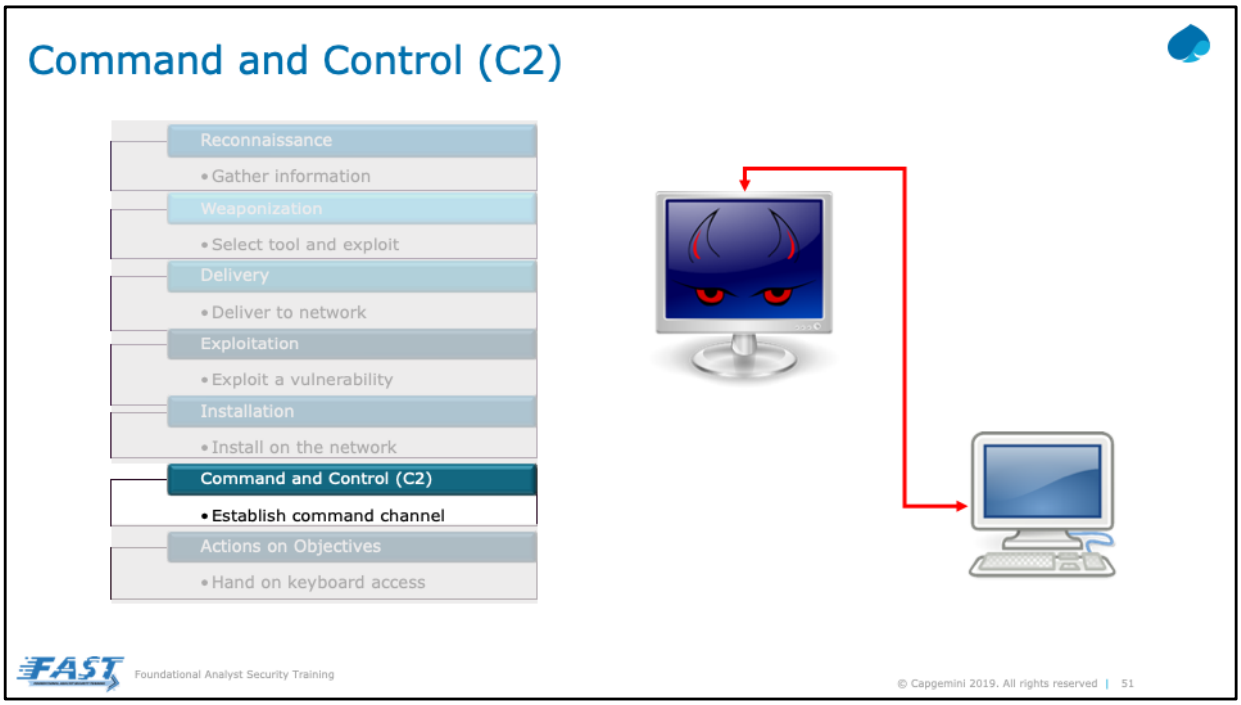


Script:

{pause}

Installation - Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

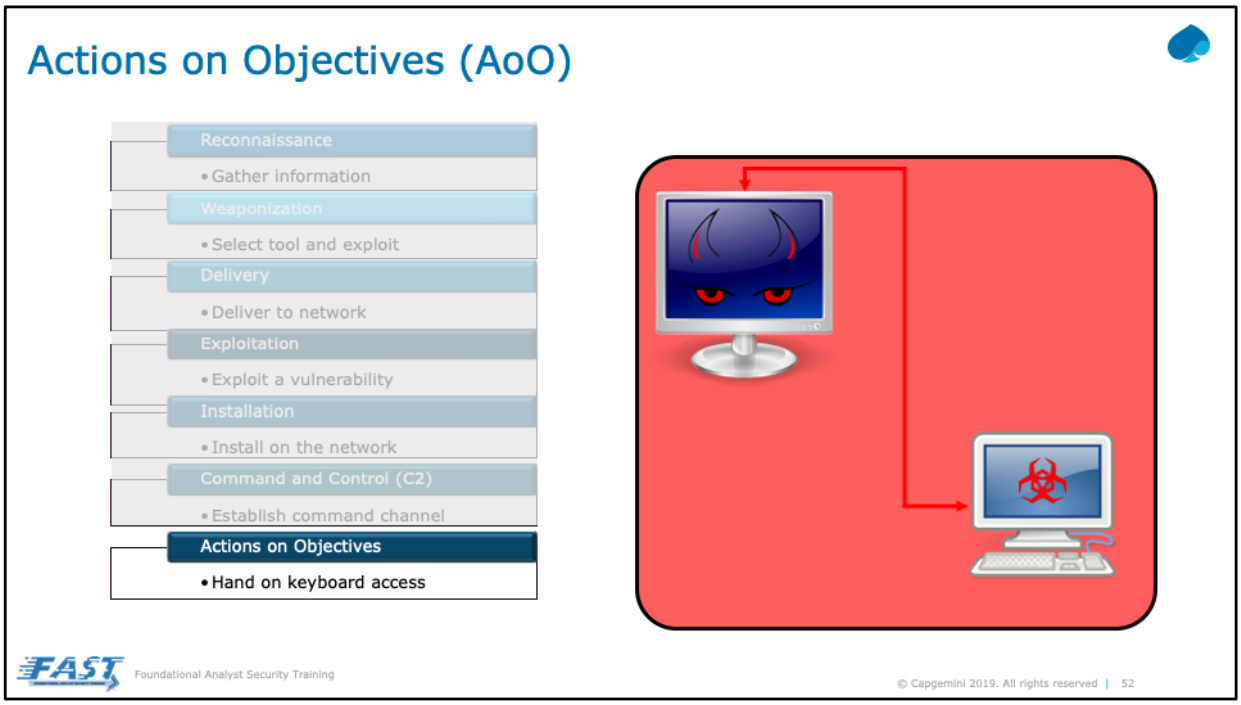
Because malware delivered through many of these methods has to be small and discreet, it may reach back out of the network to pull down more complex tools to install on the system.



Script:

{pause}

Command and Control (C2) - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have hands on the keyboard" access inside the target environment.

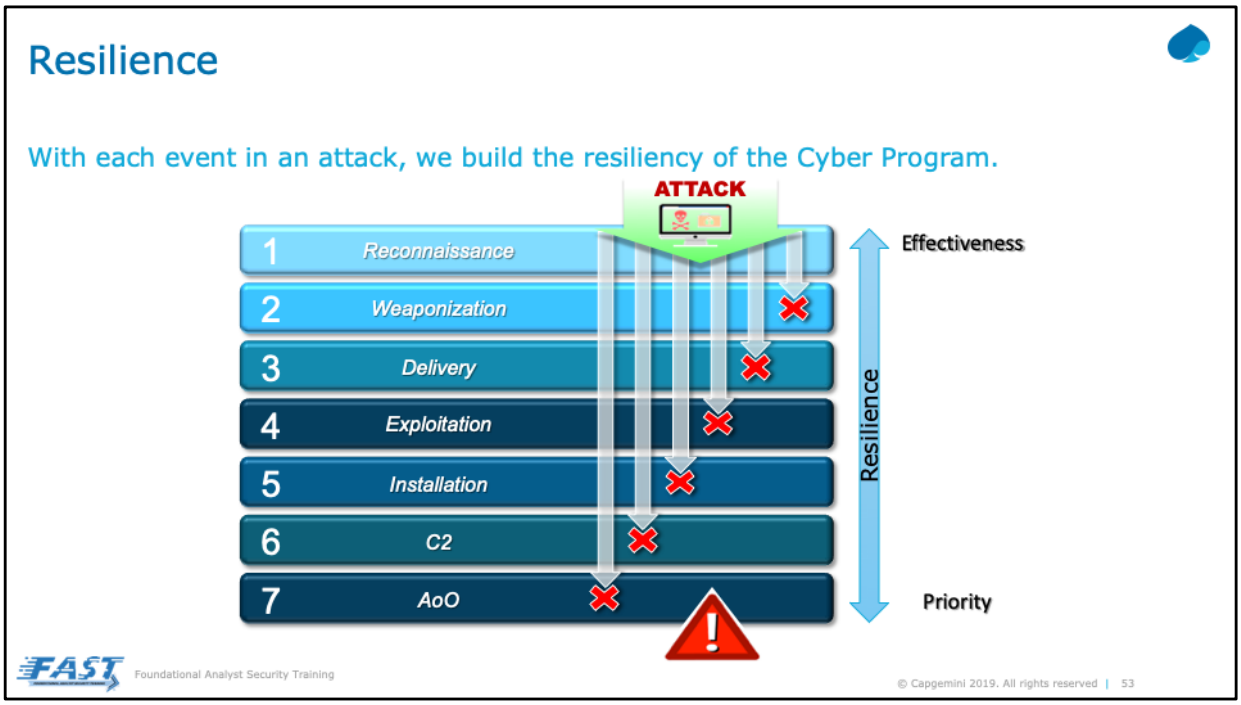


Actions on Objectives - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives.

The objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well.

Alternatively, the intruders may only desire access to the initial victim box for use as a foothold to compromise additional systems and move laterally inside the network.

This will include lateral movement into other networks, sometimes even into ICS and SCADA environments.

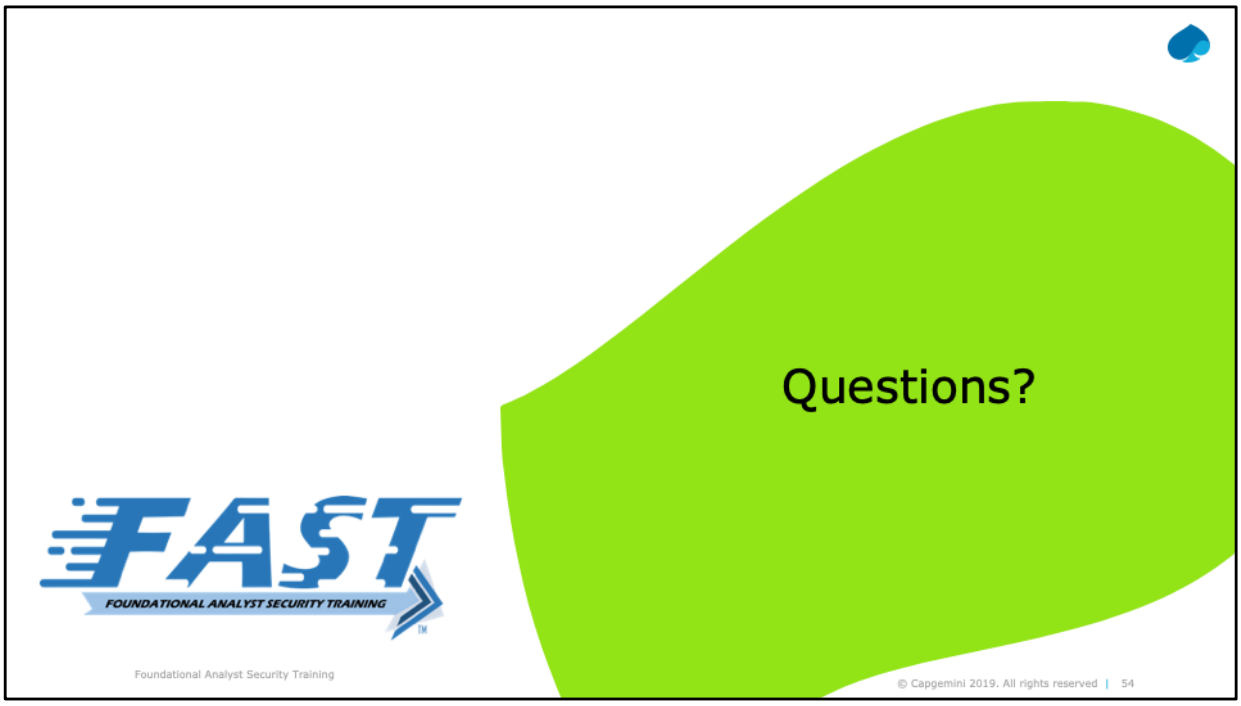


Script:

{pause}

With each event in an attack we build the resiliency of the cyber program. We capture the earliest known CKC phase of an attack so that when the incident is closed an organization can establish where the attack would be stopped if a similar attack were to occur again.

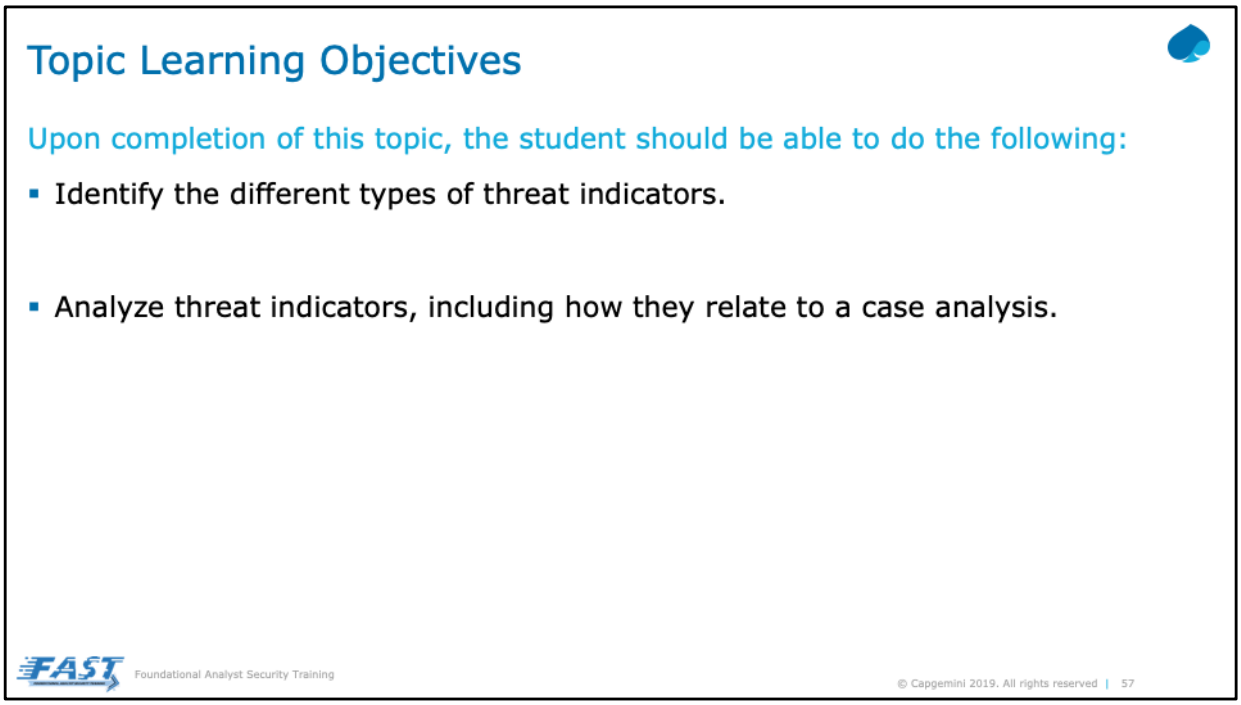
Its important to remember, that even after an attack has been stopped, and analysis has been conducted of the steps leading up to where the attack was intercepted, an organization must also use synthesis to extrapolate and determine the objectives of the attack, and determine where the attack would have progressed had it not been detected.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 54

Welcome to this module covering Threat Indicators.

