Capgemini

© Capgemini 2019. All rights reserved

Module 4 – Networking

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

Introduction to Threat Intelligence

Capgemini

Agenda

SOC Organization | Maturity | Security Intelligence | 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.

© Capgemini 2019. All rights reserved

Computer Incident Response Team (SIC) Evolution

Network Operations Center (NOC)

- Typically staffed by network and infrastructure engineers and system administrators
- Their mission is not to respond to security issues; however, they may be one of the first aware of them and critical to response efforts (such as a Distributed Denial of Service [DDoS]).

- Typically staffed by network and infrastructure engineers and system administrators
- Their mission is not to respond to security issues; however, they may be one of the first aware of them and critical to response efforts (such as a Distributed Denial of Service [DDoS]).

© Capgemini 2019. All rights reserved

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

© Capgemini 2019. All rights reserved

Computer Incident Response Team (SOC) Evolution

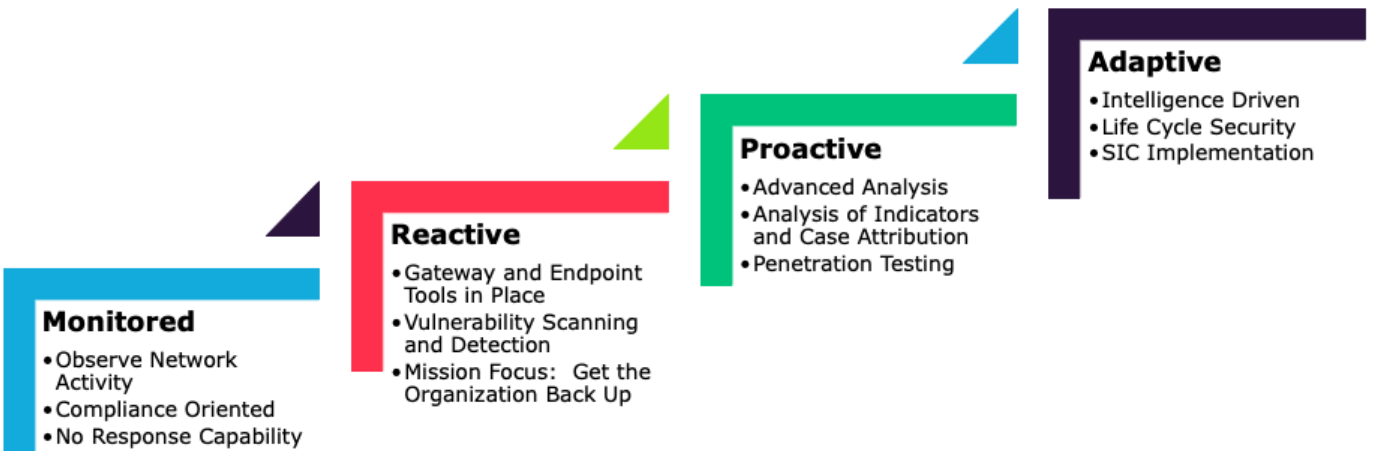
Security Intelligence Center (SIC)

- Has the mission to respond proactively (and adaptively) to and protect the network infrastructure from cyber threats
- Typically staffed with cyber intelligence analysts
- Commonly includes custom tool development, including intelligence management platforms
- Their incident response challenge is that the learning curve is often very steep; and there is often a restricted availability of situational awareness, organizational communications, and data management

© Capgemini 2019. All rights reserved

Organizational Maturity and Security Postures

Organizational Maturity



© Capgemini 2019. All rights reserved

Organizational Maturity and Security Postures (cont.)

Maturity Models

- 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

© Capgemini 2019. All rights reserved

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

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

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

- Using precise measurements, management can effectively control the software development effort.
- In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications.

© Capgemini 2019. All rights reserved

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

© Capgemini 2019. All rights reserved

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

© Capgemini 2019. All rights reserved

Security Intelligence (cont.)

Security Intelligence IS the following:

- A multi-disciplinary organizational element that builds on other foundational security elements and knowledge of the organizational infrastructure, capabilities, strengths, and weaknesses
- Focused on the threats and associated indicators
- Very focused on situational awareness, including the technologies (such as sensors, logs, and indicators) and people (collaboration and knowledge sharing)

© Capgemini 2019. All rights reserved

Security Intelligence (cont.)

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

Security Intelligence IS the following:

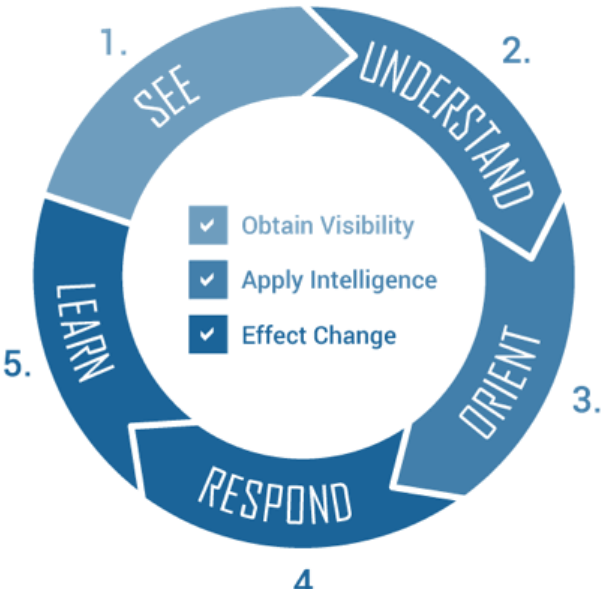
- Both responsive and predictive
- Focused on much more than just stopping the attack, as it looks forward and backward to determine what happened, why it happened, and predictive of what could have happened

© Capgemini 2019. All rights reserved

Unified Enterprise Defense (UED)

UED Life Cycle

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

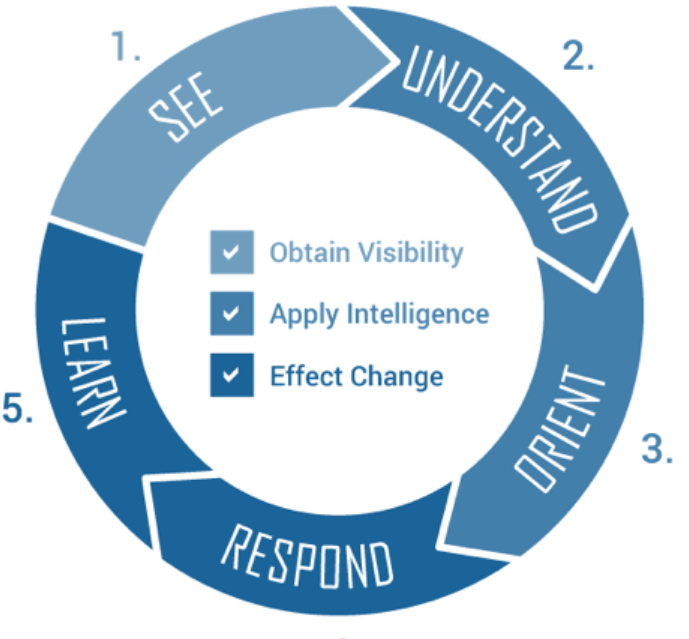


© Capgemini 2019. All rights reserved

Unified Enterprise Defense (UED) (cont.)

UED Life Cycle

1. SEE: Monitor cyber activity.
2. UNDERSTAND: Identify and isolate advanced cyber threat activity from normal network or system traffic.
3. ORIENT: Determine a course of action.
4. RESPOND: Take action to implement defenses and execute mitigations.
5. LEARN: Build new, actionable intelligence.



