MISSION BEFORE MONEY

Class #9 – Domain 7

Christophe Foulon

Christophe Foulon - CPF Coaching, Founder & Coach
Quick housekeeping reminder.

• The online/live chat that’s provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.

• At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.

• Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.

• Failure to abide by the rules may result in disabling chat for you.

• Do not copy or share copy of copyrighted materials.
DAD JOKE TIME

WHY DOES PETER PAN FLY?
BECAUSE HE NEVERLANDS!
I LOVE THIS JOKE.
IT NEVER GROWS OLD!

WANT TO HEAR A PIZZA JOKE?
NEVER MIND, IT’S TOO CHEESY.

HOW DOES A TREE GET ON THE INTERNET?
IT LOGS ON

THE DAD-JOKES ARE STRONG
WITH THIS ONE
WHO I AM?

Outside of being a security practitioner focused on helping businesses tackle their cybersecurity risks while minimizing friction resulting in increased resiliency and helping to secure people and processes with a solid understanding of the technology involved.

I am a dad, dog dad and career coach. I love helping other to achieve their best. Through this channel, I help veterans with their transitions and others via non-profits like Whole Cyber Human Initiative, Boots2Books and others.

I give back by producing a podcast focused on helping people who are “Breaking into Cybersecurity” by sharing the stories of those who have done it in the past 5 years to inspire those looking to do it now.

Co-authored:
“Develop Your Cybersecurity Career Path: How to Break into Cybersecurity at Any Level”
“Hack the Cybersecurity Interview: A complete interview preparation guide for jumpstarting your cybersecurity career”
And advised on “Understand, Manage, and Measure Cyber Risk”
INTRODUCTION

Agenda

• Welcome, Reminders, & Introduction
• Questions
• Domain 7 – Communication and Network Security (pp. 463 - Kindle)
INTRODUCTION

Agenda

- Welcome, Reminders, & Introduction
- Questions
- **Domain 7 – Communication and Network Security (pp. 463 - Kindle)**

Only 15 sections to cover in this most excellent domain...
Quick housekeeping reminder.

- The online/live chat that’s provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT** share or post copywritten materials. (pdf of book)
We're through Chapters 1, 2, 3, and part way into Chapter 4!

• Check-in.

• How many have read Chapter 1, 2 & 3?

• Questions?

Managing Risk!

Study Tips:
• Study in small amounts frequently (20-30 min)
• Flash card and practice test apps help
• Take naps after heavy topics (aka Security Models)
• Write things down, say them out loud
• Use the Slack Channels
• Exercise or get fresh air in between study sessions
We're through Chapters 1, 2, 3, and part way into Chapter 4!

• Check-in.
• How many have read Chapter 1, 2 & 3?
• Questions?

CISSP® MENTOR PROGRAM – SESSION NINE

GETTING GOING...
Managing Risk!

Study Tips:
• Study in small amounts frequently (20-30 min)
• Flash card and practice test apps help
• Take naps after heavy topics (aka Security Models)
• Write things down, say them out loud
• Use the Slack Channels
• Exercise or get fresh air in between study sessions

Stick with it. You’ll be glad you did. I promise.
CISSP® MENTOR PROGRAM – SESSION NINE

GETTING GOING...

THANK YOU!

• **Ron** – GREAT job Monday on Domain #6 - Security Assessment and Testing!

• **Ryan** is keeping us ready with all the live streamy techy stuff!

• **AJ** welcome to the team!

• **Brandon Matis** running things and things.

• Many unsung **FRSecure heroes** doing heroey things.
• Christophe – GREAT job Monday on Domain #6 – Security Assessment and Testing!

• Ryan is keeping us ready with all the live streamy techy stuff!

• Ron is still EL MEJOR PROFESOR! Answering questions ALL DAY.

• Brandon Matis running things and things.

• Many unsung FRSecure heroes doing heroey things.

CISSP® MENTOR PROGRAM – SESSION NINE

GETTING GOING…

THANK YOU!

#MissionBeforeMoney
INTRODUCTION

Agenda

- Welcome, Reminders, & Introduction
- Questions
- Domain 7 – Security Operations (pp. 463 - Kindle)
How about some practice ones?

1. What is the essential difference between a self-audit and an independent audit?
   a. Tools used
   b. Competence
   c. Results
   d. Objectivity
QUESTIONS.

How about some practice ones?

1. What is the essential difference between a self-audit and an independent audit?
   a. Tools used
   b. Competence
   c. Results
   d. Objectivity
How about some practice ones?

2. Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

   a. Black box testing
   b. Pilot Testing
   c. Parallel Test
   d. Regression Testing
How about some practice ones?

2. Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?
   a. Black box testing
   b. Pilot Testing
   c. Parallel Test
   d. Regression Testing
How about some practice ones?

3. What would a significant benefit be from conducting an unannounced penetration test?

a. The pen test would be a more realistic analysis of the target network
b. The security analyst could not provide an honest analysis
c. It is best to catch critical infrastructure unpatched:
d. Network security would be in a "best state" posture
How about some practice ones?

3. What would a significant benefit be from conducting an unannounced penetration test?

   a. The pen test would be a more realistic analysis of the target network
   b. The security analyst could not provide an honest analysis
   c. It is best to catch critical infrastructure unpatched
   d. Network security would be in a "best state" posture
QUESTIONS.

How about some practice ones?

4. Which of the following answers represents part of the attack phase of a penetration test?
   a. Getting the legal documents signed
   b. Active or Passive Reconnaissance
   c. Escalate Privileges
   d. Removing all tools and exploits:
How about some practice ones?

4. Which of the following answers represents part of the attack phase of a penetration test?

a. Getting the legal documents signed
b. Active or Passive Reconnaissance
c. Escalate Privileges
d. Removing all tools and exploits:
How about some practice ones?

5. Which well-known model is used for understanding the maturity level of a process?
   a. The Zachman Framework
   b. CMM - Capability Maturity Model
   c. HIPAA
   d. PCI-DSS
How about some practice ones?

5. Which well-known model is used for understanding the maturity level of a process?
   a. The Zachman Framework
   b. **CMM - Capability Maturity Model**
   c. HIPAA
   d. PCI-DSS
How about some practice ones?

5. Which well-known model is used for understanding the maturity level of a process?
   a. The Zachman Framework
   b. CMM - Capability Maturity Model
   c. HIPAA
   d. PCI-DSS
QUESTIONS.

How about some practice ones?

6. What would you call a collection of tools that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means?

a. The pandora toolbox
b. Advanced Persistent Threats
c. Such a collection of tools does not exist
d. Breach & attack Simulation
How about some practice ones?

6. What would you call a collection of tools that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means?

a. The pandora toolbox  
b. Advanced Persistent Threats  
c. Such a collection of tools does not exist  
d. Breach & attack Simulation
How about some practice ones?

7. Organizations should not view disaster recovery as which of the following?

a. Committed expense
b. Enforcement of legal statutes
c. Compliance with regulations
d. Discretionary expense
How about some practice ones?