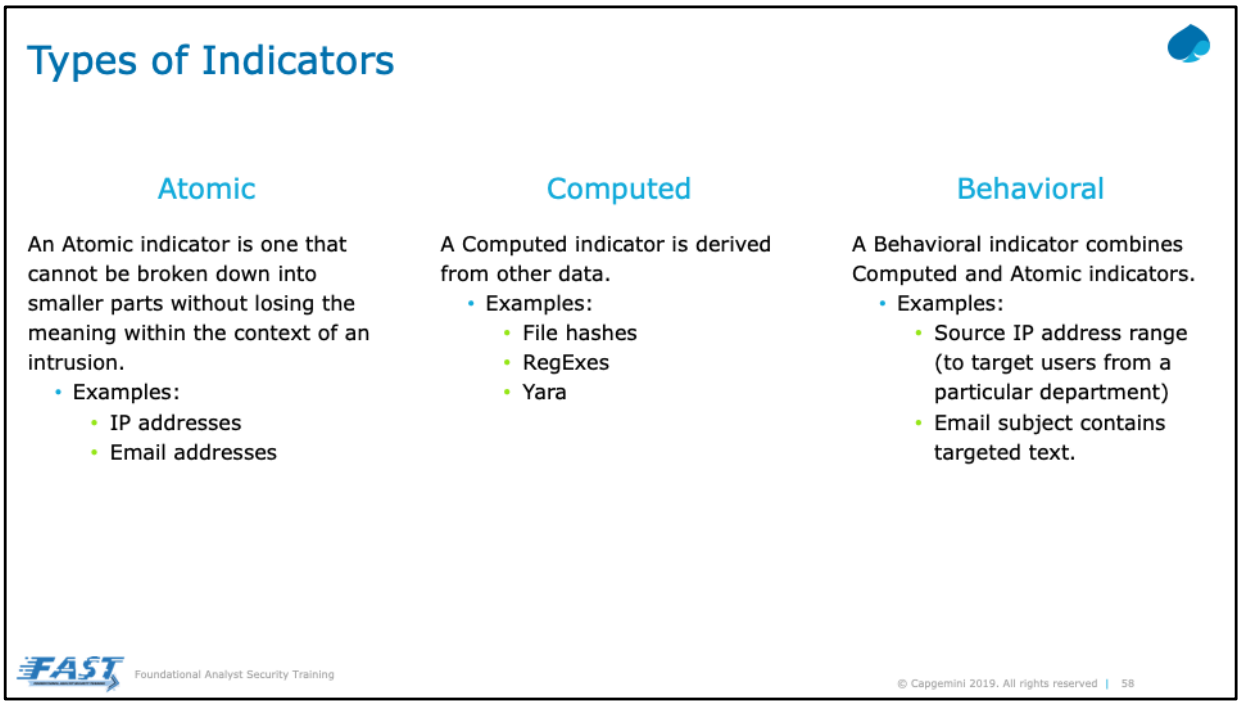
Agenda

TYPES OF THREAT INDICATORS | ANALYSIS OF THREAT INDICATORS



Upon completion of this module, students should be able to:

- Identify the different types of threat indicators
- Analyze threat indicators, including how they relate to a Case Analysis

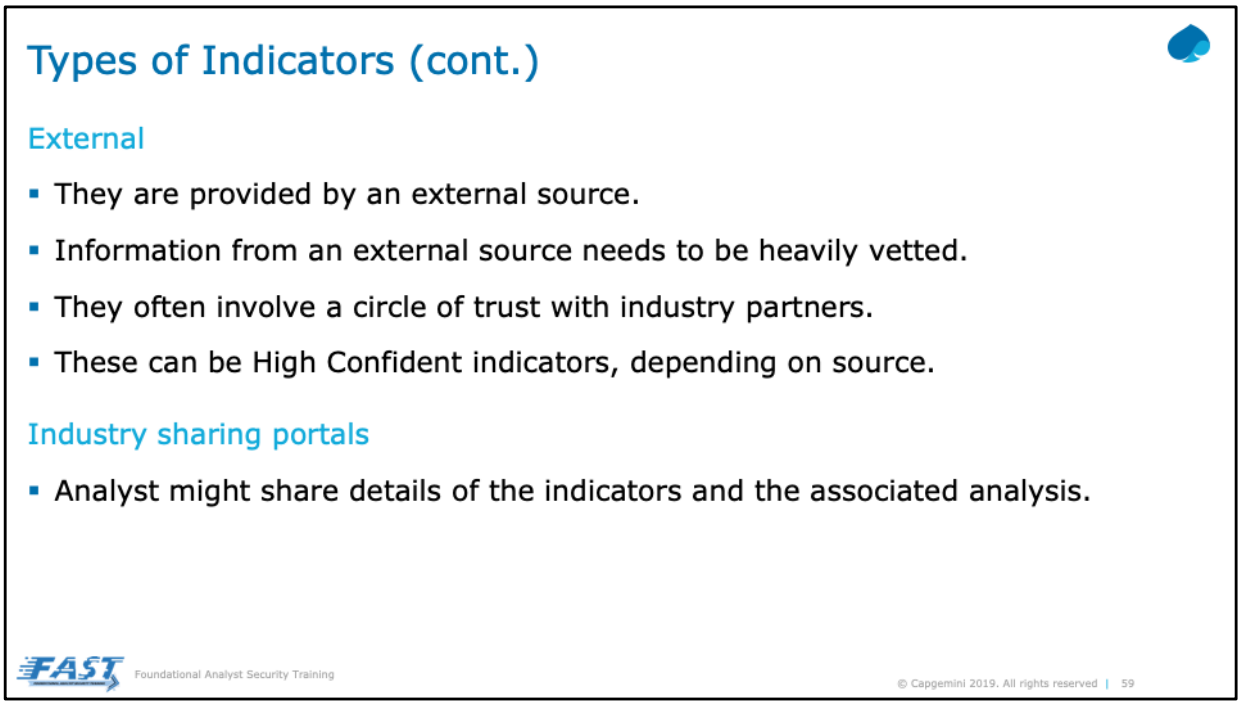


One way to categorize indicators is whether they can be broken down or if they are derived from other data.

An Atomic indicator is one that cannot be broken down into smaller parts without losing the meaning within the context of an intrusion, such as an IP addresses, MAC address, and Email addresses.

A Computed indicator is derived from other data, such as a File hash, which is derived from or computed from the actual file or message data.

A Behavioral indicator combines computed and atomic indicator, such as a Source IP address range (which could be used to target users from a particular department), or an Email subject which could contain targeted text.



Another way to categorize indicators is based on whether they are external or internal.

Paid feeds and subscriptions are often seen as very low value as its full of noise and the required vetting is impossible on the volume.

Second best are vendor provided intel/indicators.

Third are specialized industry feeds of active targeted threats,

Defense / Government feeds

Internally developed indicators.

Characteristics of External indicators include that:
- They are provided by an external source.
- Information from an external source needs to be heavily vetted, in order to determine the validity of the indicator.
- They often involve a circle of trust with industry partners.
- These can be High Confident indicators, depending on source.
- Industry sharing portals will often contain external indicators, including measures of their validity.
- Analyst might share details of the indicators and the associated analysis.

Characteristics of Internal indicators include that:
- They are discovered internally (where the perspective of internal versus external typically depends on the scope or sphere of influence of the entity you are working with).
- They are known applicable and have a high level of confidence, since typically some measures of inherent vetting has already taken place.

Types of Indicators (cont.)

Internal

- They are discovered internally.
- Provides high level of confidence because they are generated by active threat actors targeting the organization. Internal

FAST Foundational Analyst Security Training

Another way to categorize indicators is based on whether they are external or internal.

Characteristics of External indicators include that:

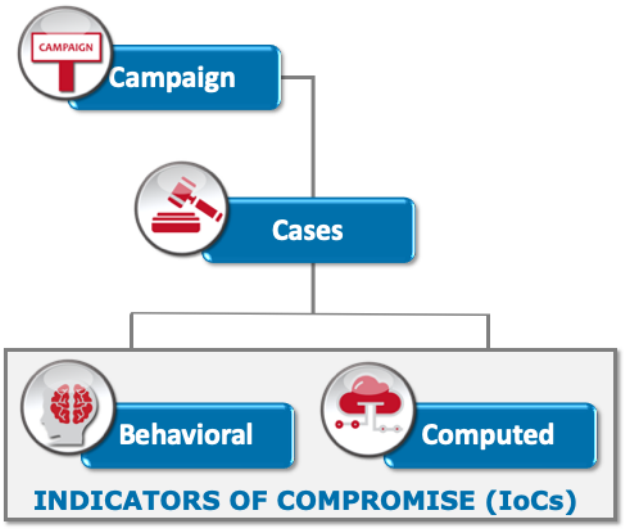
- They are provided by an external source.
- Information from an external source needs to be heavily vetted, in order to determine the validity of the indicator.
- They often involve a circle of trust with industry partners.
- These can be High Confident indicators, depending on source.
- Industry sharing portals will often contain external indicators, including measures of their validity.
- Analyst might share details of the indicators and the associated analysis.

Characteristics of Internal indicators include that:

- They are discovered internally (where the perspective of internal versus external typically depends on the scope or sphere of influence of the entity you are working with).
- They are known applicable and have a high level of confidence, since typically some measures of inherent vetting has already taken place.

Analysis of Threat Indicators

A case analysis includes determining what information and indicators correlate to seemingly unrelated events.



FAST Foundational Analyst Security Training

Determining what information correlates to seemingly unrelated events, and adding it to inform campaigns is a key part of the Kill Chain.

As previously mentioned, there are different type of indicators, and the Kill Chain considers different types of information, or indicators, in order to inform cybersecurity decisions. As previously mentioned, indicators are often categorized as Atomic, Computed and Behavioral. Atomic indicators cannot be broken down into smaller parts and still retain their meaning. Computed indicators are derived from other. Behavioral indicators are collections of computed and atomic indicators.

Analysis of Threat Indicators (cont.)

Threat intelligence is understanding that information and indicators inform all parts of a Cyber Kill Chain®.

Analysis of Threat Indicators (cont.)

Pivoting is the process of using known information to find unknown information.

Many SOC Teams fail at doing this well.

It is extremely important to use the pivoted data to enhance monitoring, or it is worthless.

FAST Foundational Analyst Security Training

Pivoting is an essential intelligence generating process, that allows an agile defender to develop new intelligence by correlating information from multiple attacks, attackers, and environments. However, to be able to effectively pivot, the information, or

intelligence, from other attacks must exist. When pivoting, you will consider various factors and how they might relate to other known attacks or campaigns, such as:

Who may be compromised?

What methods of infiltration is the adversary using?

When did they attack?

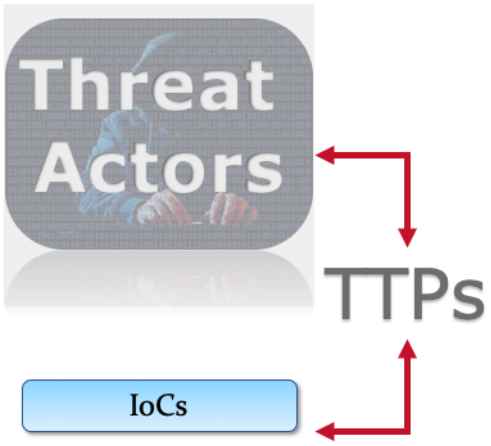
Where is the adversary in our network?

Why were certain users targeted?

How do we decode the C2 commands?

Analysis of Threat Indicators (cont.)

The principle goal of case analysis is to determine what TTPs a particular APT is utilizing to associate other information.



FAST Foundational Analyst Security Training

The Principle goal of Case Analysis, is to determine what Tactics, Techniques, and Procedures a particular APT is utilizing in order to associate other information. A Case Analysis will look at, analyze, and correlate those types of factors covered on the previous slide to try to be proactive and adaptive in our defenses, such as:

- Considering who may be compromised and how that relates to a previous attack, such as whether a particular group was compromised or whether those who were compromised share particular characteristics or attributes.
- Or looking at when the attack occurred, such as whether it occurred at a particular time of day or after a particular event, such as the launching of a new web site or at the beginning of a major holiday.

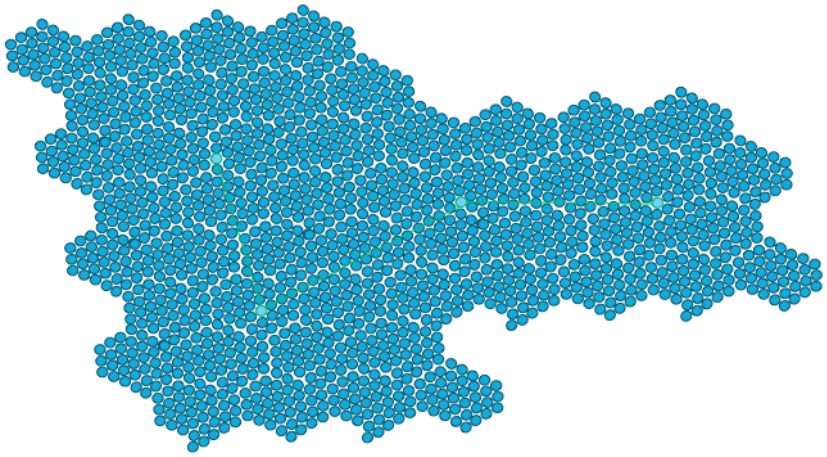
Analysis of Threat Indicators (cont.)

This allows the organization to evaluate the threat actor and try to discern their intent.

FAST Foundational Analyst Security Training

The first time an action is observed, with no other meaningful intelligence, it is very difficult to determine the next actions or intent. However, with intelligence and knowledge of past events, indicators, and campaigns, this allows the organization to evaluate the threat actor, and try and discern their intent and upcoming actions.

Analysis of Threat Indicators (cont.)



Indicators can be linked to pivot to new indicators.

This is important because we cannot always easily see the indicators; they will be obscured by the vast amount of data that is available for analysis.

FAST Foundational Analyst Security Training

Analyzing multiple intrusion kill chains over time will identify commonalities and overlapping indicators. Again, this is knowledge, or intelligence, that organizations can use to discern an attacker's intent or next actions in order to try to stay a step ahead of the attacker. This allows organizations to be proactive and adaptive, rather than always being reactive to events that occur.

Most consistent indicators, the campaigns key indicators, help defenders prioritize mitigation development and derive defensive courses of action.

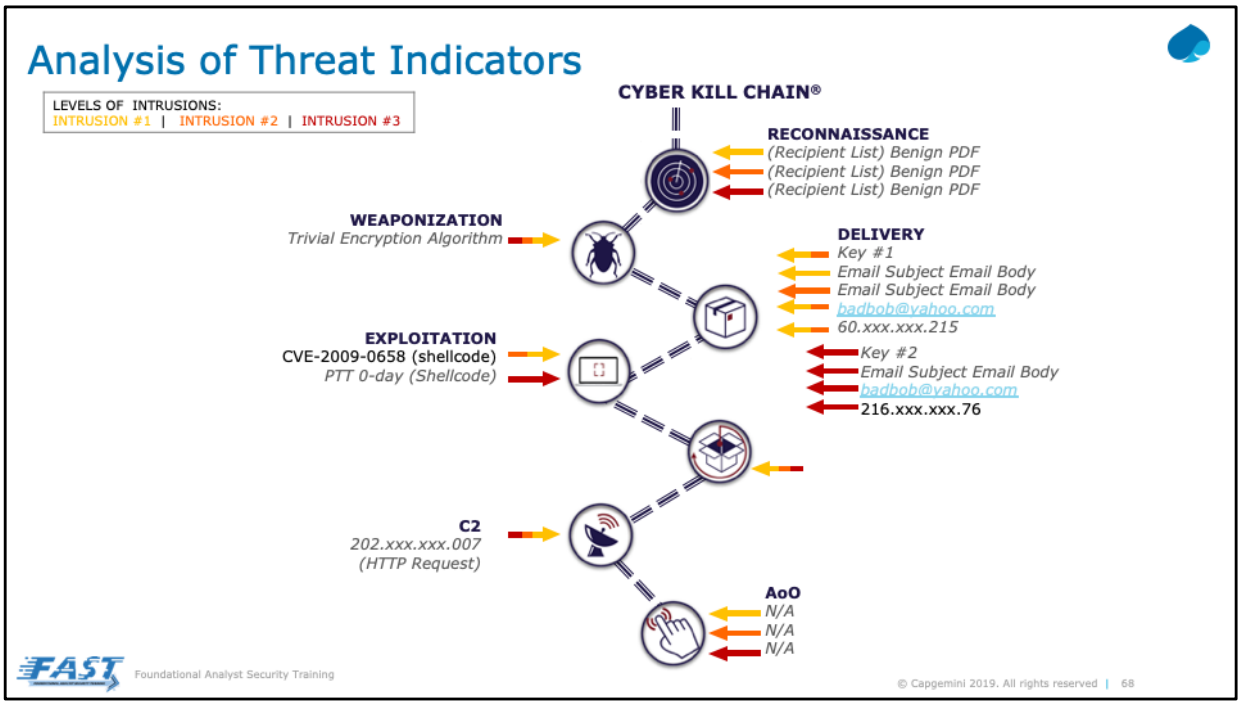
How about an example…

Social Media Traffic

- Social media traffic has become so pervasive in our network environments; it is everywhere, and it is harmless… or is it?
- This is the perfect example of the type of traffic that an APT might use to obscure their traffic.