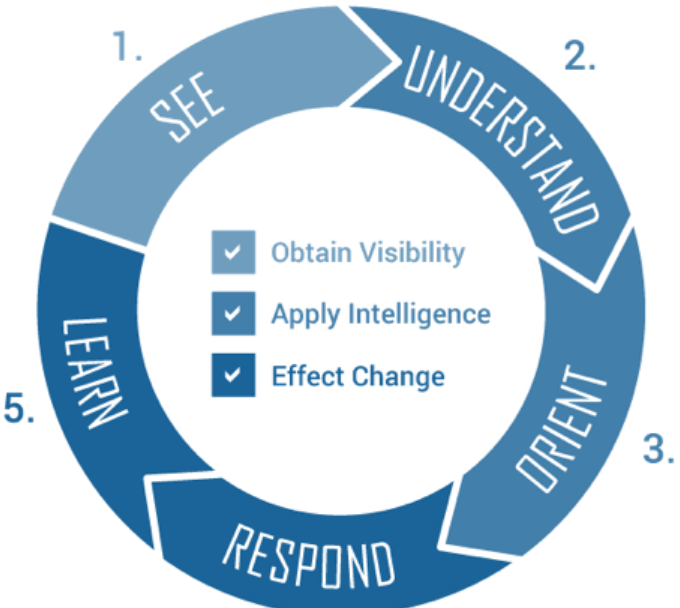
© Capgemini 2019. All rights reserved

Unified Enterprise Defense (UED) (cont.)

UED Life Cycle

An effective organization will establish support throughout the following:

- Information Security Team/Mission
- Leadership Support
- Collaboration
- Culture
- A SIC has the core responsibility to develop visibility into systems, apply intelligence, and effect change within the organization.
- Essentially enabling the security of a company to be SIC intelligence driven



© Capgemini 2019. All rights reserved

Security Intelligence

Security Intelligence Components are as follows:

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

© Capgemini 2019. All rights reserved

Security Intelligence (cont.)

Security Intelligence Elements are as follows:

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

© Capgemini 2019. All rights reserved

Security Intelligence (cont.)

A Security Intelligence Team is multi-disciplinary, and it is typically comprised of personnel with many different skills such as the following:

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

Note: The focus must remain on the collaborative efforts of the team to accomplish the overall mission.

© Capgemini 2019. All rights reserved

Threats

Tactics, Techniques, and Procedures
Threat Elements

- Intent
- Opportunity
- Capability

Note: This is often expressed as TTPs.

- The security intelligence process → addresses threats that are targeted, advanced, and persistent in nature.

© Capgemini 2019. All rights reserved

Threats (cont.)

Targeted Threats

Intent: Defined objectives, typically specific to a person, product, program, technology, or business goal

Opportunity: Adversary develops tools, capabilities, and supporting infrastructure specifically aimed at the particular target.

Capability: An attack will typically coincide with target or infrastructure, technology, and human vulnerabilities.

© Capgemini 2019. All rights reserved

Threats (cont.)

Advanced Threats

Intent: Often seeking significant goals that can range from espionage, sabotage, theft, or denial of operations; advanced threats go beyond uncoordinated smash-and-grab threats.

Opportunity: Adversary often demonstrates patience, coordination, and timing.

Capability: Adversary often employs highly complex attacks for exploiting and compromising target systems; the adversary will then maintain access and conduct further exploitation.

© Capgemini 2019. All rights reserved

Threats (cont.)

Persistent Threats

Intent: Adversary continues attack until they gain and maintain access, extract intelligence, and hide activity.

Opportunity: Adversary has almost unlimited opportunity to act on intentions, as long as they are able to maintain access without detection.

Capability: Malware is designed to provide Command and Control (C2), lateral movement, and data exfiltration.

© Capgemini 2019. All rights reserved

Advanced Persistent Threats (APTs)

APT characteristics are as follows:

- Targeted, long-term attacks
- Conducted utilizing technical means and social engineering
- Well coordinated
- Robust infrastructure of support
- High-level, campaign-scale intrusions
- Target valuable data

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

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

© Capgemini 2019. All rights reserved

Questions?

© Capgemini 2019. All rights reserved

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).

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

The Cyber Kill Chain® (cont.)

What it is…

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

© Capgemini 2019. All rights reserved

The Cyber Kill Chain® (cont.)

What it is…

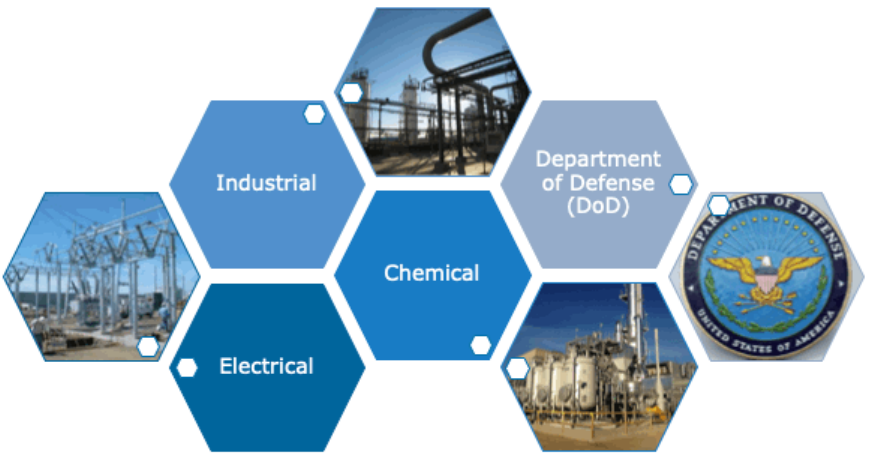
The Cyber Kill Chain® framework tracks the phases that an attacker must complete successfully to achieve their desired objectives.

© Capgemini 2019. All rights reserved

The Cyber Kill Chain® (cont.)

© Capgemini 2019. All rights reserved

The Cyber Kill Chain® (cont.)



© Capgemini 2019. All rights reserved

What it is…

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

© Capgemini 2019. All rights reserved

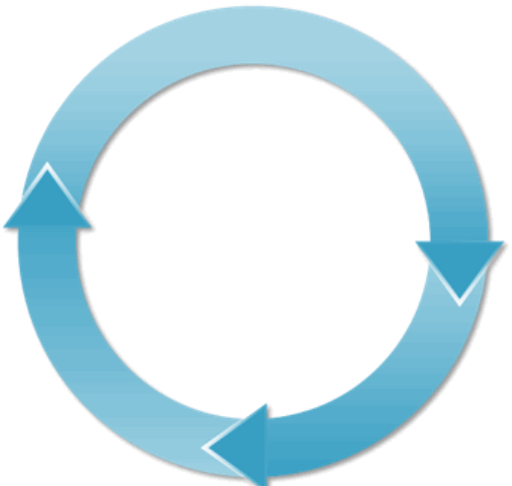
What it is… (cont.)

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.

© Capgemini 2019. All rights reserved

What it is… (cont.)

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

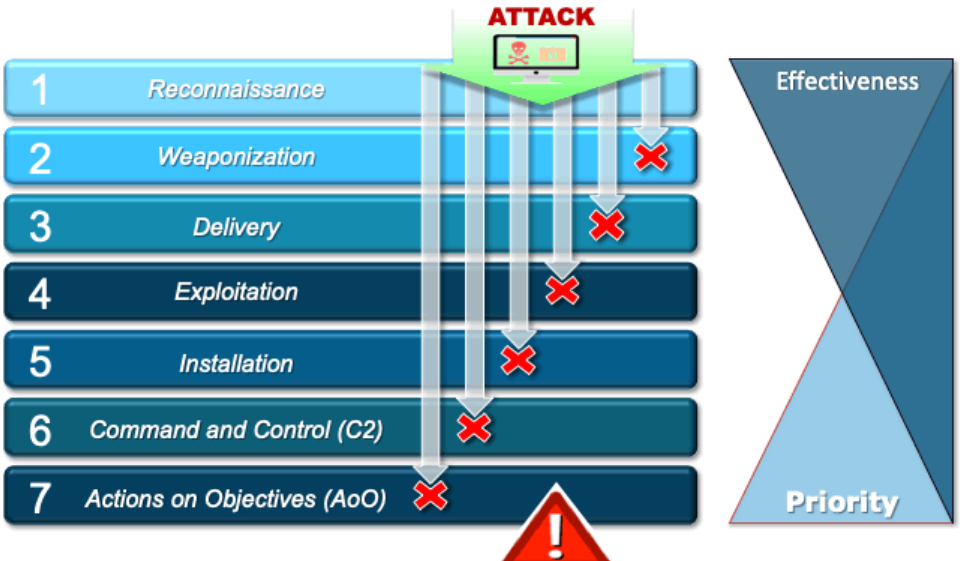


© Capgemini 2019. All rights reserved

What it is… (cont.)