7. Organizations should not view disaster recovery as which of the following?
   a. Committed expense
   b. Enforcement of legal statutes
   c. Compliance with regulations
   d. Discretionary expense
How about some practice ones?

8. What is a common way of preventing users from running code that has been altered or corrupted since it was originally approved and installed?

a. Software Accreditation
b. IDEA - International Data Encryption Algorithm
c. Code Signing
d. Code Hashing
How about some practice ones?

8. What is a common way of preventing users from running code that has been altered or corrupted since it was originally approved and installed?

a. Software Accreditation
b. IDEA - International Data Encryption Algorithm

c. **Code Signing**
d. Code Hashing
QUESTIONS.

How about some practice ones?

9. Which answer is generally not associated with a resource exhaustion attack?
   a. Teardrop Attack
   b. Fork Bomb
   c. Smurf Attack
   d. Memory Leak
How about some practice ones?

9. Which answer is generally not associated with a resource exhaustion attack?

a. Teardrop Attack
b. Fork Bomb
c. Smurf Attack
d. Memory Leak
How about some practice ones?

10. What process can tell an executive manager about the state of the organization's security program?

a. Internal Risk Assessment
b. A Security Audit
c. Change Control Processes
d. Security Incident Logs
How about some practice ones?

10. What process can tell an executive manager about the state of the organization’s security program?

   a. Internal Risk Assessment
   b. A Security Audit
   c. Change Control Processes
   d. Security Incident Logs
How about some practice ones?

10. What process can tell an executive manager about the state of the organization's security program?

   a. Internal Risk Assessment
   b. A Security Audit
   c. Change Control Processes
   d. Security Incident Logs

There!
10 outta 10.
INTRODUCTION

Agenda

• Welcome, Reminders, & Introduction
• Questions
• Domain 7 – Security Operations (pp. 463 - Kindle)
INTRODUCTION

Agenda

- Welcome, Reminders, & Introduction
- Questions
- Domain 7 – Security Operations (pp. 463 - Kindle)

Now this...
Domain 7 – Security Operations (pp. 463 - Kindle)

• 7.1 - Understand and comply with investigations
• 7.2 - Conduct logging and monitoring activities
• 7.3 - Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
• 7.4 - Apply foundational security operations concepts
• 7.5 - Apply resource protection
• 7.6 - Conduct incident management
• 7.7 - Operate and maintain detective and preventative measures
• 7.8 - Implement and support patch and vulnerability management
Domain 7 – Security Operations (pp. 463 - Kindle)

- 7.9 - Understand and participate in change management processes
- 7.10 - Implement recovery strategies
- 7.11 - Implement Disaster Recovery (DR) processes
- 7.12 - Test Disaster Recovery Plans (DRP)
- 7.13 - Participate in Business Continuity (BC) planning and exercises
- 7.14 - Implement and manage physical security
- 7.15 - Address personnel safety and security concern
INTRODUCTION

Agenda

Domain 7 – Security Operations (pp. 463 - Kindle)

• 7.9 - Understand and participate in change management processes
• 7.10 - Implement recovery strategies
• 7.11 - Implement Disaster Recovery (DR) processes
• 7.12 - Test Disaster Recovery Plans (DRP)
• 7.13 - Participate in Business Continuity (BC) planning and exercises
• 7.14 - Implement and manage physical security
• 7.15 - Address personnel safety and security concern

Alright, piece of cake.
INTRODUCTION

Domain 7 – Security Operations (pp. 463 - Kindle)

- 7.9 - Understand and participate in change management processes
- 7.10 - Implement recovery strategies
- 7.11 - Implement Disaster Recovery (DR) processes
- 7.12 - Test Disaster Recovery Plans (DRP)
- 7.13 - Participate in Business Continuity (BC) planning and exercises
- 7.14 - Implement and manage physical security
- 7.15 - Address personnel safety and security concerns

Hold up a second though...

Alright, piece of cake.
DAD JOKE...
If you don’t like it, it’s Brad’s fault!
DAD JOKE...
If you don’t like it, it’s Brad’s fault!

How many tickles does it take to make an octopus laugh?
DAD JOKE...
If you don’t like it, it’s Brad’s fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!
DAD JOKE...
If you don’t like it, it’s Brad’s fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!

You get it right?! Ten tickles, like tentacles.
DAD JOKE...
If you don’t like it, it’s Brad’s fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!

You get it right?! Ten tickles, like tentacles.

Octopuses have tentacles! LOL!
DAD JOKE...
If you don’t like it, it’s Brad’s fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!

You get it right?! Ten tickles, like tentacles.

Octopuses have tentacles! LOL!

NO? Whatever...
Security operations is about day-to-day operations and maintenance of the information security program.

- Also known as “SecOps”.
- If information security is “risk management”, SecOps is continual risk management.
- Take all the things you’ve learned so far and operationalize them.
- ...and a little more.
CISSP® MENTOR PROGRAM – SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS
Understand and comply with investigations

Topics include:

• Evidence collection and handling
• Reporting and documentation
• Investigative techniques
• Digital forensics tools, tactics, and procedures
• Artifacts (e.g., computer, network, mobile device)

It’s important to get this right. A CISSP isn’t expected to be a DFIR expert, but they must know the basics.
Evidence Collection and Handling

- Evidence supports something an assertion or proposition.
- The better the evidence, the better the support.
- There are four types evidence by which facts can be proven or disproven at trial which include:
  - Real evidence;
  - Demonstrative evidence;
  - Documentary evidence; and
  - Testimonial evidence.

Real evidence

- often called physical evidence: material items involved in a case, objects and things a jury can physically hold and inspect. Examples of real evidence include fingerprints, blood samples, DNA, a knife, a gun, and other physical objects.
- Usually admitted because it tends to prove or disprove an issue of fact in a trial.
- In order to be used at trial, real evidence must be relevant, material, and authentic. MUST establish the item's chain of custody.

Demonstrative Evidence

- Usually charts and diagrams, to demonstrate or illustrate the testimony of a witness.
- It's admissible when it fairly and accurately reflects the witness's testimony and is more probative than prejudicial. Maps, diagrams of a crime scene, charts and graphs that illustrate physical or financial injury to a plaintiff are examples of demonstrative evidence.
- Witnesses create and use demonstrative evidence at trial and opposing counsel may use the same evidence to prove contrary positions.

Documentary Evidence

• The production of documents at trial is documentary evidence.
• Presented to prove or disprove certain allegations at trial.
• Documents can be from a vast number of sources from diaries, letters, contracts, newspapers, and any other type of document that you can think of.
• There are restrictions and qualifications for using documents at trial as there is a need to make sure they are authentic and trustworthy.

Testimonial Evidence]

When a person gets up on the stand at trial and relates something that they saw or heard, that is testimonial evidence. It is simply a witness giving testimony under oath about the facts of the case.