FAST Foundational Analyst Security Training

Also real Facebook can be used for C2 commands. Attackers use a profile and updates to it can be looked at. The attacker will place hidden html code in it, that their malware will see. The malware gets commands on what to do and where to send the output.



Organizations must be prepared to defend against sophisticated intrusion attempts by well-trained and organized adversaries.

The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. Therefore, the idea of the cyber kill chain is to understand the discrete steps that an attacker must progress through to meet their objectives.

So even if the exploit is different or a Zero-day is used, there is high likelihood that the tools and techniques used in other phases will remain the same. As a network defender, identifying this puts the advantage back our court. There is something to learn from each phase – we can examine each step to determine if our defenses are adequate.

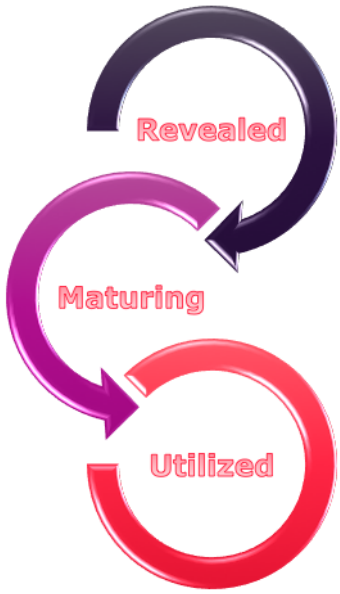
This may include exercises like sandboxing the exploit or malware to learn more about how it works. If we have a “Late Phase Detection”, we look at earlier phases to find indicators. If we have an “Early Phase Detection”, we look down the chain to

learn more about the attacker's methods and objectives. This is where we really start using the Cyber Kill Chain concept to our advantage and tune our defense in depth strategy accordingly.

Analysis of Threat Indicators (cont.)

Indicator Life Cycle

- **Revealed**
  - Through analysis or collaboration
- **Matured**
  - Leveraged into tools
- **Utilized**
  - Matching activity discovered



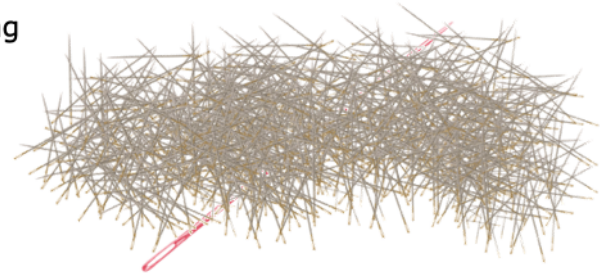
FAST Foundational Analyst Security Training

Indicators go through a process of maturity which makes them more useful to the organization. When a new indicator is revealed it still must be vetted and corroborated by other indicators, as an indicator matures it becomes more useful and can be more effectively utilized. Indicators are revealed through analysis or collaboration; as they are vetted, they mature and will be leveraged into tools; then the are more utilized and matching activities are discovered.

How Do We Find These Indicators?

Are they just lying around?

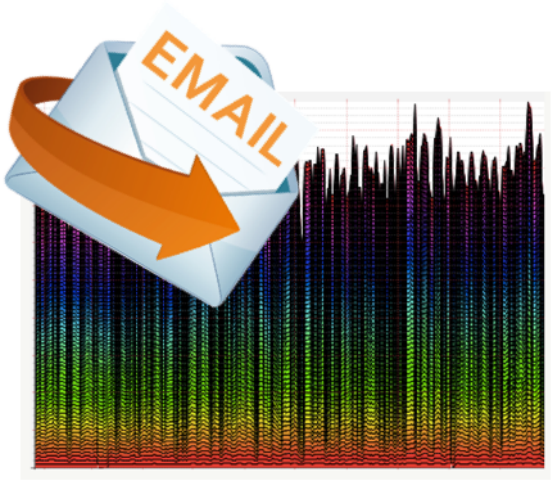
- APTs are good at what they do; they are not going to make things easy.
- They are skilled at leaving as little evidence behind as possible and hiding what they do leave in a way where normal network traffic will prevent its discovery.
- A needle in a stack of needles…



Another Example…

Phishing Emails

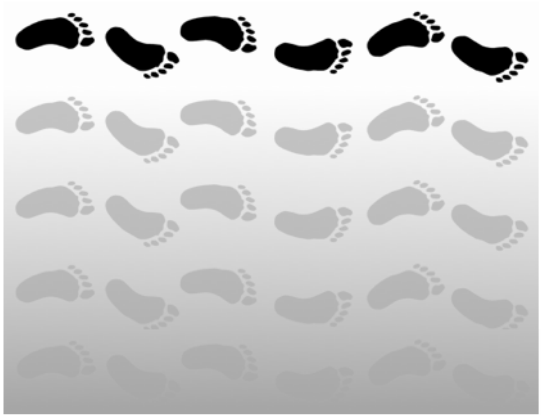
- Phishing emails are another technique that hides in plain sight.
- Without input from users, they would be very difficult to find.
- Those annoying phishing tests are inconvenient, but they are a good way to find new or targeted phishing attacks.

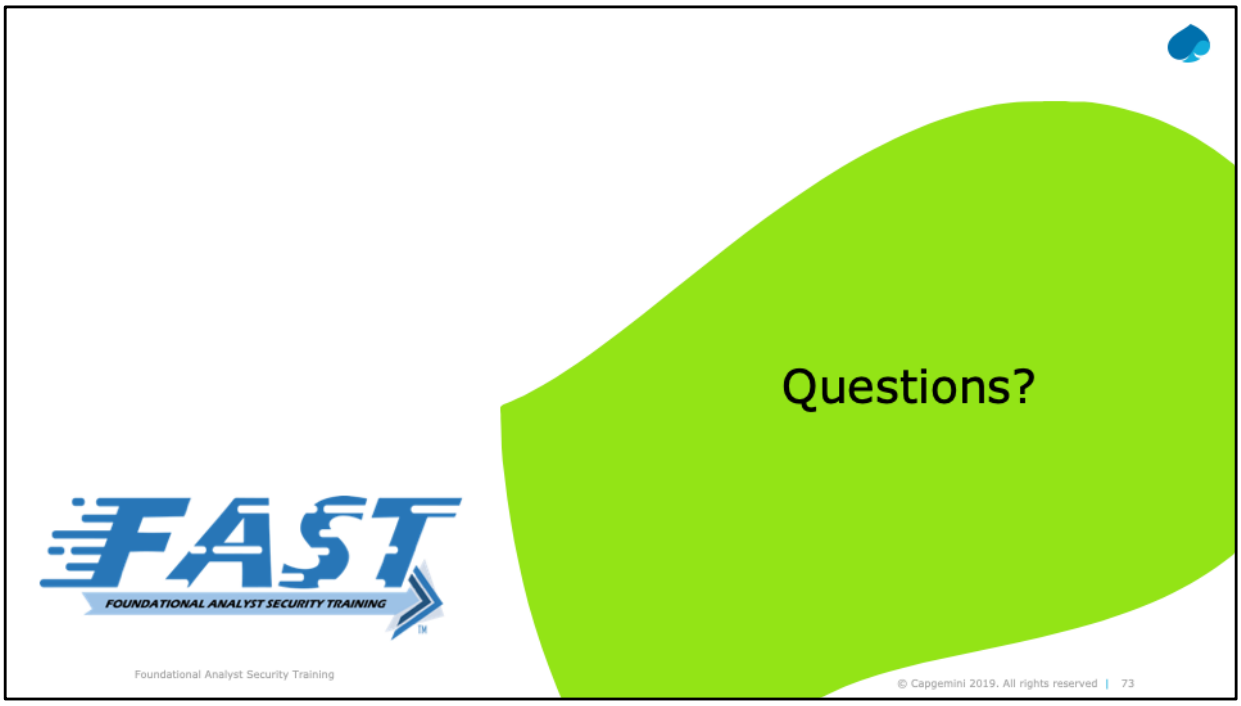


Hide in Plain Sight

If an infiltration or exfiltration is obvious, then it is not effective.

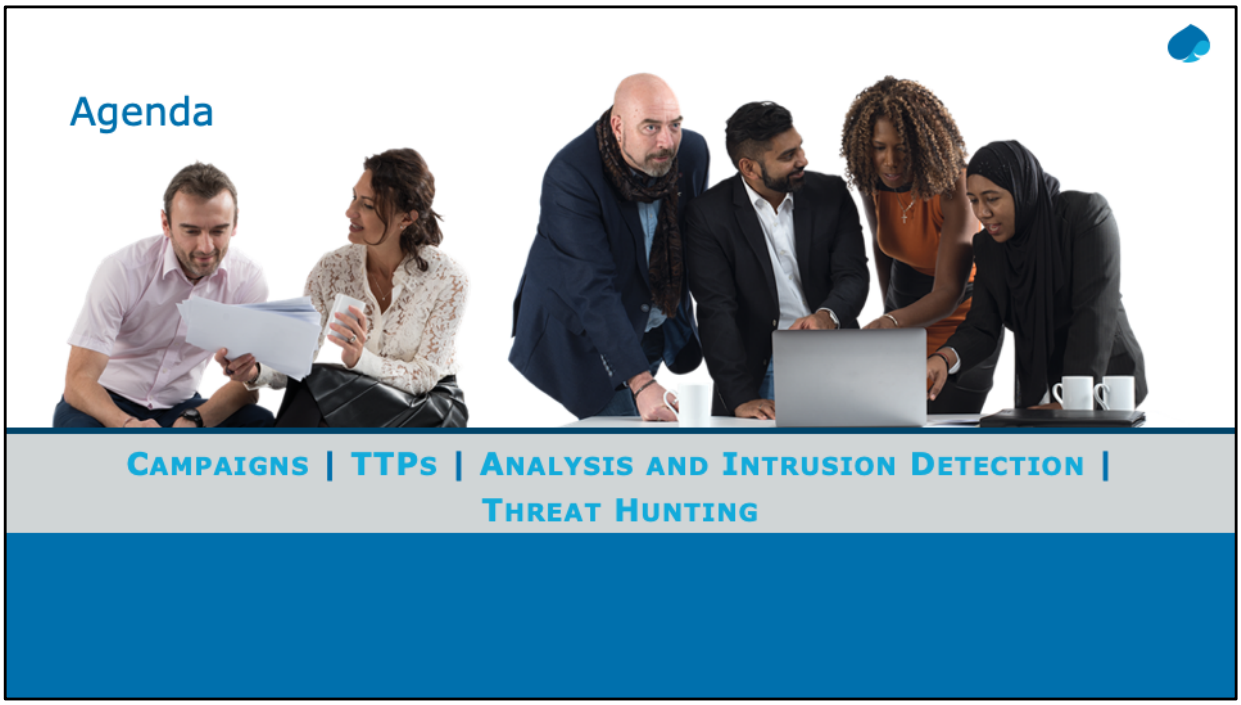
- An APT will attempt to leave as little of a footprint in the network as he can.
- When we attempt to locate indicators, it will not be easy.
- In this class, we lay things out for you in a straight line; but, in real life, it will not be so easy!



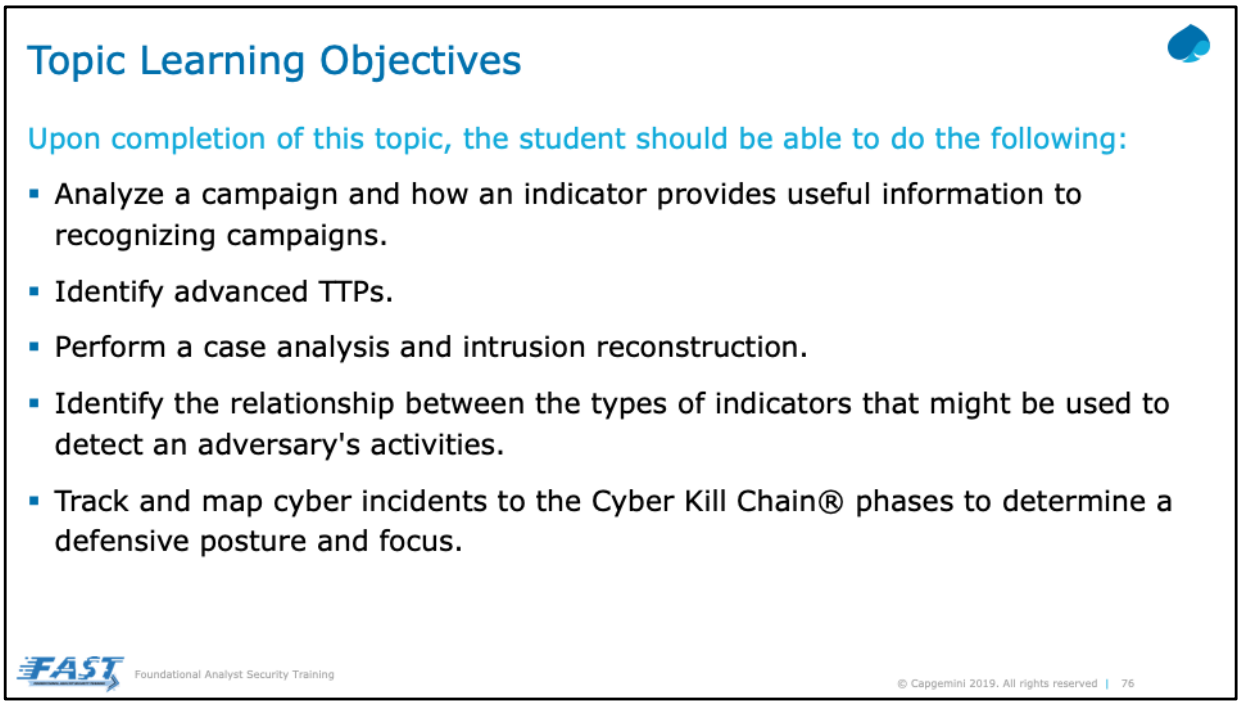

Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 73

Case Analysis

Capgemini



- Case Analysis
- Tactics, Techniques, and Procedures (TTP)
- Analysis and Intrusion Reconstruction
- Cyber Threat Hunting
- Cyber Strategy – Kill-Chain



Upon successful completion of this module, students will be able to:

- Analyze a campaign and how an indicator provides useful information to recognizing campaigns
- Identify advanced tactics, techniques, and procedures
- Perform a Case Analysis and intrusion reconstruction
- Identify the relationship between the types of indicators you might use to detect an adversary's activities
- Track and map cyber incidents to the Kill Chain phases to determine a defensive posture and focus

Campaign Tracking

Over time, if valuable intelligence is collected on each of the attacks and the case information is properly managed, the adversaries' persistence becomes a liability; and the adversaries Cyber Kill Chain® TTPs can be observed.