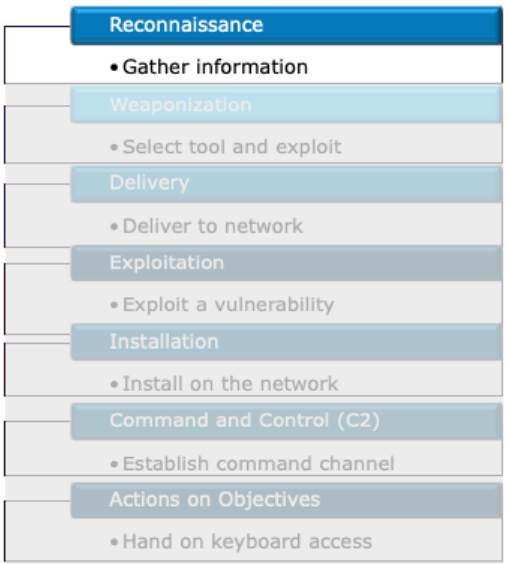
© Capgemini 2019. All rights reserved

Phases of the Cyber Kill Chain®



© Capgemini 2019. All rights reserved

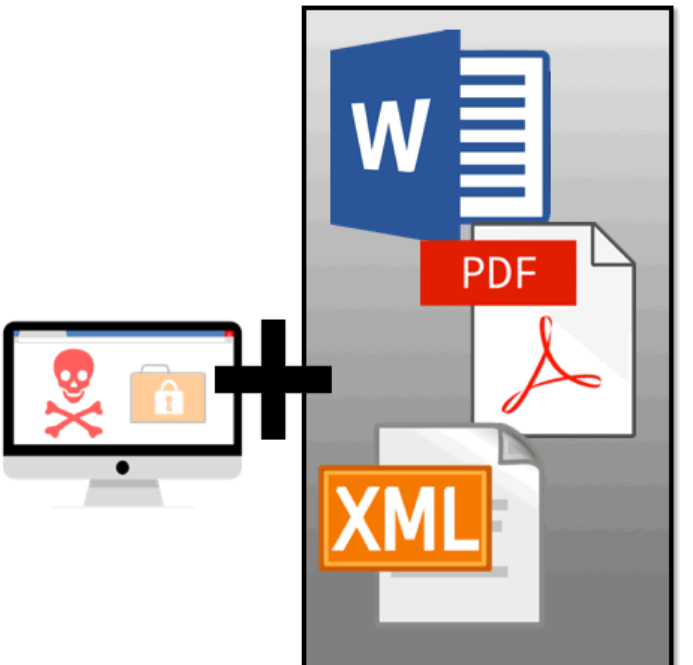
Reconnaissance



© Capgemini 2019. All rights reserved

Weaponization

- Reconnaissance
  - Gather information
- **Weaponization**
  - **Select tool and exploit**
- Delivery
  - Deliver to network
- Exploitation
  - Exploit a vulnerability
- Installation
  - Install on the network
- Command and Control (C2)
  - Establish command channel
- Actions on Objectives
  - Hand on keyboard access



© Capgemini 2019. All rights reserved

Delivery

- Reconnaissance
  - Gather information
- Weaponization
  - Select tool and exploit
- **Delivery**
  - **Deliver to network**
- Exploitation
  - Exploit a vulnerability
- Installation
  - Install on the network
- Command and Control (C2)
  - Establish command channel
- Actions on Objectives
  - Hand on keyboard access

© Capgemini 2019. All rights reserved

Exploitation

- Reconnaissance
  - Gather information
- Weaponization
  - Select tool and exploit
- Delivery
  - Deliver to network
- **Exploitation**
  - **Exploit a vulnerability**
- Installation
  - Install on the network
- Command and Control (C2)
  - Establish command channel
- Actions on Objectives
  - Hand on keyboard access

© Capgemini 2019. All rights reserved

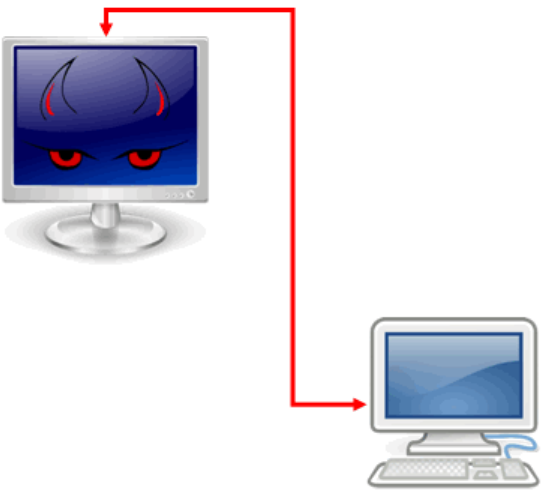
Installation

- Reconnaissance
  - Gather information
- Weaponization
  - Select tool and exploit
- Delivery
  - Deliver to network
- Exploitation
  - Exploit a vulnerability
- **Installation**
  - **Install on the network**
- Command and Control (C2)
  - Establish command channel
- Actions on Objectives
  - Hand on keyboard access

© Capgemini 2019. All rights reserved

Command and Control (C2)

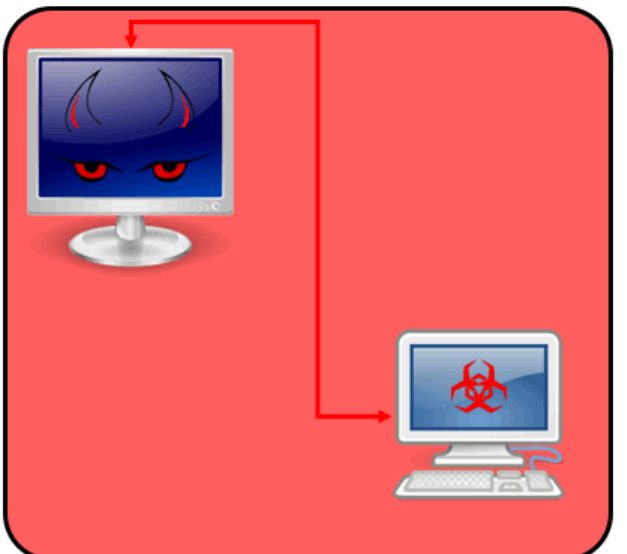
- Reconnaissance
  - Gather information
- Weaponization
  - Select tool and exploit
- Delivery
  - Deliver to network
- Exploitation
  - Exploit a vulnerability
- Installation
  - Install on the network
- **Command and Control (C2)**
  - **Establish command channel**
- Actions on Objectives
  - Hand on keyboard access



© Capgemini 2019. All rights reserved

Actions on Objectives (AoO)