Evidence Collection and Handling

Testimonial Evidence

When a person gets up on the stand at trial and relates something that they saw or heard, that is testimonial evidence. It is simply a witness giving testimony under oath about the facts of the case.

OK, back to our regularly scheduled programming...

Collecting Digital Evidence

• The integrity of the evidence is CRITICAL!
• Rule of Thumb – IF YOU’RE GOING TO FAST TO DOCUMENT EVERYTHING, THEN YOU’RE GOING TO FAST.
• Document dates, times, physical locations, logical locations, all actions that were taken, observations, etc. TIP: Take pictures too.
• NEVER tamper with original versions of anything. ALWAYS make write-block, make bit-level copies, and investigate on the copies. TIP: Make two copies and store the original safely.
Collecting Digital Evidence

- The integrity of the evidence is CRITICAL!

- Rule of Thumb
  - IF YOU'RE GOING TO FAST TO DOCUMENT EVERYTHING, THEN YOU'RE GOING TO FAST.

- Document dates, times, physical locations, logical locations, all actions that were taken, observations, etc. TIP: Take pictures too.

- NEVER tamper with original versions of anything. ALWAYS make write-block, make bit-level copies, and investigate on the copies. TIP: Make two copies and store the original safely.

I prefer hardware write-blockers.
Did I mention integrity?!  
Every second must be accounted for from the second you encounter evidence until you no longer have any contact with the evidence.  
Chain of Custody must be maintained.  
Handling Digital Evidence

- Did I mention integrity?!
- Every second must be accounted for from the second you encounter evidence until you no longer have any contact with the evidence.
- Chain of Custody must be maintained.

Appendix E – Incident Response Chain of Custody Form

**Section 1: System/Hard Drive/Computer Details** (TO BE COMPLETED BY THE ORIGINAL ACQUERER)
- Please complete as much of this section as possible.
- Each item taken into custody requires a new form.
- The IRT will assist as needed and assign an incident number.

<table>
<thead>
<tr>
<th>Incident #:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Acquirer:</td>
<td>Department:</td>
</tr>
<tr>
<td>Item #:</td>
<td>Item Description:</td>
</tr>
<tr>
<td>Manufacturer:</td>
<td>Model #:</td>
</tr>
</tbody>
</table>

**Section 2: Chain of Custody** (TO BE COMPLETED BY ALL PARTIES INVOLVED WITH EACH TRANSFER)
- Print form before proceeding to complete this section.
- Fill in each field entirely.
- If a field does not apply, enter "N/A" and initial.

<table>
<thead>
<tr>
<th>Tracking #</th>
<th>Date/Time</th>
<th>FROM</th>
<th>TO</th>
<th>Reason for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td>Signature</td>
<td>Signature</td>
</tr>
<tr>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td>Signature</td>
<td>Signature</td>
</tr>
<tr>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td>Signature</td>
<td>Signature</td>
</tr>
<tr>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology
Reporting and Documentation

• Again, document EVERYTHING.
• As much as possible, avoid subjective interpretations and space for subjective interpretations.
• As much as possible, ensure evidence is admissible (even if you’re not sure that your evidence will be presented in court).
Reporting and Documentation

Admissibility of Evidence:

• **Accuracy** – lacking errors.
• **Authenticity** - undisputed origin.
• **Comprehensibility** – paint as much of the picture as possible.
• **Convincing** – certainty in conclusions.
• **Objective** – what the evidence says, not what you say. Facts versus opinions.
• **Admissible** – for the court in question.
Admissibility of Evidence:

- **Accuracy** – lacking errors.
- **Authenticity** – undisputed origin.
- **Comprehensibility** – paint as much of the picture as possible.
- **Convincing** – certainty in conclusions.
- **Objective** – what the evidence says, not what you say. Facts versus opinions.
- **Admissible** – for the court in question.

Seek advice from legal counsel, law enforcement, or other investigative professionals to ensure evidence you collect, handle, and prepare is adequate.
Reporting and Documentation

Admissibility of Evidence:

- **Accuracy** – lacking errors.
- **Authenticity** – undisputed origin.
- **Comprehensibility** – paint as much of the picture as possible.
- **Convincing** – certainty in conclusions.
- **Objective** – what the evidence says, not what you say. Facts versus opinions.
- **Admissible** – for the court in question.

---

**Admissible Evidence**

Admissible evidence is evidence that may be presented before the trier of fact (i.e., the judge or jury) for them to consider in deciding the case. Compare inadmissible evidence.

Rules of evidence determine what types of evidence is admissible, and the trial court judge applies these rules to the case. Generally, to be admissible, the evidence must be relevant and not outweighed by countervailing considerations (e.g., the evidence is unfairly prejudicial, confusing, a waste of time, privileged, or, among other reasons, based on hearsay).

In federal court, the Federal Rules of Evidence govern whether evidence is admissible. Rule 402 provides that “relevant evidence is admissible” unless the Constitution, statute, or the rules make evidence inadmissible. Common rules of evidence that make relevant evidence inadmissible are: Rule 403, which excludes relevant evidence for prejudice, confusion, or waste of time; Rule 404, which generally excludes character evidence and evidence of other crimes, wrong, or acts; and Rule 802, which excludes hearsay, although there are several exceptions. Each state also has its own rules of evidence for state court proceedings, and many states' rules of evidence follow the Federal Rules of Evidence closely.
Reporting and Documentation

Admissibility of Evidence:

• **Accuracy** – lacking errors.
• **Authenticity** – undisputed origin.
• **Comprehensibility** – paint as much of the picture as possible.
• **Convincing** – certainty in conclusions.
• **Objective** – what the evidence says, not what you say. Facts versus opinions.
• **Admissible** – for the court in question.

Understand and comply with investigations #MissionBeforeMoney
Seek advice from legal counsel, law enforcement, or other investigative professionals to ensure evidence you collect, handle, and prepare is adequate.

[Rule 802. The Rule Against Hearsay](https://www.law.cornell.edu/rules/fre/rule_802)

Hearsay is not admissible unless any of the following provides otherwise:

- a federal statute;
- these rules; or
- other rules prescribed by the Supreme Court.

**Notes**


**Notes of Advisory Committee on Proposed Rules**

The provision excepting from the operation of the rule hearsay which is made admissible by other rules adopted by the Supreme Court or by Act of Congress continues the admissibility thereunder of hearsay which would not qualify under these Evidence Rules. The following examples illustrate the working of the exception:

**Federal Rules of Civil Procedure**

Rule 4(g): proof of service by affidavit.

Rule 32: admissibility of depositions.
DOMAIN 7 – SECURITY OPERATIONS
Understand and comply with investigations
Investigative Techniques

Four main techniques

• **Data capture** – manual and automatic capture.
• **Interviews** – ideally from someone who was a witness to an incident or a person with first-hand knowledge of the incident.
• **Interrogations** – usually done by law enforcement following stringent rules.
• **External requests** – usually warrants and subpoenas.
Four main techniques

• **Data capture** – manual and automatic capture.