Use this intelligence to determine **who** is targeted, **what** is targeted, **where** it is being targeted from, and **why** it is being targeted.

FAST Foundational Analyst Security Training

Over time, if good intelligence is collected on each of the attacks, and the case information is properly managed, the adversaries persistence becomes a liability and the adversaries cyber kill chain TTP's can be observed. With campaign tracking, you will be able to be more proactive and predictive about their next actions.

Use this intelligence to determine who is targeted, what is targeted, and what is being used in the attack.

Campaign Tracking (cont.)

Who is targeted?

FAST Foundational Analyst Security Training

 | 78

Campaign tracking will help to correlate who is targeted with the associated TTPs in order to be a step ahead of the adversary.

Campaign Tracking (cont.)

What technology is being targeted?

FAST Foundational Analyst Security Training

In the same manner, you will analyze what technology is being targeted.

Campaign Tracking (cont.)

What specific infrastructure is used in the attack?

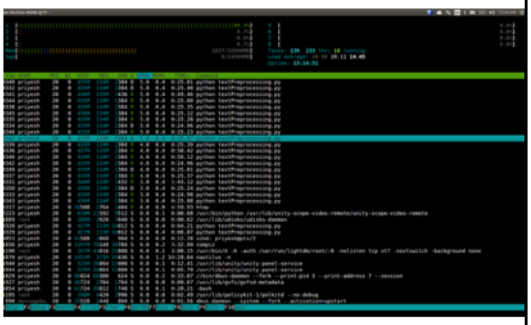
FAST Foundational Analyst Security Training

 | 80

Identify what specific infrastructure is used in the attack?

Campaign Tracking (cont.)

What exploits and installation are being utilized?



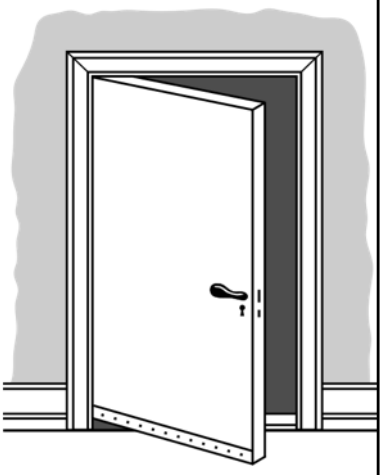
FAST Foundational Analyst Security Training

 | 81

Determine what exploits and installation are being utilized.

Campaign Tracking (cont.)

What backdoor is being utilized?



FAST Foundational Analyst Security Training

 | 82

Determine if a backdoor is being utilized.

Campaign Tracking (cont.)

What C2 infrastructure is being used?

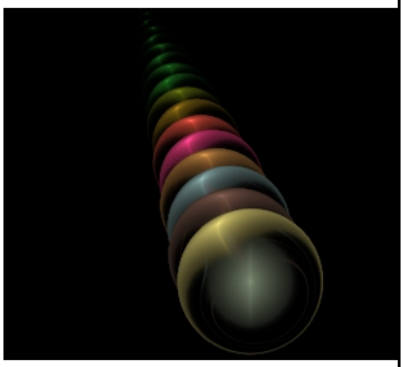
FAST Foundational Analyst Security Training

 | 83

Determine what command and control infrastructure is being used.

Campaign Tracking (cont.)

Ensure multiple indicators align with high fidelity before attributing them to a specific attacker.



FAST Foundational Analyst Security Training

Bear in mind we must be careful when correlating information, some attackers use similar infrastructure, so before assigning attribution, it is important to have multiple indicators that align with a high fidelity. Likewise, through advanced analysis and campaign tracking, you should be able to establish this high fidelity at a much faster rate.

Tactics, Techniques, and Procedures (TTPs)

Tactics

- What an attacker uses to execute the attack

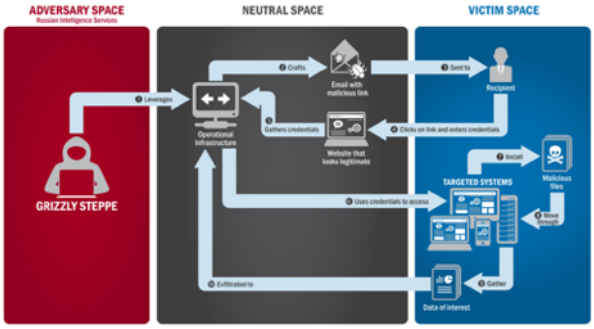
TACTICS are what an attacker uses to execute the attack.

An example of a “Tactic” is using a particular malware to steal a user’s credentials.

Tactics, Techniques, and Procedures (TTPs) (cont.)

Techniques

- How the exploit is executed or delivered to the organization



FAST Foundational Analyst Security Training

 | 86

How the exploit is executed (Universal Serial Bus [USB] drive, email, honeypot).

An example of a “Technique” is a threat actor who uses a particular attachment with a specific exploit, that compresses and transmits all Office documents, and sends them to the threat actor via a command and control channel established during the attack.

Attackers often have playbooks that they implement once they are inside your organization.

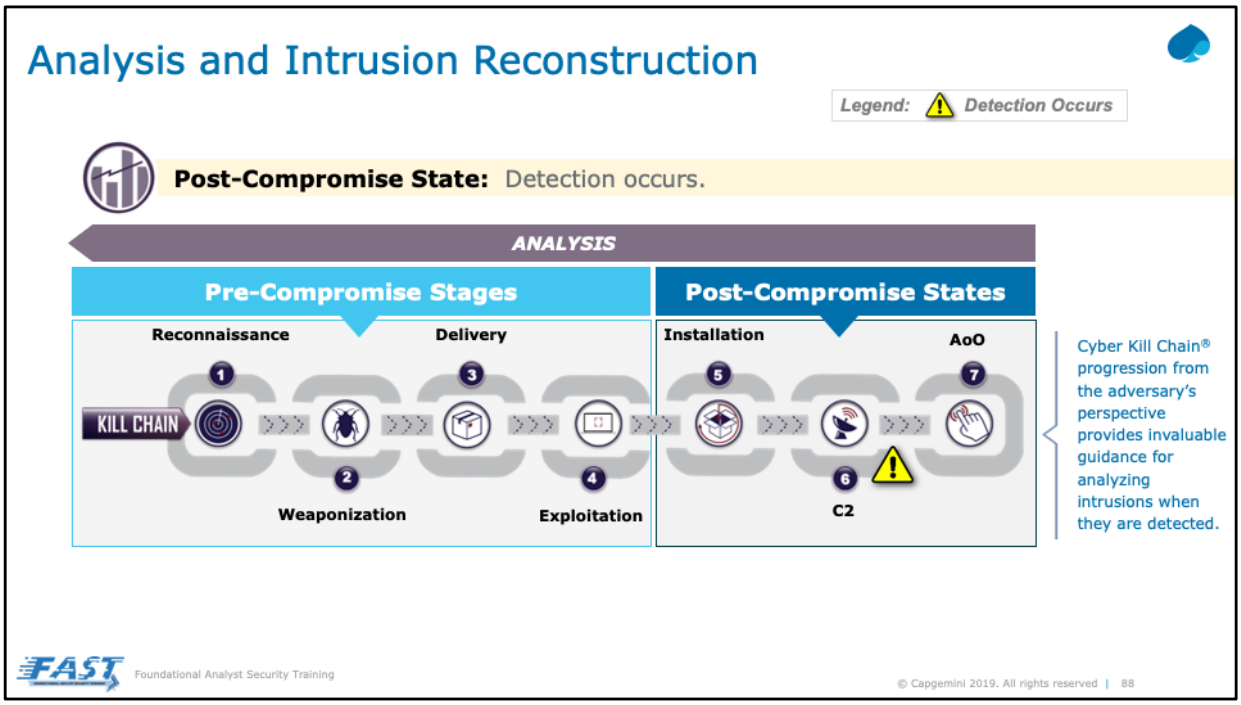
Tactics, Techniques, and Procedures (TTPs) (cont.)

Procedures

- How different tools and processes are used in concert with one another

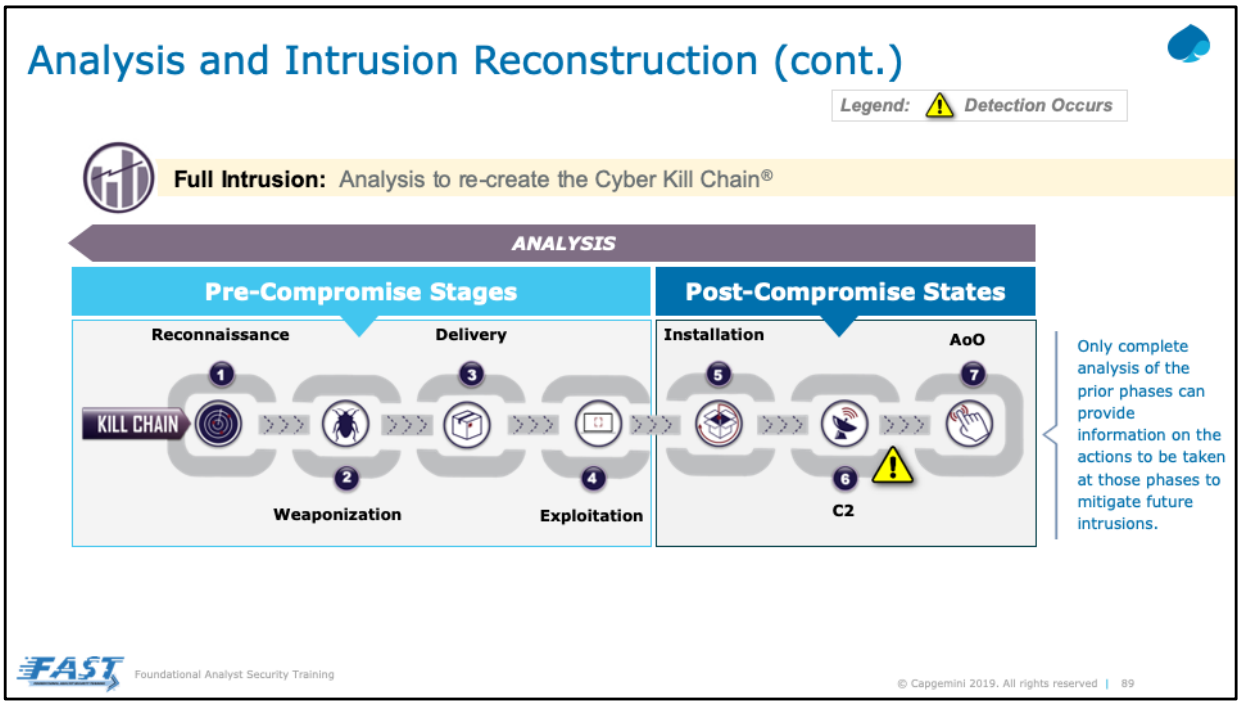
Procedures are how different tools and processes are used in concert with one another.

An example of a “Procedure” is determining which targets are most easily compromised, crafting an email that will encourage the user to interact, and finally delivering an exploit that will shut down Anti-Virus software, and connect to the command and control server by registering a domain and sending an email.



Seeing and understanding the kill chain progression from the adversary's perspective provides invaluable guidance for analyzing intrusions when they are detected. A given detection will typically provide a limited set of attributes for any single phase of an attack, but further analysis can reveal many other features and provide options for multiple courses of defensive action.

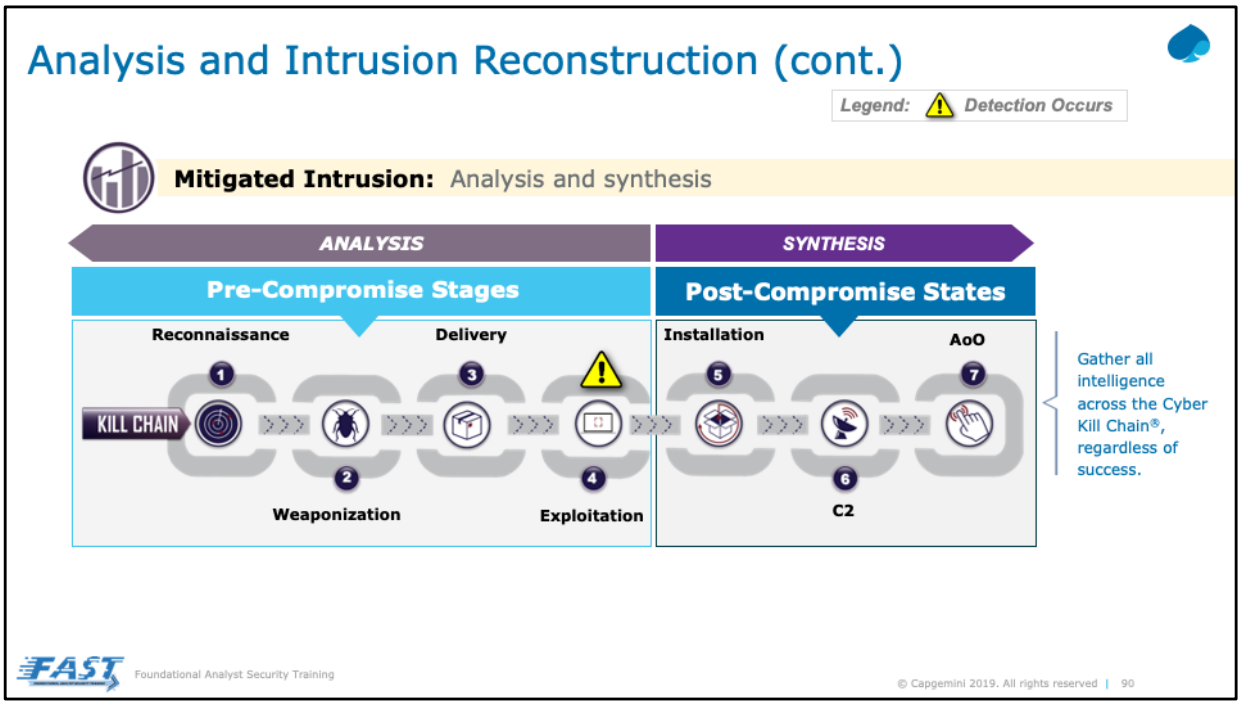
Furthermore, detecting an intrusion in one phase allows defenders to track the attack to prior phases that were executed successfully without detection. The early intrusion phases can then be analyzed to gather information that will help disrupt future attacks earlier in the kill chain.



For example, for a full intrusion, only through complete analysis, synthesis, and extrapolation of the prior phases can provide information on the actions to be taken at those phases to mitigate future intrusions.

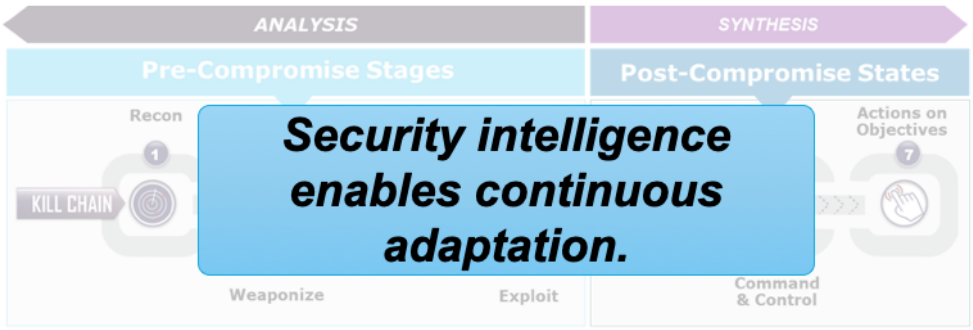
If one cannot reproduce the delivery phase of an intrusion, one cannot hope to act on the delivery phase of subsequent intrusions from the same adversary.