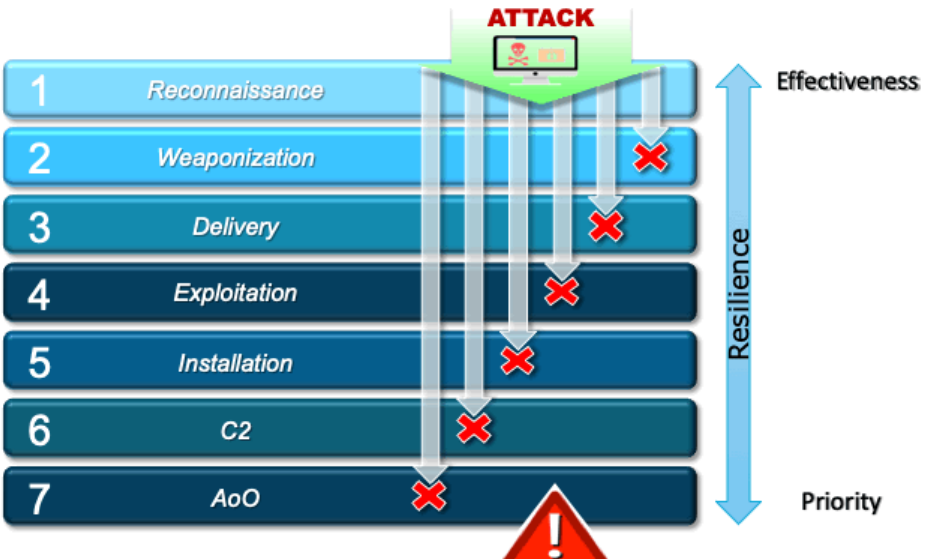
- **Reconnaissance**
  - Gather information
- **Weaponization**
  - Select tool and exploit
- **Delivery**
  - Deliver to network
- **Exploitation**
  - Exploit a vulnerability
- **Installation**
  - Install on the network
- **Command and Control (C2)**
  - Establish command channel
- **Actions on Objectives**
  - Hand on keyboard access



© Capgemini 2019. All rights reserved

Resilience

With each event in an attack, we build the resiliency of the Cyber Program.



© Capgemini 2019. All rights reserved

Questions?

© Capgemini 2019. All rights reserved

Threat Indicators

Capgemini

Agenda

Types of Threat Indicators | Analysis of Threat Indicators

Topic Learning Objectives

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

- Identify the different types of threat indicators.

- Analyze threat indicators, including how they relate to a case analysis.

© Capgemini 2019. All rights reserved

Types of Indicators

Atomic

An Atomic indicator is one that cannot be broken down into smaller parts without losing the meaning within the context of an intrusion.

- Examples:
  - IP addresses
  - Email addresses

Computed

A Computed indicator is derived from other data.

- Examples:
  - File hashes
  - RegExes
  - Yara

Behavioral

A Behavioral indicator combines Computed and Atomic indicators.

- Examples:
  - Source IP address range (to target users from a particular department)
  - Email subject contains targeted text.

© Capgemini 2019. All rights reserved

Types of Indicators (cont.)

External

- They are provided by an external source.
- Information from an external source needs to be heavily vetted.
- They often involve a circle of trust with industry partners.
- These can be High Confident indicators, depending on source.

Industry sharing portals

- Analyst might share details of the indicators and the associated analysis.

© Capgemini 2019. All rights reserved

Types of Indicators (cont.)

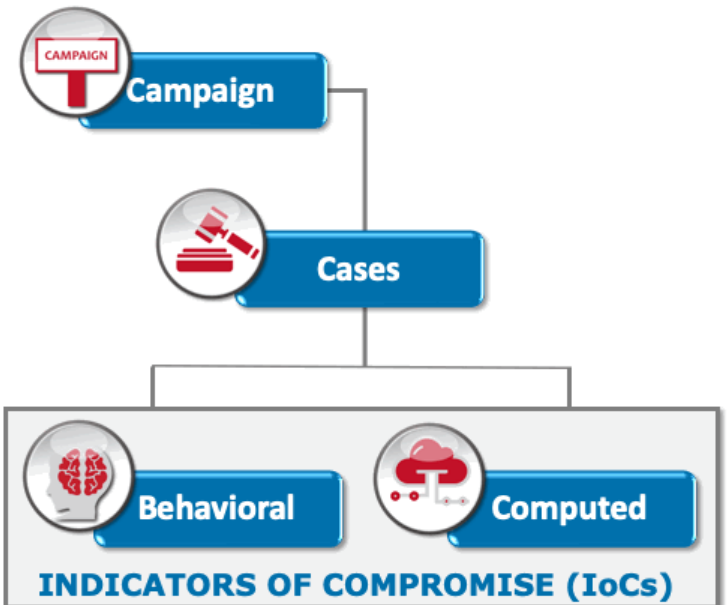
Internal

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

© Capgemini 2019. All rights reserved

Analysis of Threat Indicators

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



© Capgemini 2019. All rights reserved

Analysis of Threat Indicators (cont.)

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

© Capgemini 2019. All rights reserved

Analysis of Threat Indicators (cont.)

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

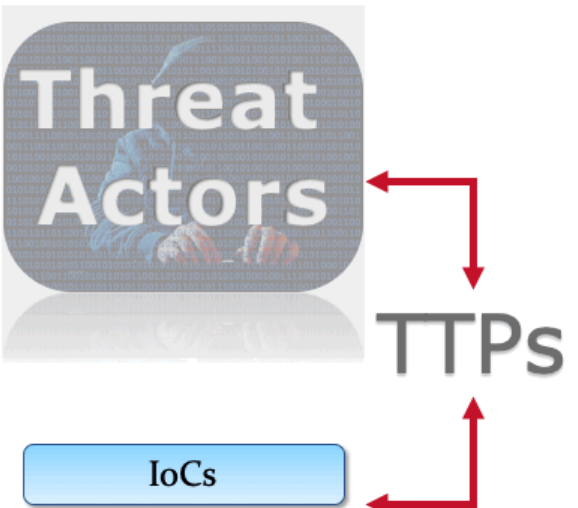
Many SOC Teams fail at doing this well.

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

© Capgemini 2019. All rights reserved

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.



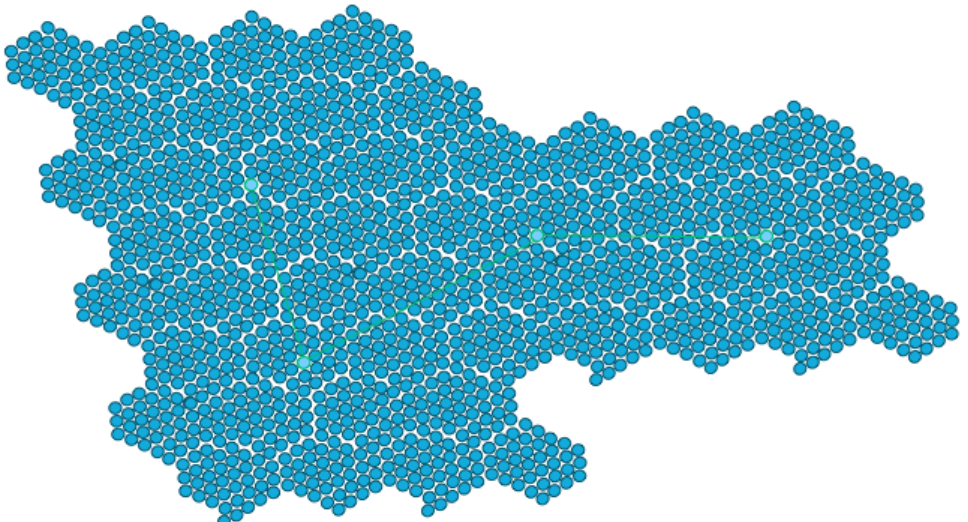
© Capgemini 2019. All rights reserved

Analysis of Threat Indicators (cont.)