• **Interviews** – ideally from someone who was a witness to an incident or a person with first-hand knowledge of the incident.

• **Interrogations** – usually done by law enforcement following stringent rules.

• **External requests** – usually warrants and subpoenas.

Let the evidence draw your conclusions. If the evidence isn’t available (coming later), you may not be able to draw conclusions.

When in question, leave it to the experts.
DIGITAL FORENSICS TOOLS, TACTICS, AND PROCEDURES

DOMAIN 7 – SECURITY OPERATIONS
Understand and comply with investigations

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Forensics investigators (the good ones) have a “jumpbag” with their tools ready to use.

Write blockers and drive imagers designed to allow examination or imaging of a storage device, typically a hard drive, without writing any data to the storage device, which would violate the integrity of the evidence.
Digital Forensics Tools, Tactics, and Procedures

Write blockers and drive imagers designed to allow examination or imaging of a storage device, typically a hard drive, without writing any data to the storage device, which would violate the integrity of the evidence.

CISSP® MENTOR PROGRAM – SESSION NINE

DOMAINE 7 – SECURITY OPERATIONS

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

#MissionBeforeMoney
Digital Forensics Tools, Tactics, and Procedures

Faraday containers

Protects evidence from electromagnetic interference.
Digital Forensics Tools, Tactics, and Procedures

Faraday containers
Protects evidence from electromagnetic interference.
SESSION NINE

CURIETY OPERATIONS
comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Faraday containers
Protects evidence from electromagnetic interference.

CISSP® MENTOR PROGRAM

– SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Digital Forensics Tools, Tactics, and Procedures

Faraday containers

Protects evidence from electromagnetic interference.

CISSP® MENTOR PROGRAM – SESSION NINE

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Video and audio recording tools

I’ve heard it in court before, “video doesn’t lie”. Might be sorta true, but video and audio can be very compelling. Can save a lot of time during an investigation too.

In general, Secure the physical ”crime scene” first.
Digital Forensics Tools, Tactics, and Procedures

- **Network traffic analysis** tools - Wireshark (and similar) for pcap and analysis.
- **Log analysis** tools - SIEM (and similar) to reconstruct events across systems and for context.
- **Data recovery** tools – file recovery for things deleted or overwritten
- **Virtual machines** – useful for rebuilding (isolated) environments.
- **Code analysis** tools - decompilers and reverse-engineer software.
- **Hashing** tools – integrity verification.
- **Toolkits** – software suite specifically designed for forensic investigations.
• **Network traffic analysis tools** - Wireshark (and similar) for pcap and analysis.

• **Log analysis tools** - SIEM (and similar) to reconstruct events across systems and for context.

• **Data recovery tools** - file recovery for things deleted or overwritten.

• **Virtual machines** – useful for rebuilding (isolated) environments.

• **Code analysis tools** - decompilers and reverse engineer software.

• **Hashing tools** – integrity verification.

• **Toolkits** – software suite specifically designed for forensic investigations.
Digital Forensics Tools, Tactics, and Procedures

- Network traffic analysis tools - Wireshark (and similar) for pcap and analysis.
- Log analysis tools - SIEM (and similar) to reconstruct events across systems and for context.
- Data recovery tools - file recovery for things deleted or overwritten.
- Virtual machines - useful for rebuilding (isolated) environments.
- Code analysis tools - decompilers and reverse engineer software.
- Hashing tools - integrity verification.
- Toolkits - software suite specifically designed for forensic investigations.
Digital Forensics Tools, Tactics, and Procedures

Techniques and Procedures

• Digital forensics is a specialized skill.
• Strict procedures should be prepared ahead of time and followed for conducting a forensic investigation.
• Either part of an incident response (IR) plan or a supplement to an IR plan.
• Documented standards for the collection, handling, and investigation of digital evidence include ISO 27041, 27042, 27043, and 27050
• SANS - https://www.sans.org/posters/?focus-area=digital-forensics
Digital Forensics Tools, Tactics, and Procedures

Techniques and Procedures

• Digital forensics is a specialized skill.
• Strict procedures should be prepared ahead of time and followed for conducting a forensic investigation.
• Either part of an incident response (IR) plan or a supplement to an IR plan.
• Documented standards for the collection, handling, and investigation of digital evidence include ISO 27041, 27042, 27043, and 27050.

SANS - https://www.sans.org/posters/?focus-area=digital-forensics

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Techniques and Procedures

• Digital forensics is a specialized skill.
• Strict procedures should be prepared ahead of time and followed for conducting a forensic investigation.
• Either part of an incident response (IR) plan or a supplement to an IR plan.
• Documented standards for the collection, handling, and investigation of digital evidence include ISO 27041, 27042, 27043, and 27050
• SANS - https://www.sans.org/posters/?focus-area=digital-forensics
• NIST Computer Forensics Tool Testing Program (CFTT) site: nist.gov/itl/ssl/software- quality-group/computer-forensics-tool-testing-program-cftt
Digital Forensics Tools, Tactics, and Procedures

Techniques and Procedures

- Digital forensics is a specialized skill.
- Strict procedures should be prepared ahead of time and followed for conducting a forensic investigation.
- Either part of an incident response (IR) plan or a supplement to an IR plan.
- Documented standards for the collection, handling, and investigation of digital evidence include ISO 27041, 27042, 27043, and 27050.
- SANS - https://www.sans.org/posters/?focus-area=digital-forensics
- NIST Computer Forensics Tool Testing Program (CFTT) site: nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

CISSP® MENTOR PROGRAM

#MissionBeforeMoney
Techniques and Procedures (generic procedure steps in book)

1. Define priorities
2. Identify data sources
3. Plan to collect data and execute
4. Document and preserve integrity
5. Look for hidden or erased data
6. Perform analysis

In reality, you are performing analysis continually (so this is not serial). **ALWAYS** let the evidence (and logic) lead the investigation. Do **NOT** make assumptions whenever possible.
DOMAIN 7 – SECURITY OPERATIONS
Understand and comply with investigations
Digital Forensics Tools, Tactics, and Procedures
Cloud-Specific
Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing

June 2013
DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Artifacts
Edmond Locard, also known as the "Sherlock Holmes of France" came up with a principle that states that every contact by a criminal leaves behind a trace.

"Elementary, my dear Watson!"

Locard’s Principle
Artifacts – Computers (Sources)

Windows
Logs (Event Viewer and others), Recycle Bin, Registry, etc.

Apple macOS
Logs (Console and others), Trash, Time Machine, property list (PLIST) files.

Linux
/usr folder, /tmp (volatile temporary files), /var (caches, log files, and information about currently running processes).
Artifacts – Computers (Sources)

Browsers
Cache, history, cookies, etc.

Local Storage
File remnants, deleted files, file movement, etc.

Cloud Storage
Not unlike local storage, but investigators typically don’t have the same level of access; therefore, requests are made informally and/or formally of cloud providers.
Artifacts – Network (Sources)

NetFlow
Collect IP network traffic as it enters or exits interfaces. A network administrator can determine the source and destination of traffic, class of service, data types, etc.