By completely understanding an intrusion we force an adversary to change every phase of their intrusion in order to successfully achieve their goals in subsequent intrusions. In this way, we use the persistence of adversaries' intrusions against them to achieve a level of resilience.

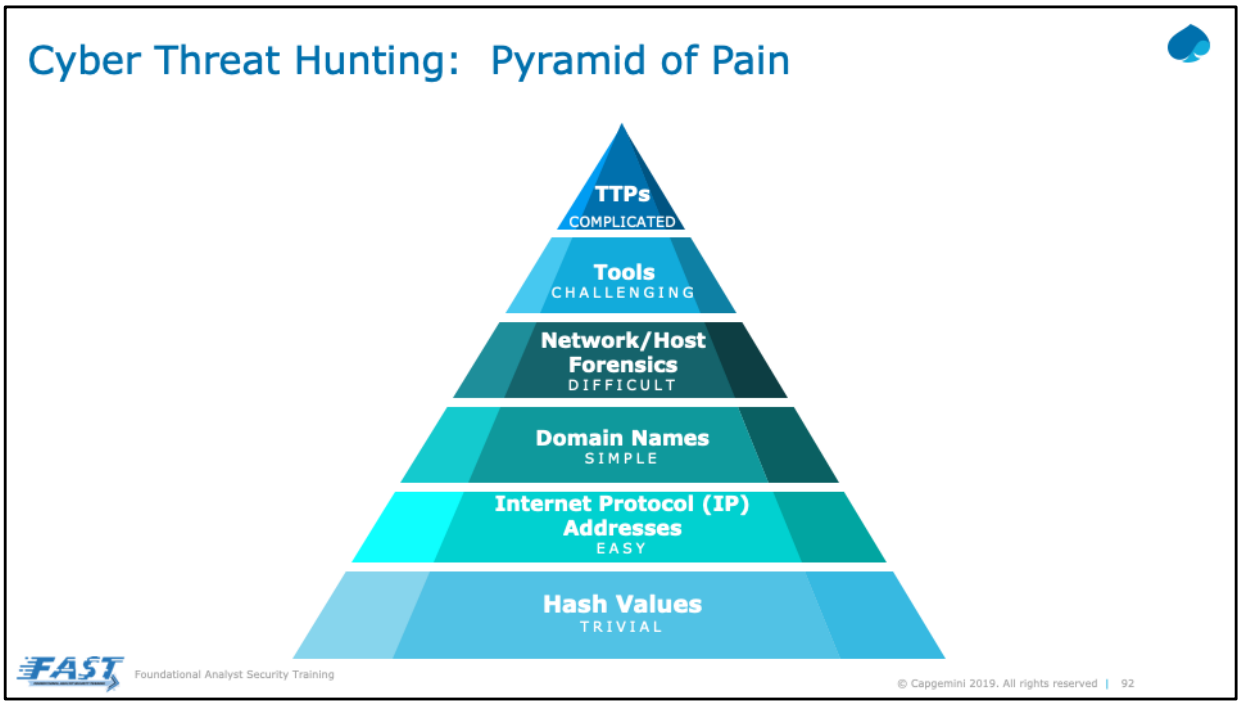


Equally as important as thorough analysis of successful compromises is synthesis of unsuccessful intrusions. We collect data on adversaries enabling us to push detection from the latter phases of the kill chain into earlier ones. Detection and prevention at pre-compromise phases also necessitates a response. Therefore, we collect as much information on the mitigated intrusion as possible, so that we can synthesize what might have happened should future intrusions circumvent the currently effective protections and detections.

Analysis and Intrusion Reconstruction (cont.)



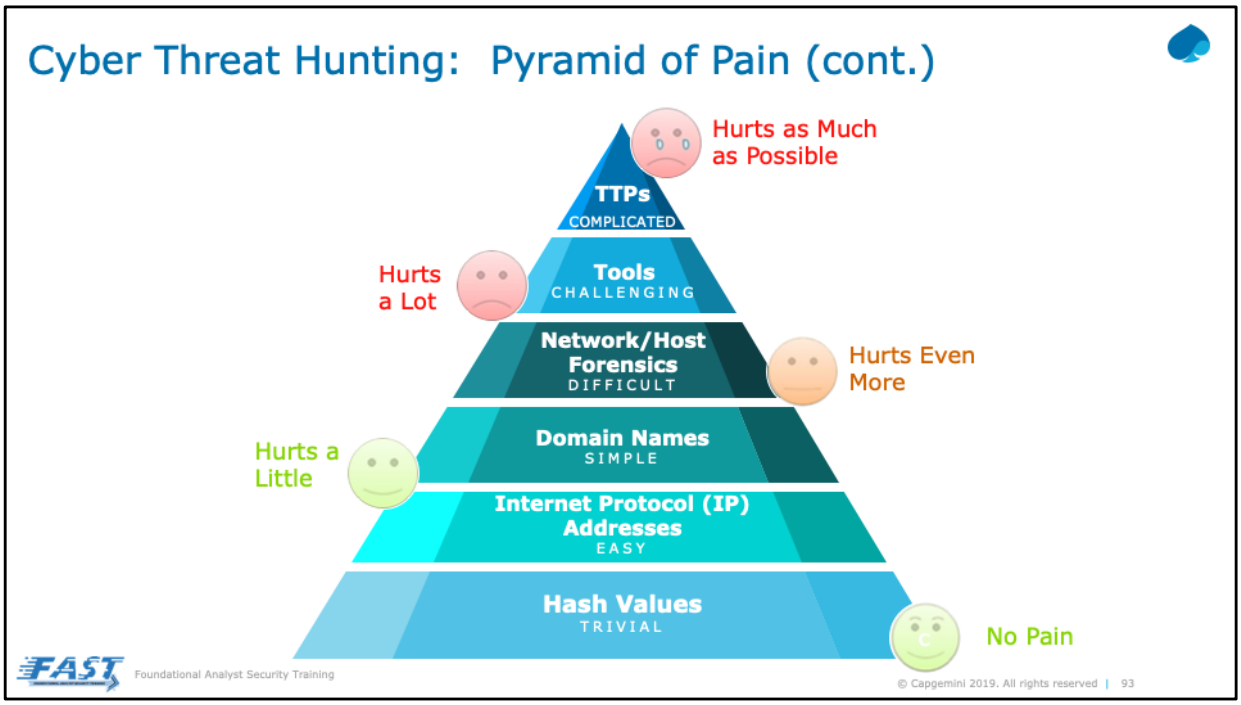
For example, an adversary could send a zero day exploit within a spear phishing email to an individual in the organization. The exploit would not be discovered by the anti-virus software at the gateway or the workstation, but the delivery of the email included indicators that were associated with a known APT campaign, and the intrusion is blocked at the delivery phase. Synthesis of the remaining kill chain might reveal a new exploit or backdoor contained therein. Without this knowledge, future intrusions, delivered by different means, may go undetected. This realization allows us to be much more effective in developing resilient mitigations, mounting a proactive defense instead of playing catch-up, and prioritizing investments in new technology and processes.



The Pyramid of pain is a hierarchy of how difficult it is to collect and apply indicators of compromise to cyber defenses…

Malicious hash values and IP addresses are relatively easy to acquire and integrate into security tools. TTPs are more difficult to identify and apply, as most security tools are not well suited to take advantage of them.

Tus, as it becomes more difficult to acquire and integrate the indicators, it increases the level of “pain” – or difficulty, but it also represents information that you be more useful or valuable during an attack.



Just like at the doctors, we need to know much pain can an indicator of compromise inflict on our adversaries.

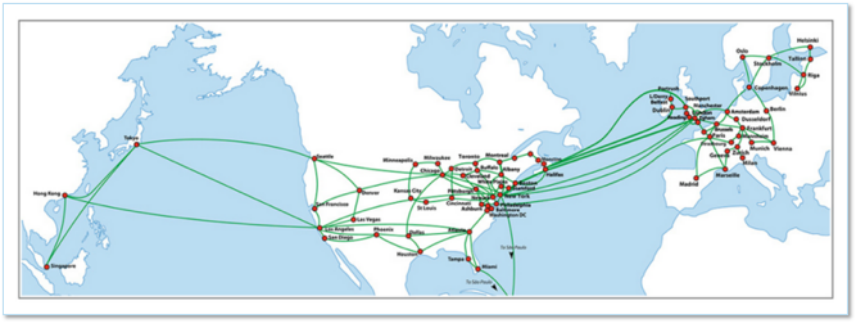
It is relatively easy for an adversary to obfuscate malware code and change the hash values, as these are lower on the pyramid of pain.

Domain names and IP addresses can be dynamically changed easily with little to no cost; again, these are also relatively low on the pyramid of pain.

Tactics, Tools, and Procedures are more complex and expensive for an adversary to change, as these are high on the pyramid of pain.

As a result, security tools that leverage Tactics, Techniques, and Procedures can inflict more pain on an adversary when they are properly integrated into cybersecurity processes.

The Cyber Kill Chain® in Cyber Strategy

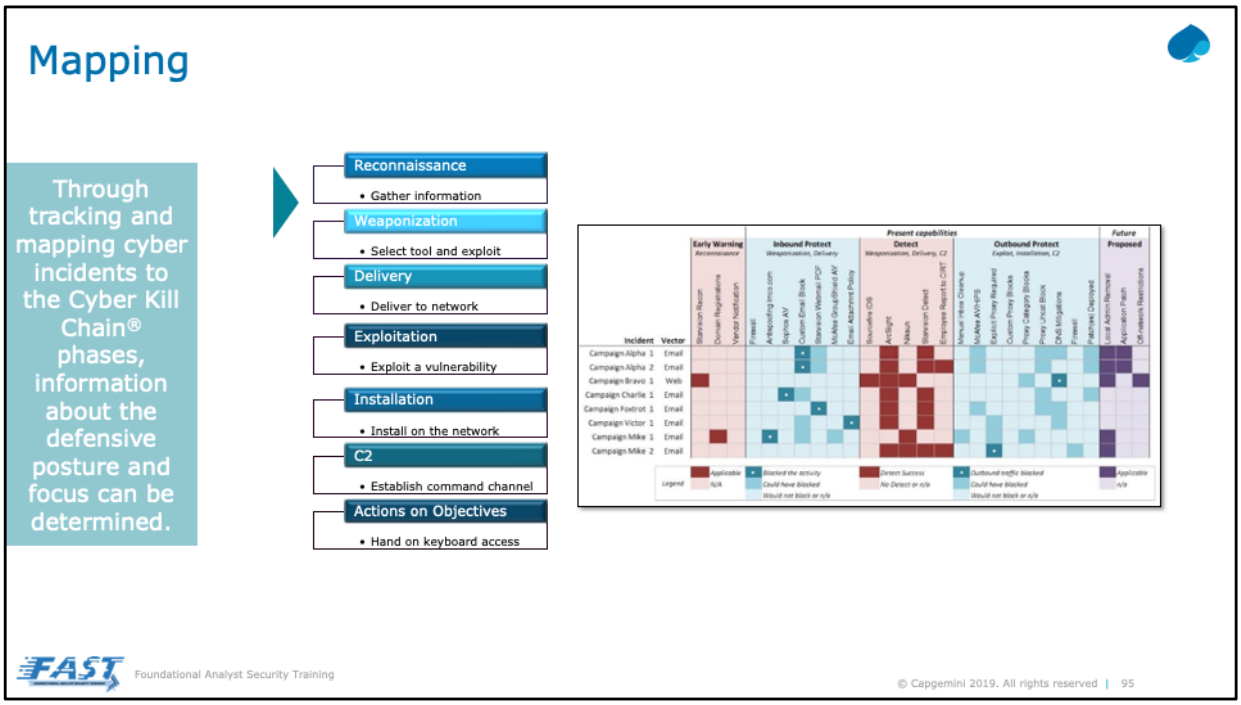


Through tracking and mapping cyber incidents to the Cyber Kill Chain® phases, information about the defensive posture and focus can be determined.

FAST Foundational Analyst Security Training

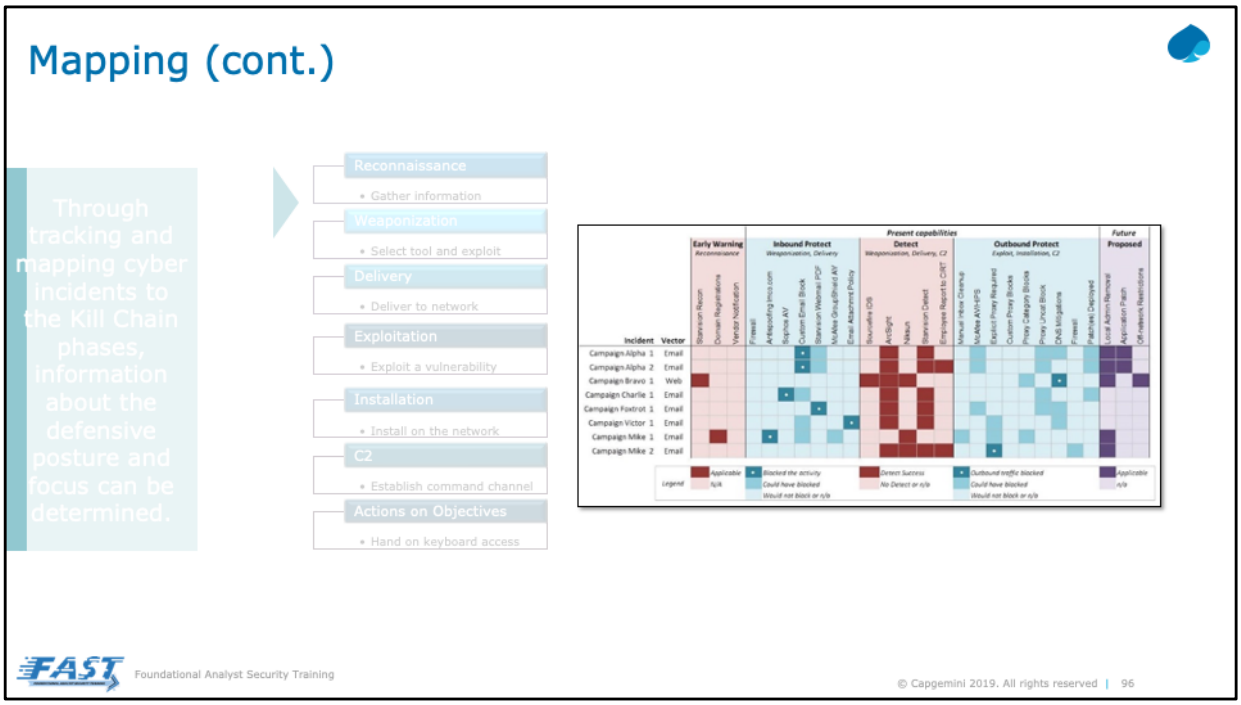
Through tracking and mapping cyber incidents to the Kill Chain phases, information about the defensive posture and focus can be determined.

This information is collected and presented in a Mitigation Scorecard, it aids determining where resources should be applied to strengthen current defenses.



Using the Mitigation Scorecard to target investment to specific threat defenses is a practical output of the scorecard. The Mitigation Scorecard is depicted on the next slide.

Through tracking and mapping cyber incidents to the Kill Chain phases, information about the defensive posture and focus can be determined.



The Mitigation Scorecard is the pinnacle of metrics for an active network defense team.