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

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

How about an example…

Social Media Traffic

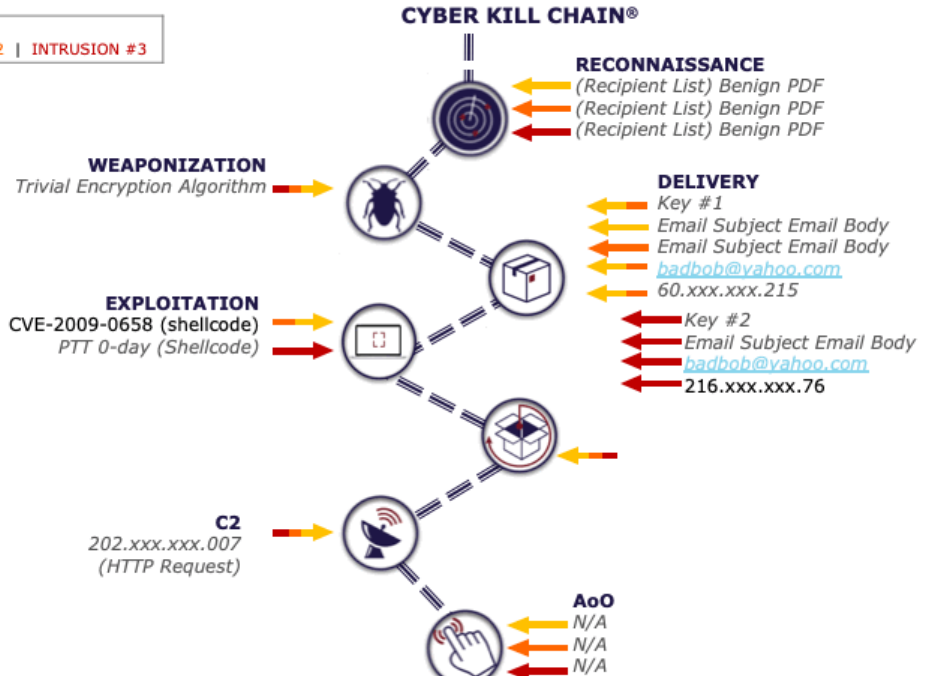
- Social media traffic has become so pervasive in our network environments; it is everywhere, and it is harmless… or is it?

- This is the perfect example of the type of traffic that an APT might use to obscure their traffic.

© Capgemini 2019. All rights reserved

Analysis of Threat Indicators

LEVELS OF INTRUSIONS:
INTRUSION #1 | INTRUSION #2 | INTRUSION #3



© Capgemini 2019. All rights reserved

Analysis of Threat Indicators (cont.)

Indicator Life Cycle

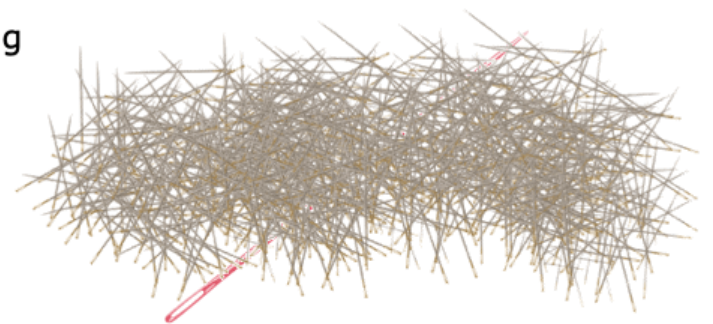
- **Revealed**
  - Through analysis or collaboration
- **Matured**
  - Leveraged into tools
- **Utilized**
  - Matching activity discovered

© Capgemini 2019. All rights reserved

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…

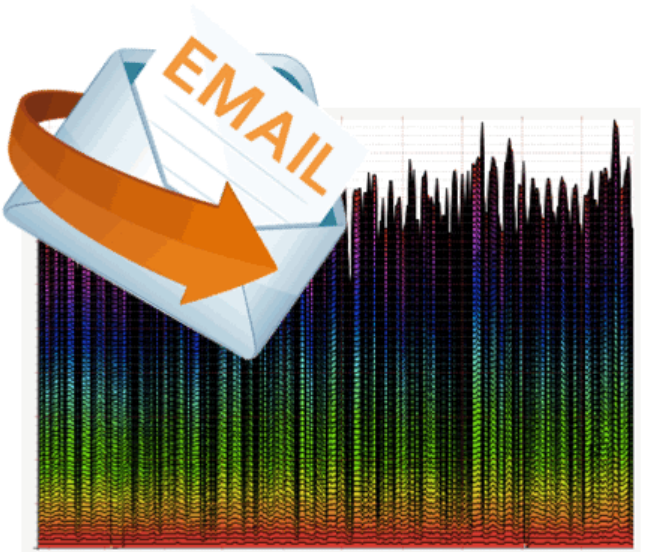


© Capgemini 2019. All rights reserved

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.



© Capgemini 2019. All rights reserved

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!

© Capgemini 2019. All rights reserved

Questions?

© Capgemini 2019. All rights reserved

Case Analysis

Capgemini

Agenda

Campaigns | TTPs | Analysis and Intrusion Detection | Threat Hunting

Topic Learning Objectives

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

- Analyze a campaign and how an indicator provides useful information to recognizing campaigns.
- Identify advanced TTPs.
- Perform a case analysis and intrusion reconstruction.
- Identify the relationship between the types of indicators that might be used to detect an adversary's activities.
- Track and map cyber incidents to the Cyber Kill Chain® phases to determine a defensive posture and focus.

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

Campaign Tracking (cont.)

Who is targeted?

© Capgemini 2019. All rights reserved

Campaign Tracking (cont.)

What technology is being targeted?

© Capgemini 2019. All rights reserved

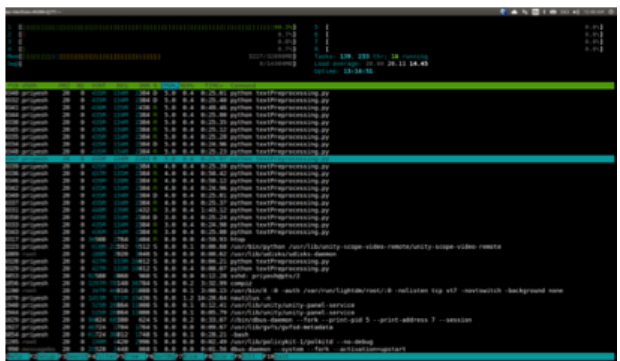
Campaign Tracking (cont.)

What specific infrastructure is used in the attack?

© Capgemini 2019. All rights reserved

Campaign Tracking (cont.)

What exploits and installation are being utilized?



© Capgemini 2019. All rights reserved

Campaign Tracking (cont.)

What backdoor is being utilized?

© Capgemini 2019. All rights reserved

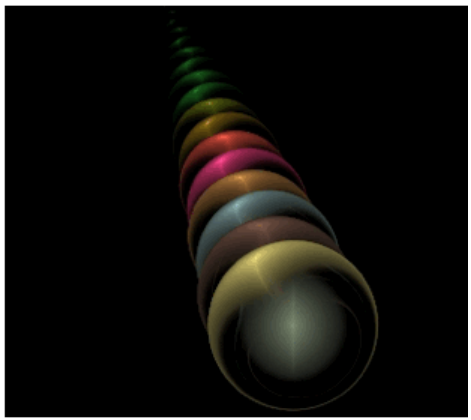
Campaign Tracking (cont.)

What C2 infrastructure is being used?

© Capgemini 2019. All rights reserved

Campaign Tracking (cont.)

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



© Capgemini 2019. All rights reserved

Tactics, Techniques, and Procedures (TTPs)

Tactics

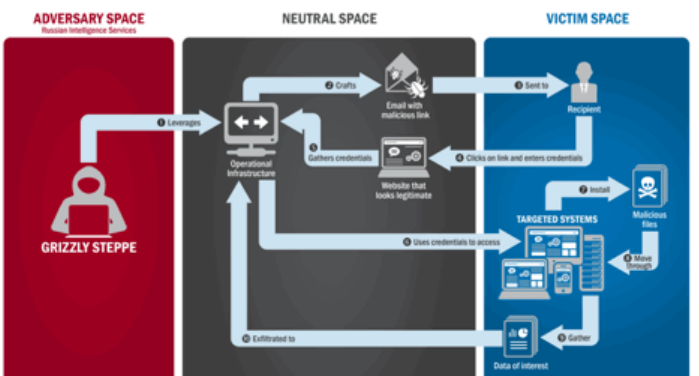
- What an attacker uses to execute the attack