Packet analysis (pcap)
Captures details about communications and the data itself.

Known bad traffic (block list)
C2 traffic, known malicious sites, etc. This one is big for IoCs.

Network device log files
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>0.31180</td>
<td>10.0.0.101</td>
<td>74.125.226.163</td>
<td>HTTP</td>
<td>749</td>
<td>GET /api/manifest/hls_variant/source/yt_live_broadcast/ipbits/0/fexp/935633%2C92761</td>
</tr>
<tr>
<td>45</td>
<td>0.37830</td>
<td>74.125.226.163</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>731</td>
<td>100 OK (application/vnd.apple.mpegurl)</td>
</tr>
<tr>
<td>49</td>
<td>0.47546</td>
<td>10.0.0.101</td>
<td>74.125.226.163</td>
<td>HTTP</td>
<td>893</td>
<td>GET /manifest/hls_playlist/id/veja5b5j20/itag92/source/yt_live_broadcast/ra</td>
</tr>
<tr>
<td>59</td>
<td>0.59009</td>
<td>74.125.226.163</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>1294</td>
<td>100 OK (application/vnd.apple.mpegurl)</td>
</tr>
<tr>
<td>63</td>
<td>0.59582</td>
<td>74.125.226.163</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>928</td>
<td>GET /videoplayback/id/veja5b5j20/itag92/source/yt_live_broadcast/sq/3011/file/s</td>
</tr>
<tr>
<td>66</td>
<td>0.66426</td>
<td>74.125.226.163</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>827</td>
<td>302 Found (text/html)</td>
</tr>
<tr>
<td>73</td>
<td>0.79807</td>
<td>74.125.9.146</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>982</td>
<td>GET /videoplayback/id/veja5b5j20/itag92/source/yt_live_broadcast/sq/3017/rateby</td>
</tr>
<tr>
<td>396</td>
<td>1.21265</td>
<td>10.0.0.101</td>
<td>74.125.9.146</td>
<td>HTTP</td>
<td>250</td>
<td>100 OK (application/octet-stream)</td>
</tr>
<tr>
<td>401</td>
<td>1.24678</td>
<td>10.0.0.101</td>
<td>74.125.226.163</td>
<td>HTTP</td>
<td>928</td>
<td>GET /videoplayback/id/veja5b5j20/itag92/source/yt_live_broadcast/sq/3012/file/s</td>
</tr>
<tr>
<td>405</td>
<td>1.30746</td>
<td>74.125.226.163</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>827</td>
<td>302 Found (text/html)</td>
</tr>
<tr>
<td>410</td>
<td>1.34801</td>
<td>74.125.9.146</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>982</td>
<td>GET /videoplayback/id/veja5b5j20/itag92/source/yt_live_broadcast/sq/3012/rateby</td>
</tr>
<tr>
<td>699</td>
<td>1.85702</td>
<td>74.125.9.146</td>
<td>10.0.0.101</td>
<td>HTTP</td>
<td>1094</td>
<td>100 OK (application/octet-stream)</td>
</tr>
<tr>
<td>707</td>
<td>1.89737</td>
<td>10.0.0.101</td>
<td>74.125.226.163</td>
<td>HTTP</td>
<td>928</td>
<td>GET /videoplayback/id/veja5b5j20/itag92/source/yt_live_broadcast/sq/3013/file/s</td>
</tr>
</tbody>
</table>

- **Frame 401**: 928 bytes on wire (7424 bits), 928 bytes captured (7424 bits)
- **Transmission Control Protocol**, Src: 10.0.0.101 (10.0.0.101), Dst: 74.125.226.163 (74.125.226.163)

Understand and comply with investigations.
Artifacts – Mobile Devices (Sources)

- Apple's iOS and Google's Android (mostly)
- Mobile device encryption is a significant challenge.
- Cellular, WiFi, Bluetooth, and NFC are unique forensic opportunities requiring additional skill.
- Apple's Find My and Google's Find My Device allow a lost or stolen phone to be remotely locked or wiped, which destroys vital evidence.
We **CANNOT** prevent all bad things from happening, so we **MUST** be able to **detect and respond**.
Intrusion Detection and Prevention

- Detection detects (passive), Prevention prevents (active)
- Network-based and host-based.
- **NIDS** – network-based intrusion detection.
- **NIPS** – network-based intrusion prevention.
- **HIDS** – host-based intrusion detection.
- **HIPS** – host-based intrusion prevention.
- Best used at crucial network chokepoints, such as the between the demilitarized zone (DMZ) and internal networks or between a VPN terminator and an internal network.
Intrusion Detection and Prevention

- Detection detects (passive), Prevention prevents (active)
- Network-based and host-based.
- NIDS – network-based intrusion detection.
- HIDS – host-based intrusion detection.
- HIPS – host-based intrusion prevention.
- Best used at crucial network chokepoints, such as the between the demilitarized zone (DMZ) and internal networks or between a VPN terminator and an internal network.

False positives and false negatives must be handled carefully. Called “tuning”.
Security Information and Event Management (SIEM)

- **Centralization** – centralizing log files keeps them organized and protects them.

- **Normalization** – logs from different systems come in different formats, a standardized format must be used for correlation and comparison.

- **Correlation and detection** – incidents often span systems, so logs/activities must be correlated for detection.

- **Alerting** – Specific events and/or incidents can be configured to alert administrators.
Security Information and Event Management (SIEM)

- **Centralization** – centralizing log files keeps them organized and protects them.

- **Normalization** – logs from different systems come in different formats, a standardized format must be used for correlation and comparison.

- **Correlation and detection** – incidents often span systems, so logs/activities must be correlated for detection.

- **Alerting** – Specific events and/or incidents can be configured to alert administrators.

**IMPORTANT:**
- Garbage in/Garbage out
- SIEM operates on rules, so the rules must be set correctly.
Continuous Monitoring

- Information Security Continuous Monitoring (ISCM).

Conduct Logging and Monitoring Activities

Continuous Monitoring
Continuous Monitoring

Information Security Continuous Monitoring (ISCM).

CISSP® MENTOR PROGRAM – SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Continuous Monitoring

- Information Security Continuous Monitoring (ISCM).
- Steps to establish, implement, and maintain ISCM:
  - Define an ISCM strategy;
  - Establish an ISCM program;
  - Implement an ISCM program;
  - Analyze data and Report findings;
  - Respond to findings; and
  - Review and Update the ISCM strategy and program.
- A robust ISCM program thus enables organizations to move from compliance-driven risk management to data-driven risk management.
Continuous Monitoring

- Information Security Continuous Monitoring (ISCM).
- Steps to establish, implement, and maintain ISCM:
  - Define an ISCM strategy;
  - Establish an ISCM program;
  - Implement an ISCM program;
  - Analyze data and Report findings;
  - Respond to findings; and
  - Review and Update the ISCM strategy and program.