The Mitigation Scorecard will include campaigns that are of interest to other organizations.

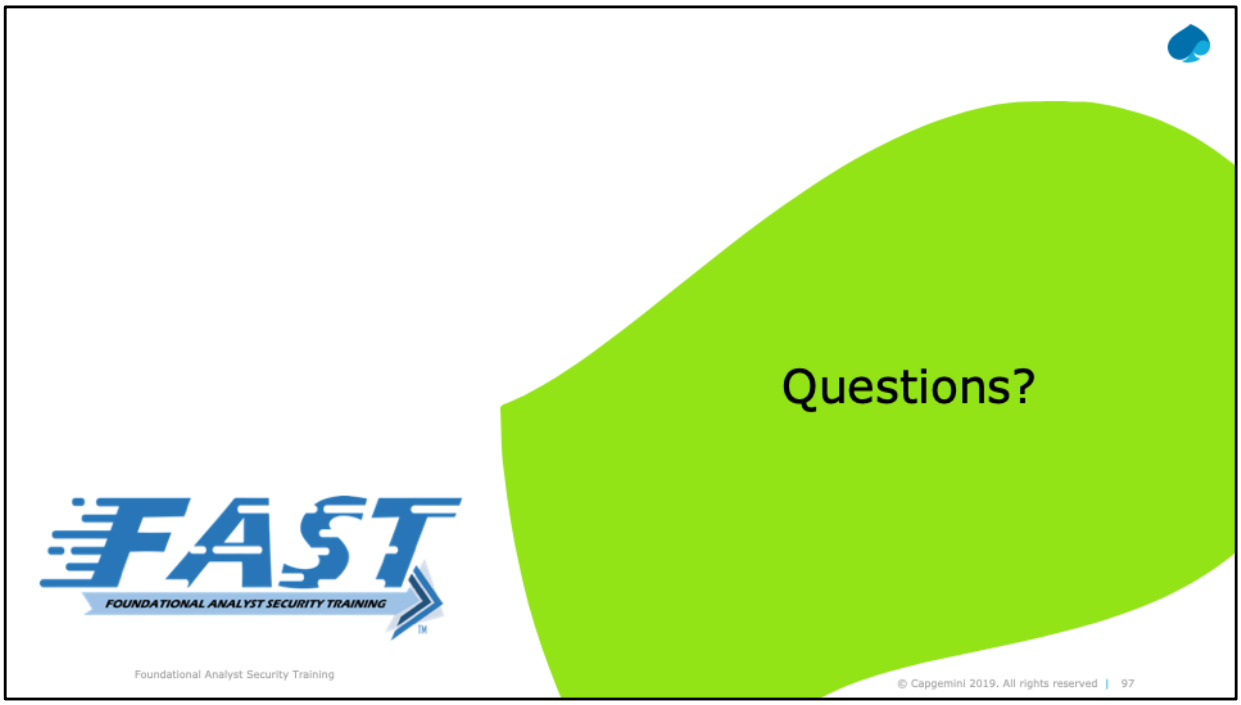
It can include both successful and blocked attacks that were synthesized. It can include successful nuisance attacks, but should really focus on APT's. When studied by upper leadership, this measurement can tell an excellent story for the network defenders.

This information is collected and presented in a Mitigation Scorecard, it aids determining where resources should be applied to build resiliency.

Using the Mitigation Scorecard to target investment to specific threat defenses is a practical output of the scorecard.

Leveraging the Measuring Success Mitigation Scorecard additional defenses can be designed against a known baseline after creating the scorecard.

The ability to pinpoint the specific defensive capabilities that are needed and to quantitatively assess the value of numerous features within tools promotes the continuing measurement of the growth of the SOC.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 97

Content Source:

https://www.schneier.com/blog/archives/2011/08/details_of_the.html
https://www.cs.bu.edu/~goldbe/teaching/HW55812/dimitris.pdf
https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/
https://www.hbarel.com/analysis/itsec/understanding-the-impact-of-the
https://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409

Case Study: Overview

RSA

The New York Times

The RSA Hack: How They Did It

BY RIVA RICHMOND APRIL 2, 2011 3:17 PM 18

The hack last month at RSA Security has been shrouded in mystery.

How did a hacker manage to infiltrate one of the world's top computer-security companies? And could the data that was stolen be used to impair its SecurID products, which are used by 40 million businesses that are trying to keep their own networks safe from intruders?

The division of the EMC Corporation is staying mum about what exactly was stolen from its computer systems, aside from that it was data related to SecurID.

But on Friday RSA shed some light on the nature of the attack. In a blog post titled "Anatomy of an Attack," the company's head of new technologies, Uri Rivner, described a three-stage operation that was similar to several other recent prominent attacks on technology companies, including a 2009 attack on Google that it said originated in China.

Case Study: What is SecurID?

What is RSA: SecurID

- RSA SecurID® is a two-factor authentication protocol developed by for authenticating users to a RSA® network resource.
- The mechanism consists of a "token" with hardware or software that creates an authentication code at fixed intervals, approximately every 60 seconds.

Two-Factor authentication is a type of multifactor authentication that uses a combination of at least two of the following:

- Something you Have
- Something you Are
- Something you Know
- Somewhere you Are

FAST Foundational Analyst Security Training

Two-factor authentication (also known as **2FA**) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of *two* different factors: 1) something they know, 2) something they have, or 3) something they are.

Most students will know what this is already, but make sure you ask….

These are just the companies I have worked for, our have direct knowledge of using SecurID, as you might guess their client list isn't something they throw around.

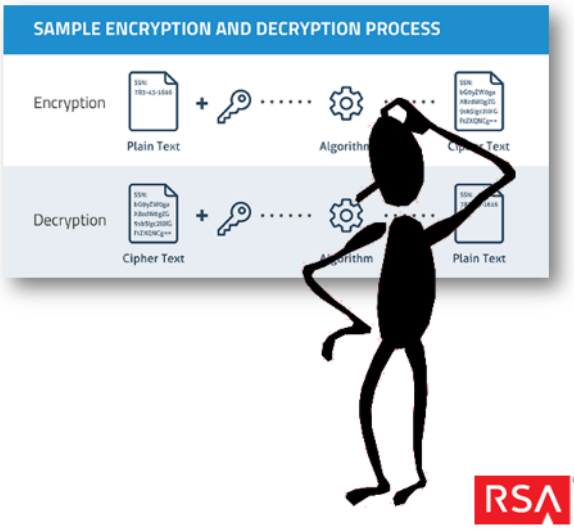
Case Study: Anatomy of an Attack

So is SecurID really secure?

Yes… but, as always, there is a but….

Two assumptions:

- The crypto is secure… cannot be reverse engineered….
- The token itself remains secure… which relies on YOU!



Case Study: Anatomy of an Attack (cont.)

So what was taken?

- Source code or design of the implementation: either design documents or source code of the logic that is carried out by the tokens, and/or by the server component, to determine the one-time password of a token at any given moment

For obvious reasons, RSA SecurID® is being a little closed mouthed about what exactly was taken.

Some things that could have been taken:

- Seed values: those secret keys that allow a server component to be able to determine what one-time password is displayed on each of a set of SecurID tokens at any given moment

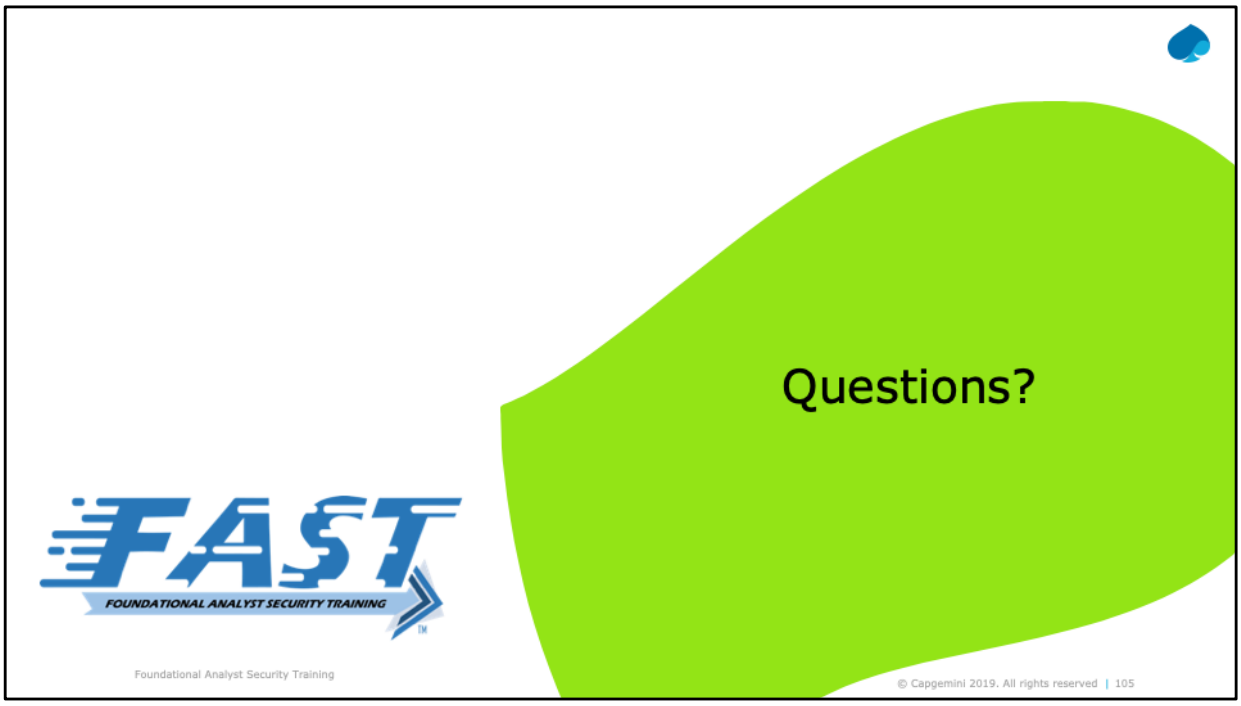
Case Study: RSA Hack – Assignment

Your mission, should you choose to accept it…..

- Use this attack to develop an attack timeline using the Cyber Kill Chain®.
- Log in to the lab environment titled "CASE001: RSA Hack."
- Find several links stored in the browser.
- Use those links (especially the Boston University link).
- Use the information found to develop a timeline of the attack, and document any indicators that may have been discovered.

FAST Foundational Analyst Security Training

The students may not necessarily come back with actual IP addresses, or specific information, just make sure they understand the KINDS of information that the responders would have come back with.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 105

The first section in this module covers an overview of basic network forensics terms and concepts.

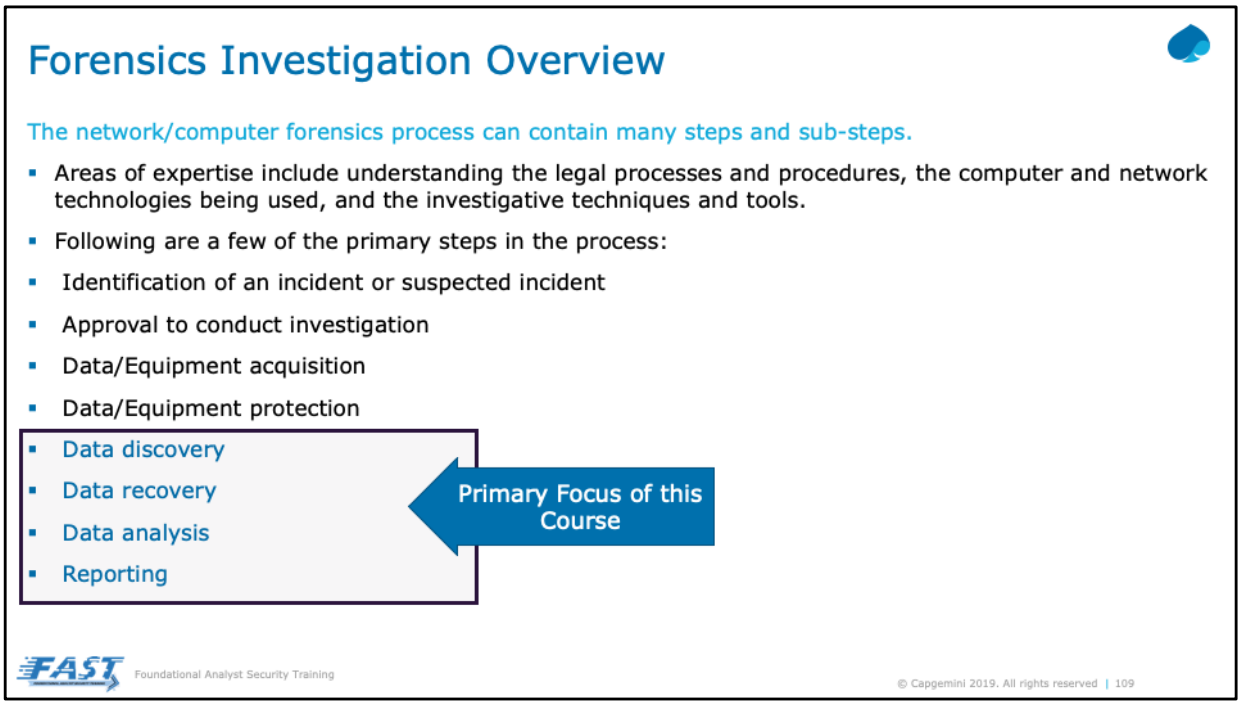
The topics covered in this module include:

- Network Forensics
- Network Vulnerabilities

Topic Learning Objectives

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

- Understand the process for conducting a forensics investigation of computer assets.

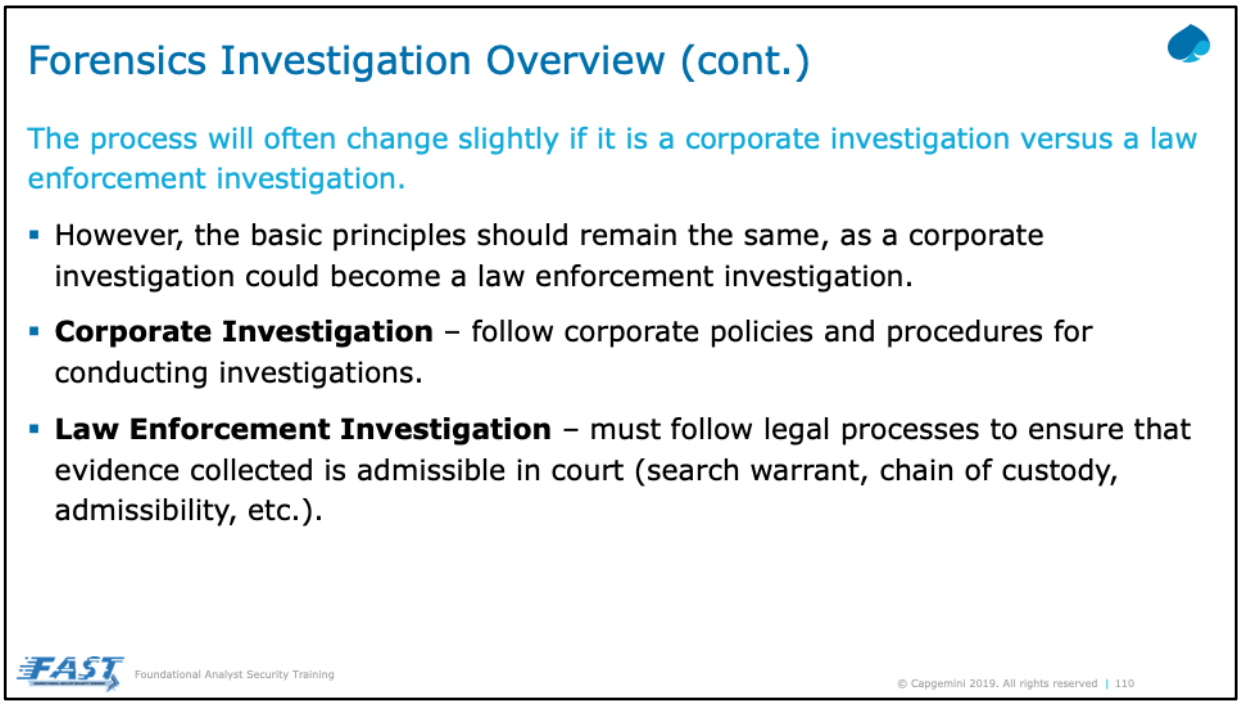


The network/computer forensic process can contain many steps and sub-steps. Likewise, there are many different areas of expertise, including understanding the legal processes and procedures, the computer and network technologies being used, and the investigative techniques and tools.