© Capgemini 2019. All rights reserved

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

Techniques

- How the exploit is executed or delivered to the organization



© Capgemini 2019. All rights reserved

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

Procedures

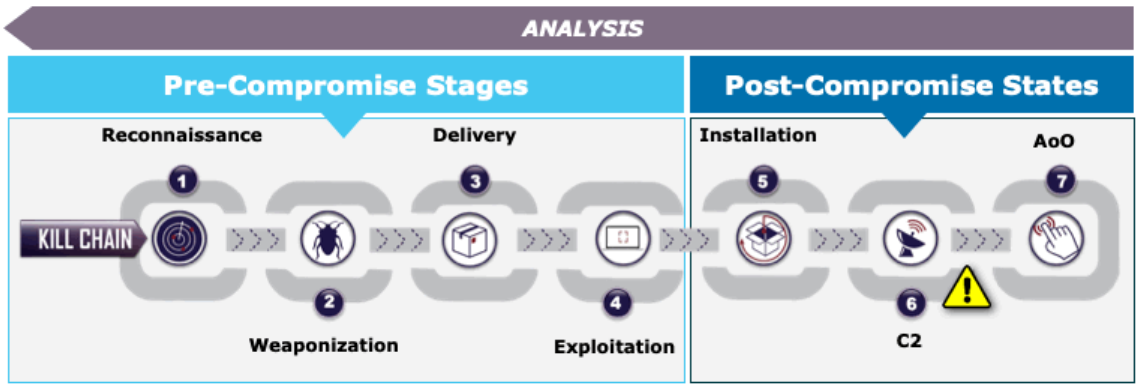
- How different tools and processes are used in concert with one another

© Capgemini 2019. All rights reserved

Analysis and Intrusion Reconstruction

Legend: ⚠ Detection Occurs

Post-Compromise State: Detection occurs.

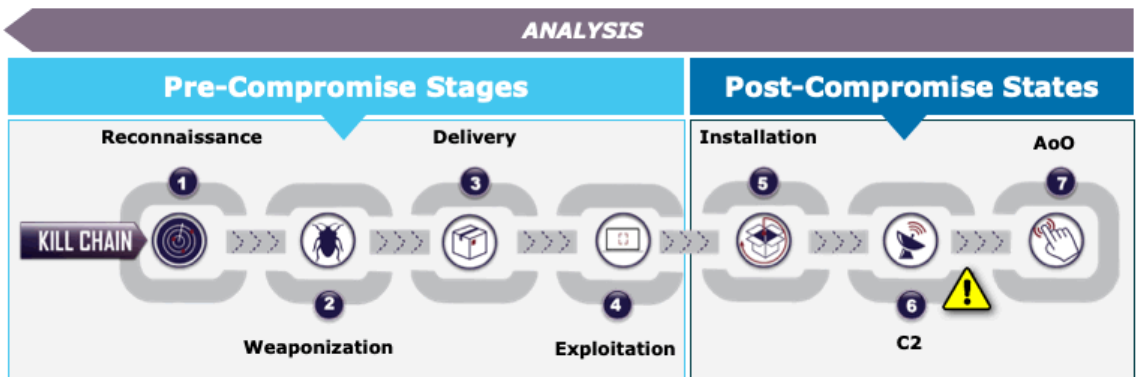


Cyber Kill Chain® progression from the adversary's perspective provides invaluable guidance for analyzing intrusions when they are detected.

© Capgemini 2019. All rights reserved

Analysis and Intrusion Reconstruction (cont.)

Full Intrusion: Analysis to re-create the Cyber Kill Chain®



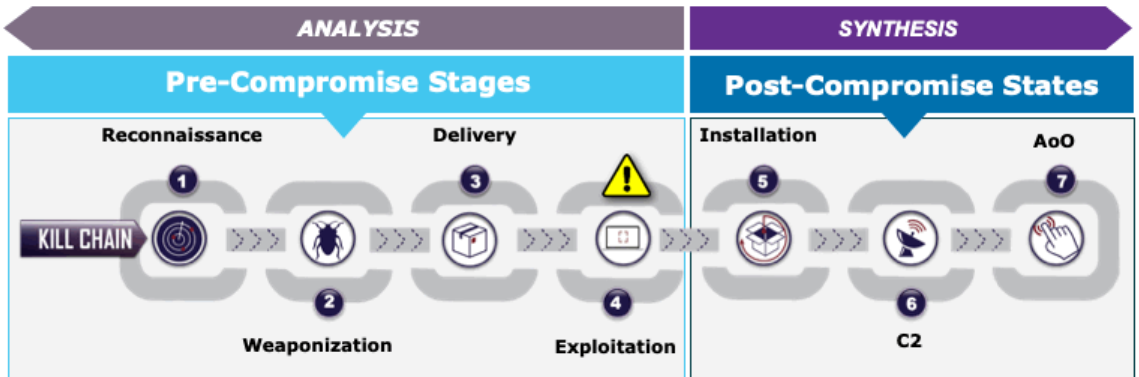
Only complete analysis of the prior phases can provide information on the actions to be taken at those phases to mitigate future intrusions.

© Capgemini 2019. All rights reserved

Analysis and Intrusion Reconstruction (cont.)

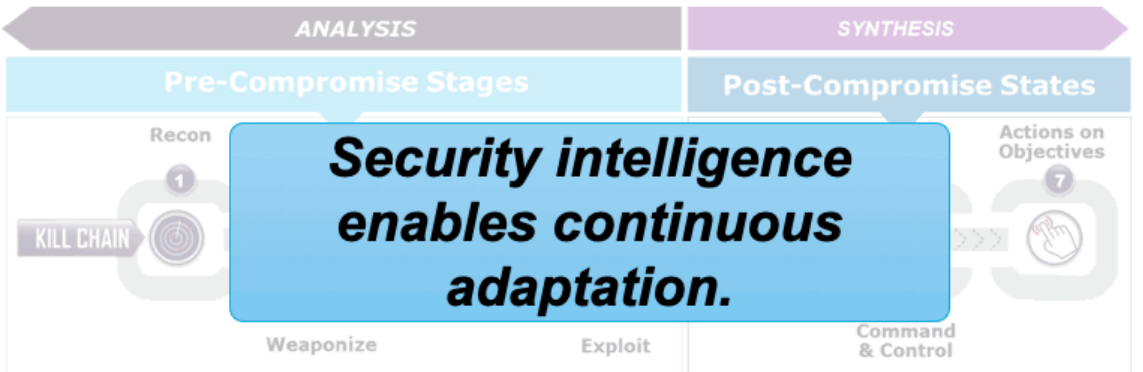
Legend: ⚠ Detection Occurs

Mitigated Intrusion: Analysis and synthesis



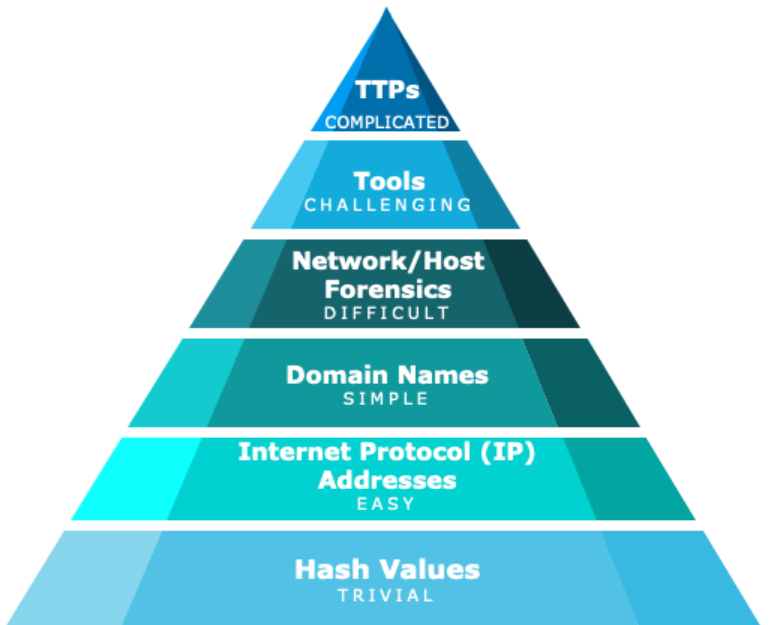
© Capgemini 2019. All rights reserved

Analysis and Intrusion Reconstruction (cont.)