A robust ISCM program thus enables organizations to move from compliance-driven risk management to data-driven risk management.
Egress Monitoring

• Firewalls (and other filtering devices) should not only be configured for ingress (inbound) traffic control and monitoring, but also egress (outbound).

• This identifies potential data exfiltration and C2C traffic.

• Data Loss Prevention (DLP) is largely built on the premise of egress filtering.

• DLP can also filter/alert on specific data patterns; XXX-XX-XXXX, XXXX XXXX XXXX XXXX, etc.
Log Management

• Log **strategy** is critical.
  • Why are we logging?
  • What should we be logging?
  • Where should we be logging?
  • What should trigger alerts and response?
  • Etc., Etc., Etc.

• CIS Benchmarks, DoD STIGs, manufacturer documentation, and specific standards can/should be all be leveraged.
Log Management - Define Auditable Events and Thresholds

• Log settings are/should be continually tuned.
• Important events to consider logging:
  • Successful and unsuccessful **access attempts** like system logins, file or data access, and application access
  • **Changes to user permissions**, especially escalation like using sudo or other admin privileges
  • **Changes to or disabling security tools and settings** like DLP
  • Copy or export of **sensitive files**
  • **Sensitive data transactions** performed in applications
Log Management - Define Auditable Events and Thresholds

- Important data to collect about the events:
  - User or process IDs
  - Timestamps, ideally in a standardized format like UTC or in a standardize time zone used by the whole organization
  - Device identifiers, hostname, IP address, or similar Name of object(s) accessed, like filename or function
  - Policy identifiers that triggered the log event, such as a failed login, admin privilege use, or file deletion
Log Management - Define Auditable Events and Thresholds

- **Important data to collect about the events:**
  - User or process IDs
  - Timestamps, ideally in a standardized format like UTC or in a standard time zone used by the whole organization
  - Device identifiers, hostname, IP address, or similar name of object(s) accessed, like filename or function
  - **Policy identifiers** that triggered the log event, such as a failed login, admin privilege use, or file deletion

DON’T forget to protect the log data, maintain it in compliance with data retention requirements, clipping levels, etc.
Threat Intelligence
Wikipedia has a good definition:

Cyber threat intelligence (CTI) is knowledge, skills and experience-based information concerning the occurrence and assessment of both cyber and physical threats and threat actors that is intended to help mitigate potential attacks and harmful events occurring in cyberspace. Cyber threat intelligence sources include open-source intelligence, social media intelligence, human Intelligence, technical intelligence, device log files, forensically acquired data or intelligence from the internet traffic and data derived for the deep and dark web.
Threat Intelligence - Threat Feeds

• Information about threats learned about from various sources according to industry, physical region, etc.

• Data can be used for threat hunting (looking for the specific threat in an environment), integration into other tools like DLP, SIEM, and SOAR.

• Commercially available (free and paid for) threat feeds and several government-sponsored ones (mostly CISA in the United States and the Canadian Centre for Cyber Security).

• Industry-specific groups known as information sharing and analysis centers (ISACs) also offer threat information to their members.
Threat Intelligence - Threat Feeds

- Information about threats learned about from various sources according to industry, physical region, etc.
- Data can be used for threat hunting (looking for the specific threat in an environment), integration into other tools like DLP, SIEM, and SOAR.
- Commercially available (free and paid for) threat feeds and several government-sponsored ones (mostly CISA in the United States and the Canadian Centre for Cyber Security).
- Industry-specific groups known as information sharing and analysis centers (ISACs) also offer threat information to their members.

The American Chemistry Council (ACC) represents a diverse set of companies engaged in the business of chemistry. An innovative, $553 billion enterprise, our mission is to deliver value to our members through advocacy, member engagement, political advocacy, information sharing, communications and scientific research. The Chemical Information Technology Center (ChemITC®) of the ACC is a forum for companies to address common IT, cyber security, and security issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC is committed to advancing the use of information technology to streamline processes, manage cyber threats, and improve decision-making. www.americanchemistry.com/
Threat Intelligence - Threat Hunting

- Seeking threats/threat actors in an environment, based upon known and unknown threats.
- Human analysts and/or software agents.
- Within an organization, can be strategic, tactical or operational.
- Outside of an organization, often done as part of security research, where a community of researchers share work and findings in the spirit of making everyone more secure.
- Details can be shared in social forums (blogs, conference talks, Twitter, etc.) and information like IoCs are integrated with security tools.
Threat Intelligence - Threat Hunting

Dark Web/Deep Web

**Dark web** – Content on non-publicly accessible networks requiring the use of special access methods like the Tor network.

**Deep web** - Content accessible over the internet but not publicly exposed, such as online banking information, private social media feeds, and even content behind paywalls like news sites.
User and Entity Behavior Analytics (UEBA)

Extends on an early type of cybersecurity practice – User Behavior Analytics, or UBA – which uses machine learning and deep learning to model the behavior of users on corporate networks and highlights anonymous behavior that could be the sign of a cyberattack.

Activities that deviate from expected activities (or baseline) are flagged as suspicious and can be used as an input to other security tools.
User and Entity Behavior Analytics (UEBA)

Extends on an early type of cybersecurity practice – User Behavior Analytics, or UBA – which uses machine learning and deep learning to model the behavior of users on corporate networks and highlights anonymous behavior that could be the sign of a cyberattack.

Activities that deviate from expected activities (or baseline) are flagged as suspicious and can be used as an input to other security tools.

CISSP® MENTOR PROGRAM – SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS

PERFORM CONFIGURATION MANAGEMENT
Also referred to as “CM”

The Theory:

• Start with a secure configuration, make only authorized and secure changes, then the asset is maintained in a secure state.
  
  • Items under CM are called Configuration Items (CIs).
  • CIs can be systems, endpoints, applications, etc.
  • The “secure configuration” of a CI is called a baseline.
  • Changes to the baseline must follow a formal change management process.

Cl sounds sexier than “Asset”?
The Two Meanings of CM

CM can be used for both configuration management and change management, which often leads to confusion as the two processes are inextricably linked but subtly different. Configuration management deals with identifying and maintaining the known good state of CIs, while change management deals with the request, approval, and implementation of changes to CIs from one secure baseline to the next.

Changes typically require the review of a change management board (CMB) or similar body, whose duty is to formally register a request for a change, assess the impact of the change, and grant approval if the proposed change does not negatively impact the security of the CI. Security practitioners should be one of the stakeholders in the CMB tasked with reviewing changes for security impact, and other stakeholders like finance and IT will also evaluate the change for cost or technology impacts.
Also referred to as “CM”

Roles and responsibilities, how CM will work, etc. should be documented in a **Configuration Management Plan**.

**Provisioning** – setup and deployment of the secure configuration (baseline).

- The CI must be entered into the **asset inventory**.
- Baseline, standard baselines include **DISA STIGs, CIS Benchmarks**, and/or **vendor-supplied** configuration information.
Also referred to as “CM”

Roles and responsibilities, how CM will work, etc. should be documented in a Configuration Management Plan.