Following are a few of the primary steps in the process:

- Identification of an incident or suspected incident
- Approval to conduct investigation
- Data / equipment acquisition
- Data / equipment protection
- Data discovery
- Data recovery
- Data analysis
- Reporting

This course focuses primarily on the Data Discovery, Data Recovery, and Data Analysis phases.



The forensic investigative process will often change slightly if it is a corporate investigation versus a law enforcement investigation.

However, the basic principles should remain the same, as a corporate investigation could become a law enforcement investigation.

For Corporate Investigation, you will follow corporate policies and procedures for conducting such investigations. Depending on the maturity of the organization, there should be well defined forensics processes and procedures.

For Law Enforcement Investigation, you must follow legal processes to ensure that evidence collected is admissible in court (such as search warrant, chain of custody, admissibility, etc.).

During this course, we do not address the differences in these processes or procedures, as this courses addresses the Analysis phase / aspect of forensics investigations in much more detail.

Forensics Investigation Overview (cont.)

- Admissibility of evidence
- Rules of evidence
- Search and seizures typically require a search warrant.
- Criminal trials are often preceded by a suppression hearing.
- Chain-of-custody procedures

FAST Foundational Analyst Security Training

The admissibility of evidence can become an issue in both corporate investigations and law enforcement investigations.

Admissible evidence is any type of proof legally represented at trial and allowed by the judge. For evidence to be admissible, evidence must be authenticated with sufficient proof of authenticity.

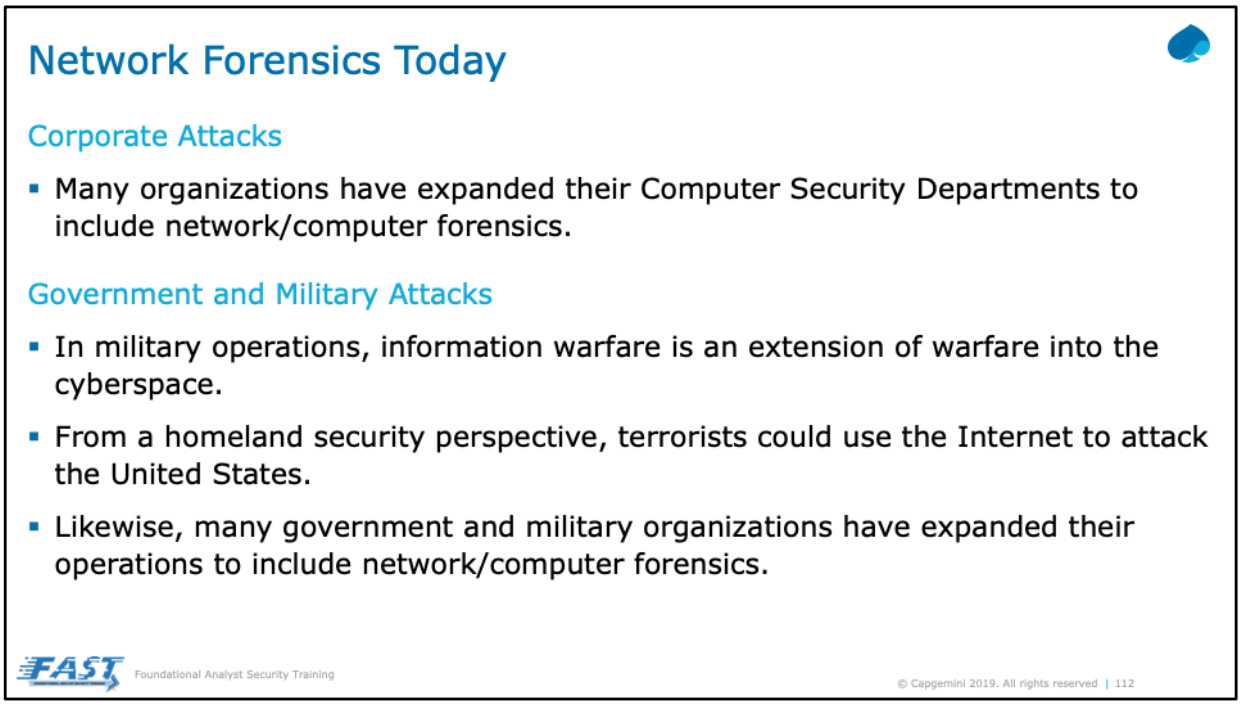
Rules of evidence are rules by which a court determines that evidence is admissible in court.

Search and seizures typically require a search warrant (requiring probable cause).

Discovery is the process of gathering information in preparation for trial, legal investigation, or administrative action.

Criminal trials are often preceded by a suppression hearing, where the admissibility or suppression of evidence is heard and determined. Evidence seized might be suppressed if the evidence is seized without having followed the proper procedures.

Additionally, after data/equipment collection, chain of custody procedures are very important, where you must keep a record or evidence log, keep record of items being released to others, restrict access to evidence, and preserve the chain of custody. Additionally, forensic investigations must be conducted on a mirrored image copy.

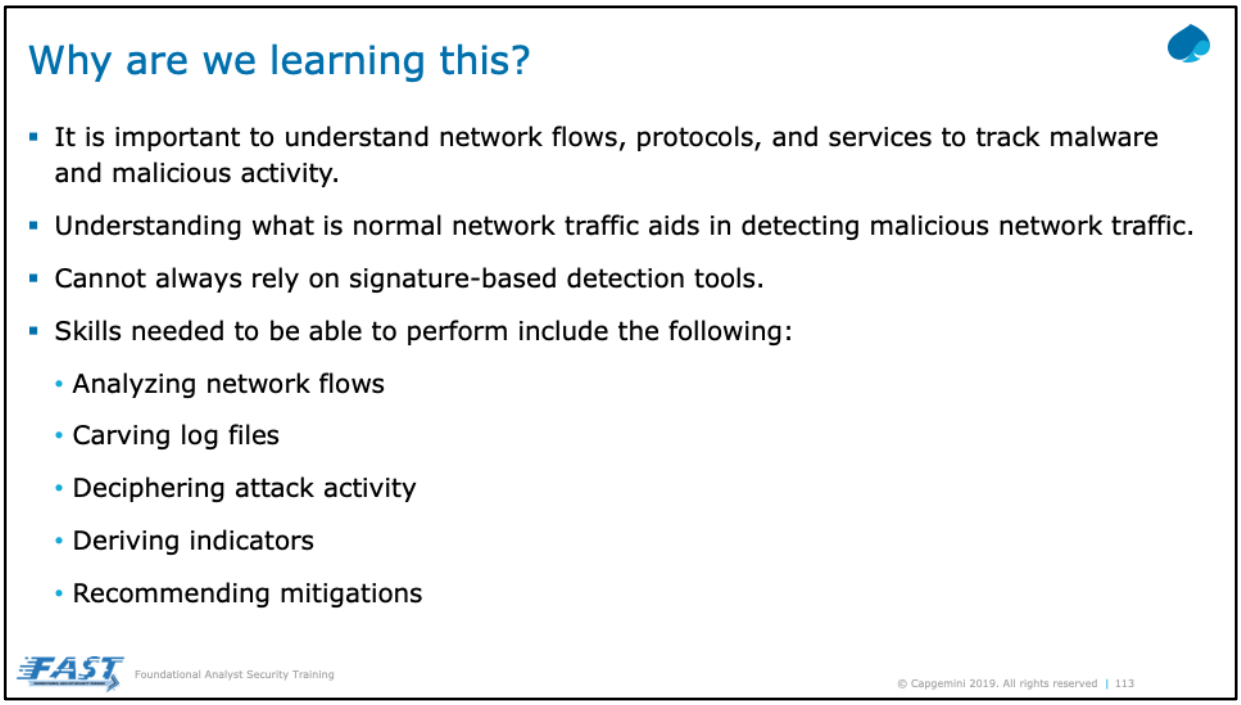


As seen over the years, there are many examples of attacks against corporate systems, as they often focus on financial motives, such as gathering credit card information

- Many organizations have expended their computer security departments to include network/computer forensics

However, the attacks expand into all areas, including government and military operations. The government has the responsibility of protecting the nation's critical infrastructure is a national priority; however, that protection requires cooperation and collaboration from the public sector as well

- In military operations, information warfare is an extension of warfare into the cyberspace
- From a homeland security perspective, terrorists could use the Internet to attack the United States
- Likewise, many government and military organizations have expended their operations to include network/computer forensics



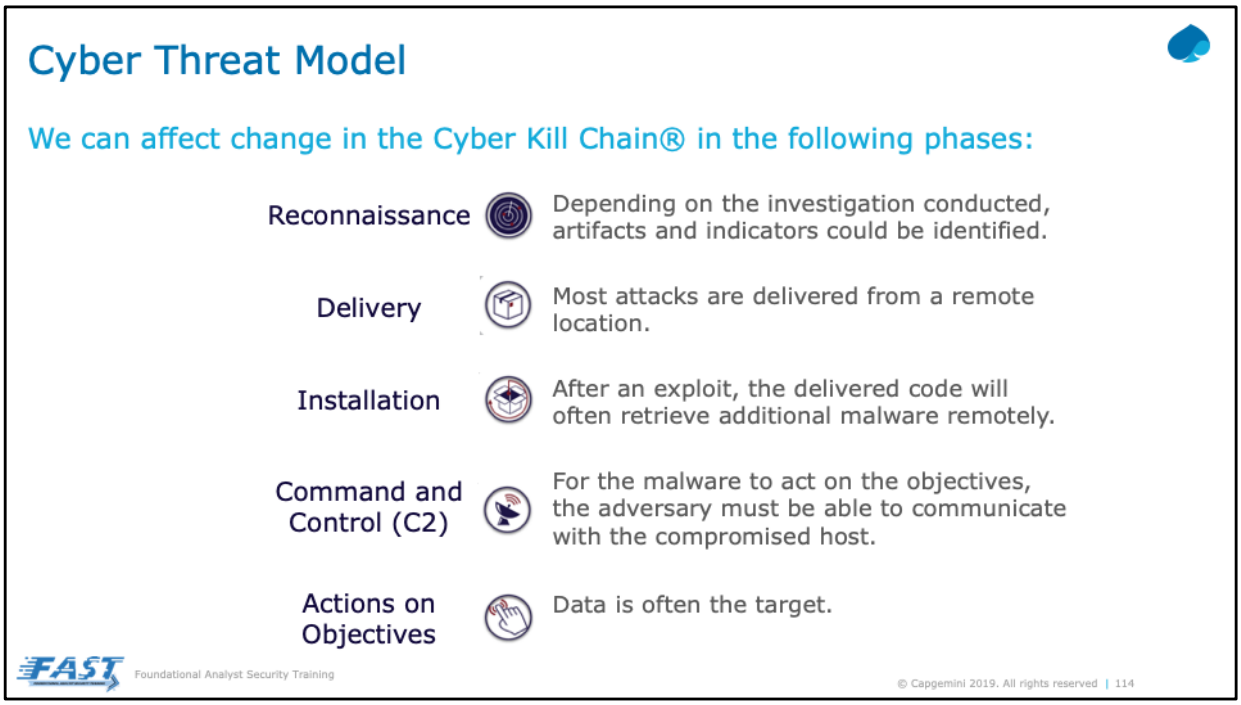
It is important to understand network flows, protocols, and services in order to track malware and malicious activity. As mentioned previously, forensics analysis requires a multi-disciplinary approach and skill set.

Understanding what is normal network traffic aids in detecting malicious network traffic.

Likewise, you cannot always rely on signature-based detection tools.

There are many skills you will need to be able to perform including:

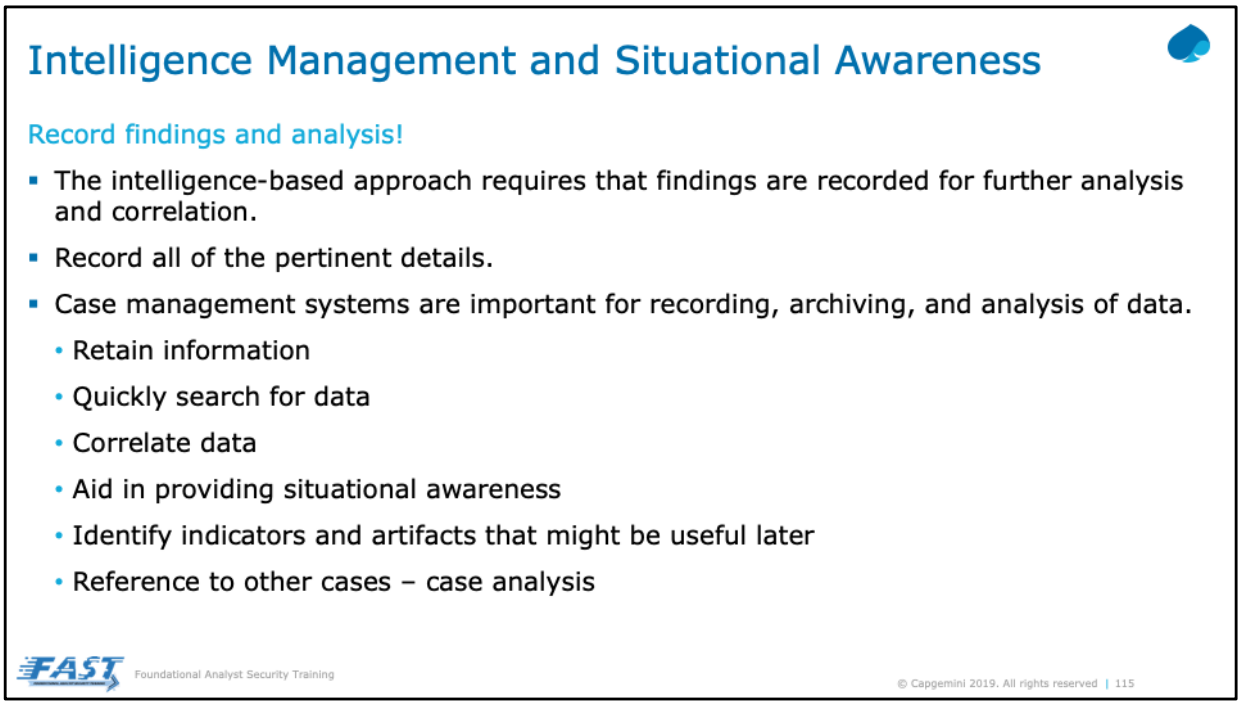
- Analyzing network flows
- Carving log files
- Deciphering attack activity
- Deriving indicators
- Recommending mitigations



The Cyber Kill Chain provides a framework for tracking and attack and the associated indicators.