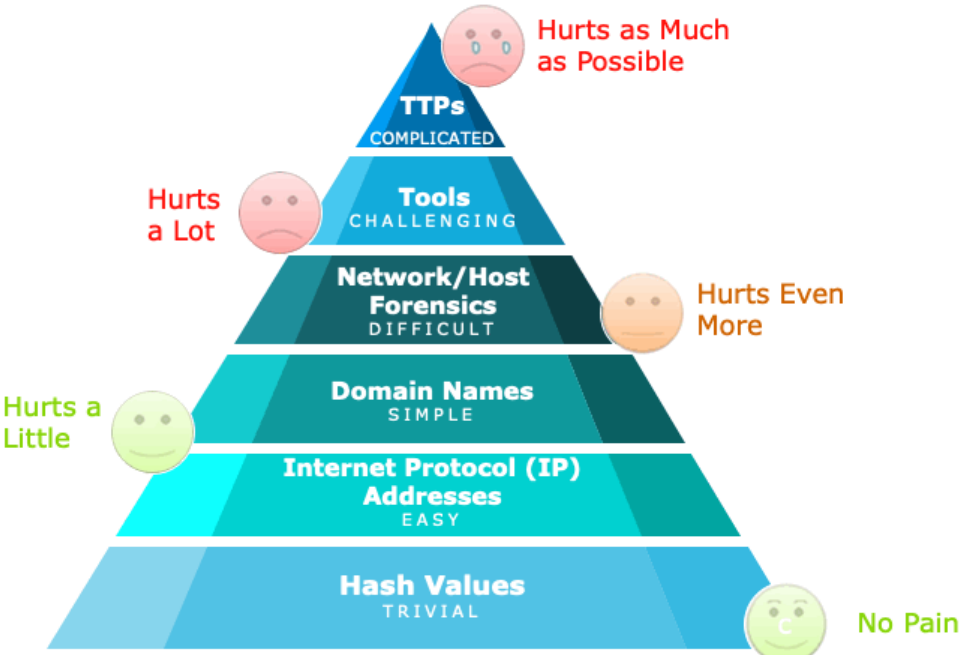
© Capgemini 2019. All rights reserved

Cyber Threat Hunting: Pyramid of Pain



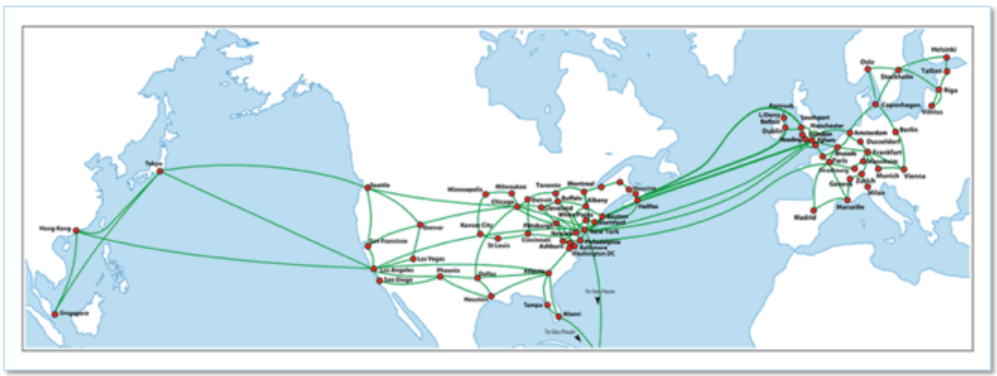
© Capgemini 2019. All rights reserved

Cyber Threat Hunting: Pyramid of Pain (cont.)



© Capgemini 2019. All rights reserved

The Cyber Kill Chain® in Cyber Strategy

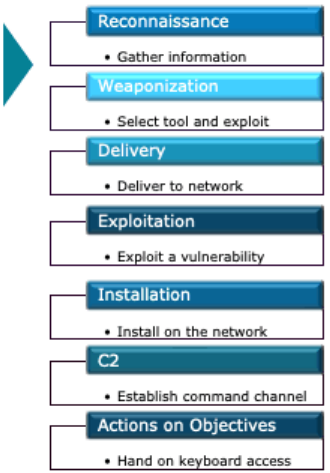


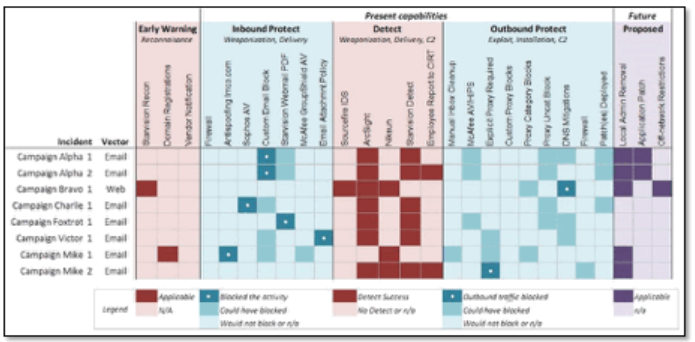
Through tracking and mapping cyber incidents to the Cyber Kill Chain® phases, information about the defensive posture and focus can be determined.

© Capgemini 2019. All rights reserved

Mapping

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



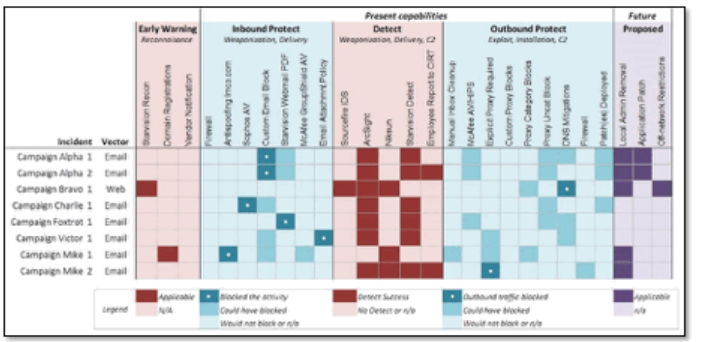


© Capgemini 2019. All rights reserved

Mapping (cont.)

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

- **Reconnaissance**
  - Gather information
- **Weaponization**
  - Select tool and exploit
- **Delivery**
  - Deliver to network
- **Exploitation**
  - Exploit a vulnerability
- **Installation**
  - Install on the network
- **C2**
  - Establish command channel
- **Actions on Objectives**
  - Hand on keyboard access



© Capgemini 2019. All rights reserved

Questions?

© Capgemini 2019. All rights reserved

Case Study: RSA® Hacked

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

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

© Capgemini 2019. All rights reserved

Case Study: Who was impacted?

Over 40,000,000 people worldwide…

Many companies and government agencies use RSA SecurID® to authenticate remote users worldwide.














© Capgemini 2019. All rights reserved

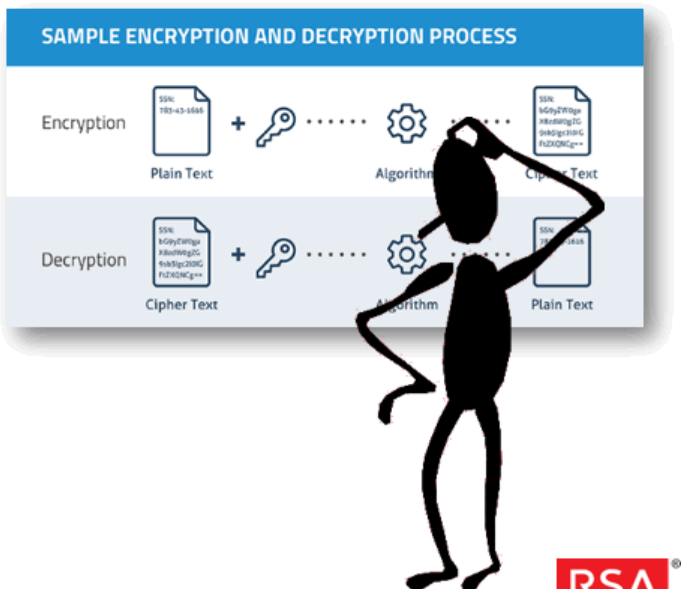
Case Study: Anatomy of an Attack

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!