• Provisioning – setup and deployment of the secure configuration (baseline).
• The CI must be entered into the asset inventory.
• Baseline, standard baselines include DISA STIGs, CIS Benchmarks, and/or vendor-supplied configuration information.
Also referred to as "CM"

Roles and responsibilities, how CM will work, etc. should be documented in a Configuration Management Plan.

- **Provisioning** – setup and deployment of the secure configuration (baseline).
- The CI must be entered into the asset inventory.
- Baseline, standard baselines include DISA STIGs, CIS Benchmarks, and/or vendor-supplied configuration information.

**CIS Benchmarks**

With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

Join a Community
Also referred to as "CM"

Roles and responsibilities, how CM will work, etc. should be documented in a **Configuration Management Plan**.

- **Provisioning** – setup and deployment of the secure configuration (baseline).
- The CI must be entered into the **asset inventory**.
- Baseline, standard baselines include DISA STIGs, CIS Benchmarks, and/or vendor-supplied configuration information.

---

**Security baselines**

Article • 02/09/2022 • 3 minutes to read • 9 contributors

**Using security baselines in your organization**

Microsoft is dedicated to providing its customers with secure operating systems, such as Windows and Windows Server, and secure apps, such as Microsoft 365 apps for enterprise and Microsoft Edge. In addition to the security assurance of its products, Microsoft also enables you to have fine control over your environments by providing various configuration capabilities.

Even though Windows and Windows Server are designed to be secure out-of-the-box, many organizations still want more granular control over their security configurations. To navigate the large number of controls, organizations need guidance on configuring various security
Insecure configurations are a **VERY** common cause of vulnerabilities and incidents. Use automation where possible.

Maintain the secure configuration through strict change management.
Also referred to as “CM”

Roles and responsibilities, how CM will work, etc. should be documented in a Configuration Management Plan.

- Provisioning – setup and deployment of the secure configuration (baseline).
  - The CI must be entered into the asset inventory.
  - Baseline, standard baselines include DISA STIGs, CIS Benchmarks, and/or vendor-supplied configuration information.

CISSP® MENTOR PROGRAM – SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS

APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

- 
- 
Need-to-Know/Least Privilege

Need-to-know and least privilege are often used interchangeably, but they are different,

- **Need-to-know** is data-driven. Does a person/subject need to know the information? Regardless of whether the person/subject has privileges.

- **Least privilege** is system-driven. Does the person/subject need this level of access to perform an authorized job function? Also called “minimum necessary access”.
Separation of Duties and Responsibilities (SoD)

Limits the potential for misuse of resources or malicious activities by separating process steps among multiple personnel.

The person requesting access must not be the same one authorizing access and/or granting access.

• **Dual control** - A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information.

• **Two-person integrity** - no single person can access an asset like a file or piece of equipment without another authorized individual present.
Separation of Duties and Responsibilities (SoD)

Limits the potential for misuse of resources or malicious activities by separating process steps among multiple personnel. The person requesting access must not be the same one authorizing access and/or granting access.

- **Dual control** - A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information.
- **Two-person integrity** - no single person can access an asset like a file or piece of equipment without another authorized individual present.

### Two-person integrity (TPI)

**Abbreviation(s) and Synonym(s):**
- TPI
- show sources

**Definition(s):**

The system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. Note: Two-Person Control refers to the handling of Nuclear Command and Control COMSEC material while Two-Person Integrity refers only to the handling of COMSEC keying material.

**Source(s):**

CNSSI 4009-2015 [Superseded] from NSA/CSS Manual Number 3-16 (COMSEC)
Privileged Account Management (PAM)

• Privileges, often called permissions, are the abilities a user is granted on a system.

• Privileged accounts (those with “elevate” privileges) require additional rigor during the access management lifecycle, such as more frequent reviews, MFA, limited use, etc..

• Provisioning, Use, Review, and Deprovisioning requirements must all be considered.
Job Rotation

• Two primary benefits
  • Cross-training which improves operational resilience.
  • Limits/mitigates internal fraud (and related)
    • Personnel are less-likely to engage when they know they rotate and
    • Fraud is more likely to be detected.
Service-Level Agreements

• Defines the level of service expected from a third party:
  • The metrics by which service is measured,
  • Remedies or penalties should agreed-on service levels not be achieved

• It is a critical component of any technology vendor contract.

• A mutual agreement of service level requirements (SLRs) is an SLA, which codifies the shared understanding of SLRs.

• SLAs should be monitored continually and should be part of third-party information security risk management.
DOMAIN 7 – SECURITY OPERATIONS
APPLY RESOURCE PROTECTION
Media Management

• Physical and electronic; paper, hard drives, devices, etc.
• ALL data should be classified as part of data management practices.
• Labeling and Marking is driven from data classification requirements, using the highest classification on the media.
Information Classification and Management Policy

Purpose

The purpose of the (Company) Information Classification and Management Policy is to provide a system for classifying and managing Information Resources according to the risks associated with its storage, processing, transmission, and destruction.

Audience

The (Company) Information Classification and Management Policy applies to any individual, entity, or process that interacts with any (Company) Information Resource.

Contents

Information Classification
Information Handling
Information Retention & Destruction

https://frsecure.com/information-classification-policy-template/
Information Classification and Management
Policy, version 1.0.0

Purpose

The purpose of the (Company) Information Classification and Management Policy is to provide guidelines for classifying and managing data, including storage, processing, transmission, and handling.

Audience

The (Company) Information Classification and Management Policy applies to any individual, entity, or process that interacts with any (Company) Information Resource.

Contents

- Information Classification
- Information Handling
- Information Retention & Destruction

https://frsecure.com/information-classification-policy-template/
Handling

• The labeling and marking communicates to the asset holder what the protection requirements are (based upon the classification).
Information Handling

• All Information should be labelled according to the (Company) Labelling Standard.

• Public:
  o Disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements.

• Internal:
  o Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
  o Must be protected by a confidentiality agreement before access is allowed.
  o Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
  o Is the “default” classification level if one has not been explicitly defined.

• Confidential:
  o When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
  o When stored on mobile devices and media, must be encrypted.
  o Must be encrypted at rest.
  o Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
  o Must not be transferred via unsecure communication channels, including, but not limited to:
Media Protection Techniques

Physical compromise is total compromise. RoT

**Transporting Media**

Encryption, hashing, and physical protections should all be considered. Physical protections should also include environmental controls.

**Sanitization and Disposal**

- Previously covered. Full disk encryption (FDE) is a mitigating control.
- Data must be securely overwritten and/or destroyed.
DOMAIN 7 – SECURITY OPERATIONS
CONDUCT INCIDENT MANAGEMENT
First, you MUST define what an “incident” is.

An **event** is something that happened.

An **incident** is something that happened an event with a negative consequence.
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, “tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents.”

Plenty of standards to draw from:

- ITIL framework incident management processes
- NIST Special Publication 800-61, “Computer Security Incident Handling Guide”
- ISO 27035, “Security incident management”
- ISACA, “Incident Management and Response”
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, "tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents."