The Cyber Kill Chain phases are:

- Recon: Depending on the investigation conducted, artifacts and indicators could be identified
- Delivery: Most attacks are delivered from a remote location
- Installation: After an exploit, the delivered code will often retrieve additional malware remotely
- Command and Control (C2): For the malware to act on the objectives, the adversary must be able to communicate with the compromised host
- Actions on Objectives: Data is often the target



For the current case or incident and for broader Case Analysis, intelligence management and situational awareness are very important to being proactive and adaptive.

You need to record your findings and analysis. The intelligence based approach requires that findings are recorded for further analysis and correlation.

Thus, you should record all of the pertinent details of each incident and indicator.

Case management systems are important for recording, archiving, and analysis of data, they enable you to:

- Retain information
- Quickly search for data
- Correlate data
- Aid in providing situational awareness
- Identify indicators and artifacts that might be useful later
- Reference to other cases – Case Analysis


Incident Response
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Capgemini
Foundational Analyst Security Training

Agenda

SECURITY INCIDENTS | INCIDENT RESPONSE

Malware and Analysis

- Traditional Malware
- File-less Malware
- Malware Analysis

Topic Learning Objectives

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

- Describe what incident response is and why it is essential to any organization.

What is a Security Incident?

A security incident is an imminent threat or attack on a host or network security policies, acceptable use, or standardized security practices.

FAST Foundational Analyst Security Training

Instructor Notes:

Because network threats evolve and grow quickly in todays fast paced world, it is essential that we have the capability to respond to these threats quickly.

We cannot have a process for each and every threat type, what we do have is a standardized process laid down in the NIST SP800-61.

It should be noted, that not every organization responds in the same way, and the processes we discuss in this class are generalized, always follow SIC team guidance for cybersecurity incident response in your organizational SOC.

Why Is Incident Response Important?

The Federal Information Security Modernization Act (FISMA) requires Federal agencies to establish incident response capabilities.

FAST Foundational Analyst Security Training

Instructor Notes:

Each Federal civilian agency must designate a primary and secondary point of contact (POC) with US-CERT and report all incidents consistent with the agency's incident response policy. Each agency is responsible for determining how to fulfill these requirements.

While these policies don't generally apply to commercial entities, some organizations that do work with government agencies may face some requirements. However, it is generally held that developing incident response capabilities is a best practice in the industry.

Incident Response Capabilities

Establishing incident response capabilities can consist of many different components depending the network.

FAST Foundational Analyst Security Training

Instructor Notes:

- Establishing an incident response capability should include the following actions: Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide Staffing and training the incident response team

Common Threats

As discussed, there are many threats to today's networks; however, with preparation for some common threat vectors, networks can be defended effectively.

FAST Foundational Analyst Security Training

Instructor Notes:

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. This publication defines several types of incidents, based on common attack vectors; these categories are not intended to provide definitive classification for incidents, but rather to be used as a basis for defining more specific handling procedures. Different types of incidents merit different response strategies. The attack vectors are:

External/Removable Media: An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.

Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.

Web: An attack executed from a website or web-based application.

Email: An attack executed via an email message or attachment.

Improper Usage: Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.

Loss or Theft of Equipment: The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.

Other: An attack that does not fit into any of the other categories.

Incident Response Guidance

- Secure Networks
- Share Information
- Prepare to React
- Detect and Analyze
- Create Written Guidance
- Use Lessons Learned

FAST Foundational Analyst Security Training

Instructor Notes:

Organizations should reduce the frequency of incidents by effectively securing networks, systems, and applications. Preventing problems is often less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important complement to an incident response capability. If security controls are insufficient, high volumes of incidents may occur.

Organizations should document their guidelines for interactions with other organizations regarding incidents. During incident handling, the organization will need to communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and victim organizations

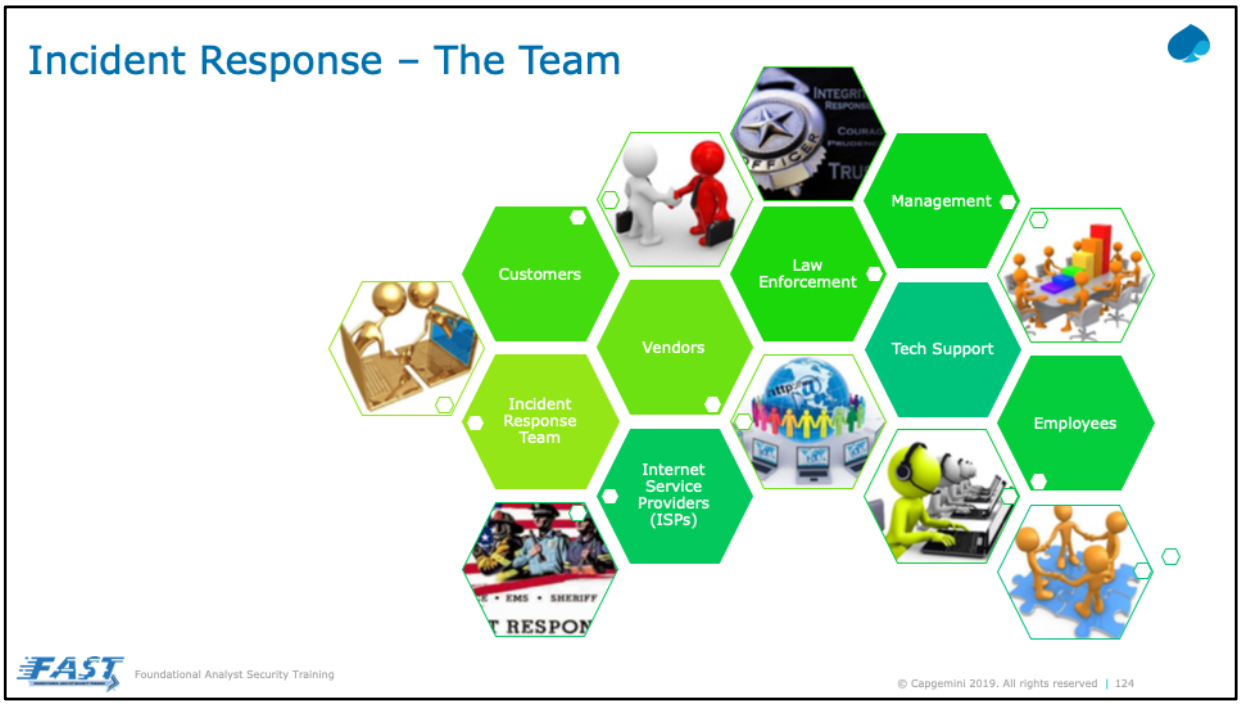
Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.

Organizations should emphasize the importance of incident detection and analysis throughout the organization. In an organization, millions of possible signs of incidents may occur each day, recorded mainly by logging and computer security software.

Automation is needed to perform an initial analysis of the data and select events of interest for human review

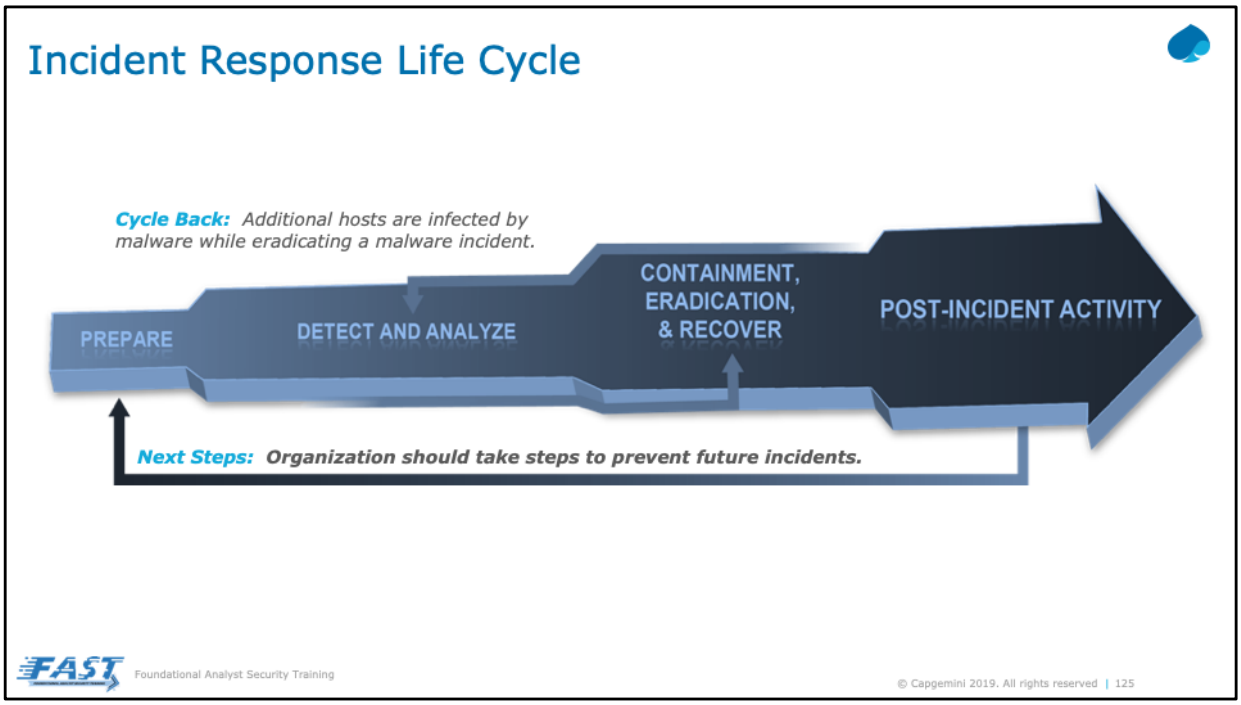
Organizations should create written guidelines for prioritizing incidents. Prioritizing the handling of individual incidents is a critical decision point in the incident response process. Effective information sharing can help an organization identify situations that are of greater severity and demand immediate attention

Organizations should use the lessons learned process to gain value from incidents. After a major incident has been handled, the organization should hold a lessons learned meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices



Instructor Notes:

An incident handling team doesn't work in a vacuum, they interact with many other teams of individuals including other incident responders at information sharing partners, customers, vendors, hardware and software support teams, law enforcement, employees who may be reported the incident, ISP's and of course the C2 Suite (management).



Instructor Notes:

Prepare: The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources.

During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented.

Detection: Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it.

Containment: During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident.

Post Incident: After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

Prepare

Most Incident Response Methodologies put the emphasis on preparing or preventing attacks.

A SOC analyst is instrumental in preventing incidents; however, they will still occur.

Be prepared to transition to response.

FAST Foundational Analyst Security Training

Instructor Notes:

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. This section provides basic advice on preparing to handle incidents and on preventing incidents.

Detect and Analyze

Incident detection is critical, and analysts play a large part in this phase of response.

Challenges in incident detection include the following:

- Various Attack Methods
- Volume of Information
- Analyst Knowledge

FAST Foundational Analyst Security Training

Instructor Notes:

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

What makes this so challenging is a combination of three factors:

- Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.

- The volume of potential signs of incidents is typically high—for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day. (See Section 3.2.4 for information on analyzing such alerts.)

- Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

Containment, Eradication, and Recover

Containment is important before an incident overwhelms resources or increases damage.

This will typically happen after the incident moves to the Incident Response Team; however, the incident response will likely move back and forth into the detection phase.

FAST Foundational Analyst Security Training

Instructor Notes:

Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions).

Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making

Post-Incident Activity

One of the most important parts of incident response is also the most often omitted: learning and improving.

Each Incident Response Team should evolve to reflect new threats, improved technology, and lessons learned.

FAST Foundational Analyst Security Training

Instructor Notes:

Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself.

Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked.

The meeting should be held within several days of the end of the incident.

Ask Questions:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?

- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?

Archiving the Incident

After an incident, any records of the attack should be archived to provide for subsequent actions such as:

- Prosecution
- Data Retention
- Cost

FAST Foundational Analyst Security Training

Instructor Notes:

Organizations should establish policy for how long evidence from an incident should be retained. Most organizations choose to retain all evidence for months or years after the incident ends. The following factors should be considered during the policy creation:

Prosecution - If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished.

Data Retention - Most organizations have data retention policies that state how long certain types of data may be kept. For example, an organization may state that email messages should be retained for only 180 days. If a disk image contains thousands of emails, the organization may not want the image to be kept for more than 180 days unless it is absolutely necessary.

Cost - Original hardware (e.g., hard drives, compromised systems) that is stored as evidence, as well as hard drives and removable media that are used to hold disk images, are generally individually inexpensive. However, if an organization stores many such components for years, the cost can be substantial. The organization also must retain functional computers that can use the stored hardware and media.

Content Source:

CASE002: Incident Response

Please open CASE002

30 minutes to read/30 minutes to discuss

There are three Portable Document Format (PDF) documents on the desktop.

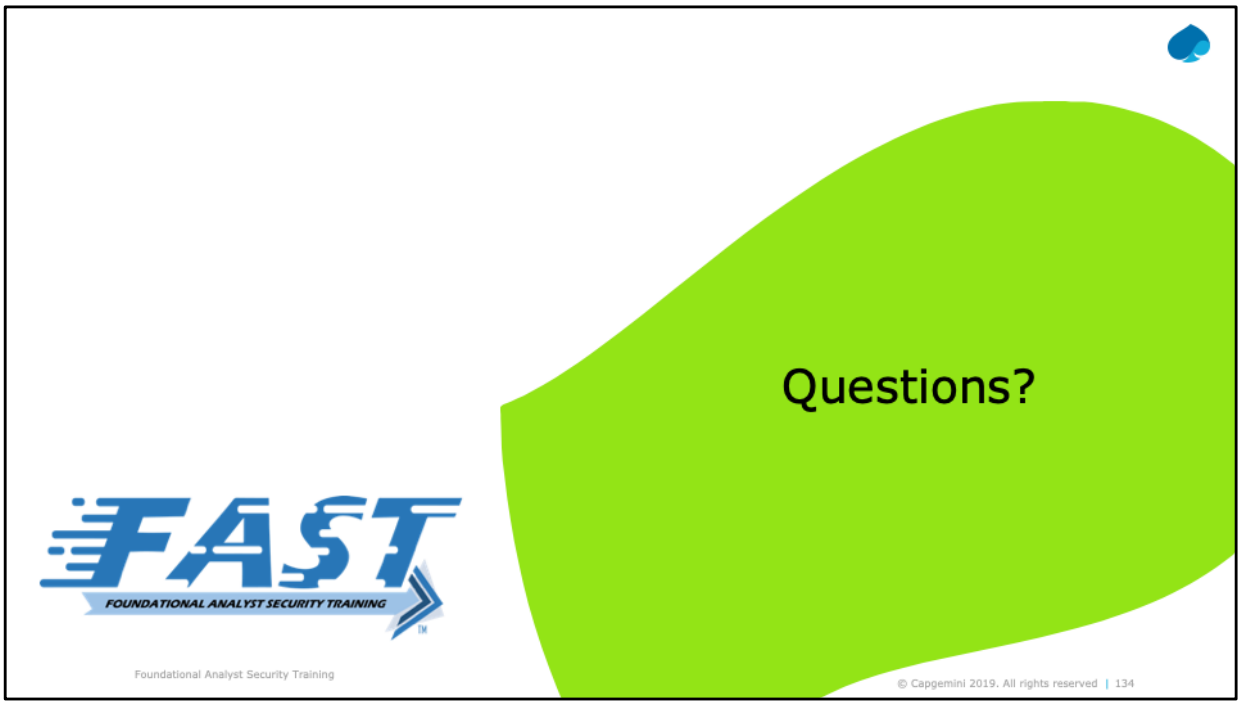
Take some time to familiarize yourself with the case studies.

CASE002: Incident Response (cont.)

Please open CASE002.

30 minutes to read/30 minutes to discuss

Upon completion of your review, we will discuss incident response and how effective response and analysis might have been conducted at each organization.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 134


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