© Capgemini 2019. All rights reserved

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

RSA®

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

Questions?

© Capgemini 2019. All rights reserved

Network Forensics

Capgemini

Agenda

Types of Investigations | Forensics

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.

© Capgemini 2019. All rights reserved

Forensics Investigation Overview

The network/computer forensics process can contain many steps and sub-steps.

- Areas of expertise include 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

Primary Focus of this Course

© Capgemini 2019. All rights reserved

Forensics Investigation Overview (cont.)

The 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.
- **Corporate Investigation** – follow corporate policies and procedures for conducting investigations.
- **Law Enforcement Investigation** – must follow legal processes to ensure that evidence collected is admissible in court (search warrant, chain of custody, admissibility, etc.).

© Capgemini 2019. All rights reserved

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

© Capgemini 2019. All rights reserved

Network Forensics Today

Corporate Attacks

- Many organizations have expanded their Computer Security Departments to include network/computer forensics.

Government and Military Attacks

- 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 expanded their operations to include network/computer forensics.

© Capgemini 2019. All rights reserved

Why are we learning this?

- It is important to understand network flows, protocols, and services to track malware and malicious activity.
- Understanding what is normal network traffic aids in detecting malicious network traffic.
- Cannot always rely on signature-based detection tools.
- Skills needed to be able to perform include the following:
  - Analyzing network flows
  - Carving log files
  - Deciphering attack activity
  - Deriving indicators
  - Recommending mitigations

© Capgemini 2019. All rights reserved

Cyber Threat Model

We can affect change in the Cyber Kill Chain® in the following phases:

Reconnaissance		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.

© Capgemini 2019. All rights reserved

Intelligence Management and Situational Awareness

Record findings and analysis!

- The intelligence-based approach requires that findings are recorded for further analysis and correlation.
- Record all of the pertinent details.
- Case management systems are important for recording, archiving, and analysis of data.
  - 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

© Capgemini 2019. All rights reserved

Incident Response

Capgemini

Agenda

Security Incidents | Incident Response

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.

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

Why Is Incident Response Important?

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

© Capgemini 2019. All rights reserved

Incident Response Capabilities

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

© Capgemini 2019. All rights reserved

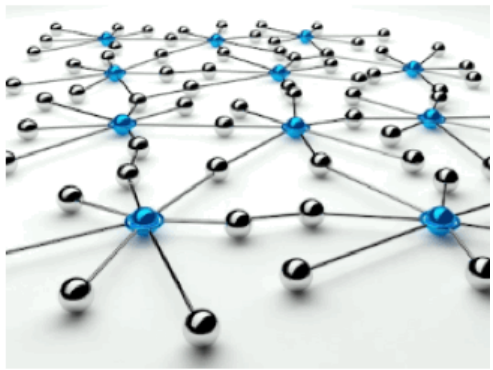
Common Threats

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

© Capgemini 2019. All rights reserved

Incident Response Guidance

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

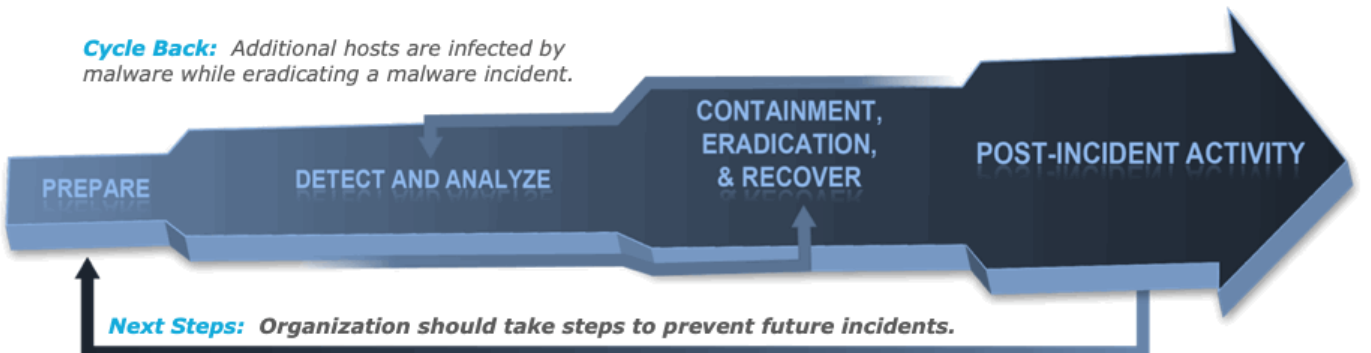


© Capgemini 2019. All rights reserved

Incident Response – The Team

© Capgemini 2019. All rights reserved

Incident Response Life Cycle



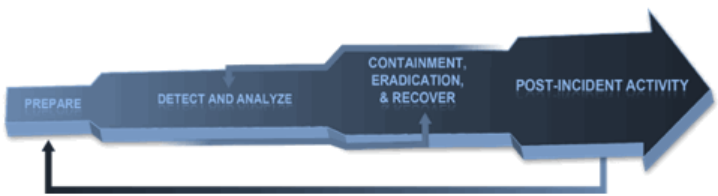
© Capgemini 2019. All rights reserved

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.



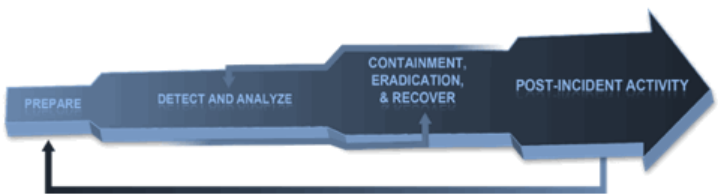
© Capgemini 2019. All rights reserved

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

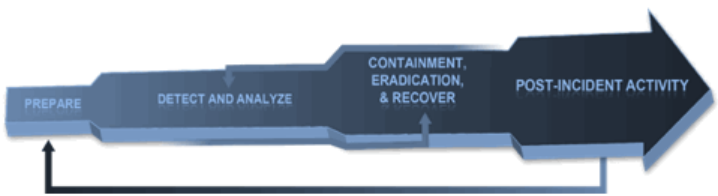


© Capgemini 2019. All rights reserved

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.

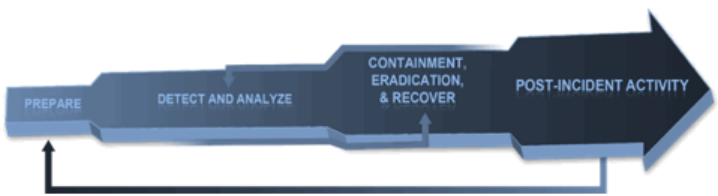


© Capgemini 2019. All rights reserved

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.

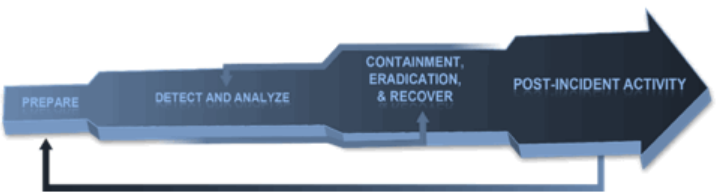


© Capgemini 2019. All rights reserved

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



© Capgemini 2019. All rights reserved

CASE002: Incident Response Case Study

SONY

TARGET

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

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.

© Capgemini 2019. All rights reserved

Questions?

© Capgemini 2019. All rights reserved

People matter, results count.

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

This presentation contains information that may be privileged or confidential and is the property of the CapGemini Group.

Copyright © 2019 CapGemini. All rights reserved.