Plenty of standards to draw from:

• ITIL framework incident management processes
• NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
• ISO 27035, "Security incident management"
• European Network and Information Security Agency (ENISA), "CSIRT Setting Up Guide"
• ISACA, "Incident Management and Response"

Information Security Incident Response Plan Template

A FREE resource from SecurityStudio
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, "tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents."

Plenty of standards to draw from:

- ITIL framework incident management processes
- NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
- ISO 27035, "Security incident management"
- European Network and Information Security Agency (ENISA), "CSIRT Setting Up Guide"
- ISACA, "Incident Management and Response"

Cheat Sheets

- CCPA Compliance Requirements Guide
- CMMC DOD Framework Guide
- Cybersecurity Terminology Guide for Schools
- Data Loss Prevention Best Practices
- Log File Monitoring and Alerting
- NY SHIELD Act Cheat Sheet
- Popular Password Manager Apps Security in 2020

Checklists

- Mergers and Acquisitions Cybersecurity Checklist
- Pre-vCISO Engagement Checklist

Incident Response Playbooks

- Business Email Compromise Response Playbook
- Compromised Credentials Response Playbook
- Lost or Stolen Laptop Response Playbook
- Malware Incident Response Playbook
- Ransomware Response Playbook
- Web Application Attack Response Playbook

Program Guides

- Incident Response Plan Template
- Incident Response Steps Checklist
- PCI SAQ Types Overview
- Preparing for a PCI Compliance Audit
- Preparing for Key IT Staff Turnover Guide
- Third Party Contracts Agreement Recommendations
- Why Remove Local Admin Rights
- You Want to Get Into Security?

Workbooks

- Incident Response Log Template
- PCI Guide Flowchart
- Ransomware Prevention Assessment
- Vendor Risk Management Classification Template
Information Security Incident Response Plan (IRP)

Document Name: %%ORGANIZATION%% Incident Response Plan (IRP)  
Version: 1.0.0

Status: 
☑ Working Draft  
☑ Approved  
☐ Adopted

Document Owner: %%ORGANIZATION%% %%%TITLE%%

Section/Context: Information Security Team Documentation  
Last Review Date: 1/23/2021

The %%ORGANIZATION%% Information Security Incident Management Plan has been developed in support of the mandates documented in the %%%ORGANIZATION%% Incident Management Policy. This plan contains the requirements for handling all information security incidents and is supported by additional procedural documents as required.
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next). The book, “tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents.”

Plenty of standards to draw from:
- ITIL framework incident management processes
- NIST Special Publication 800-61, “Computer Security Incident Handling Guide”
- ISO 27035, “Security incident management”
- ISACA, “Incident Management and Response”

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>1/23/2021</td>
<td>%FIRST, LAST%</td>
<td>Approved</td>
</tr>
</tbody>
</table>

Version History Requirements

Each time an official and authorized review of, or revision to, this document is made, the Version History must be updated. Updates to the Version History table must be made.

- **Version** – This is the version number of the document. The version number should be incremented with each review or revision, according to preference or other internal guidance. In general, version numbers are incremented as follows:
  - For **major changes**, increment the major version number (the first number to the left of the decimal) by one. For instance, from 1.00 to 2.00. Major changes typically include document section re-writes and additions.
  - For **minor changes**, increment the minor version number (the first number to the right of the decimal) by one. For instance, from 1.10 to 1.20. Minor changes are typically additions to document sections, grammatical changes, etc.
  - For **review changes**, increment the review version number (the second number to the right of the decimal) by one. For instance, from 1.00 to 1.01. Review changes are those where nothing in the document changed; however, it was reviewed as noted.

- **Date** – The date the version change was officially approved.
- **Name** – The person or department who made the document change.
- **Summary** – A short description of any/all changes made to the document. If necessary, reference a separate document where additional information is provided about the change(s).
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, “tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents.”

Plenty of standards to draw from:

- ITIL framework incident management processes
- NIST Special Publication 800-61, “Computer Security Incident Handling Guide”
- ISO 27035, “Security incident management”
- ISACA, “Incident Management and Response”

Incident Response Plan

Incident Definition
Definitions

Roles and Responsibilities
Service Desk
Incident Manager
Security Team
Incident Response Team (IRT)

Incident Response Process
Step 1: Report Event/Incident
Step 2: Log Event/Incident
Step 3: Triage Incident
Step 4: Assign Responsibility

High-Severity Incident Processes
Assembling the IRT
Step 1: Incident Validation
Step 2: Incident Communications
Step 3: Evidence Collection
Step 4: Containment
Step 5: Eradication
Step 6: Recovery
Step 7: Post-Incident

Appendix A - Definitions
Incident Types
Criticality
Sensitivity
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, "tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents."

Plenty of standards to draw from:

• ITIL framework incident management processes
• NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
• ISO 27035, "Security incident management"
• European Network and Information Security Agency (ENISA), "CSIRT Setting Up Guide"
• ISACA, "Incident Management and Response"

CISSP® MENTOR PROGRAM – SESSION NINE

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Appendix B – Information Security Incident Response Form

NOTE: All MEDIUM AND HIGH severity incidents must be logged using the Information Security Incident Response Form (below)

Section 1: Information Security Incident Response Form
(TO BE COMPLETED BY ORIGINATOR)

- Please complete as much of the form as possible.
- Contact the Service Desk or Security Team personnel to report the incident.
- The Security Team will assist if needed and assign an Incident Number

Incident Date: Click here to enter a date. Report Date: Click here to enter a date.
Incident Reported By: Click here to enter text.
Department: Click here to enter text.
Phone: Click here to enter text.

Form Completed By: Click here to enter text.
Department: Click here to enter text.
Phone: Click here to enter text.

Section 2: Incident Information
(TO BE COMPLETED BY ORIGINATOR)

Please be as descriptive as possible

Physical Location of the Affected Information Resource(s):
Click here to enter text.

Type of Incident (Check All That Apply):
- Denial of Service
- Intrusion
- Virus/Malicious Code
- System Misuse
- Technical Vulnerability
- Web Site Defacement
- User Account Compromise
- Hoax
- Network Scanning/Probing
- Internal/Employee Fraud
- Privacy
- Policy Violation
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, “tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents.”

Plenty of standards to draw from:

- ITIL framework incident management processes
- NIST Special Publication 800-61, “Computer Security Incident Handling Guide”
- ISO 27035, “Security incident management”
- ISACA, “Incident Management and Response”

Appendix E – Incident Response Chain of Custody Form

**Section 1: System/Hard Drive/Computer Details** (TO BE COMPLETED BY THE ORIGINAL ACQUIRER)

- Please complete as much of this section as possible.
- Each item taken into custody requires a new form
- The IRT will assist as needed and assign an Incident Number

<table>
<thead>
<tr>
<th>Incident #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Original Acquirer:  
Department:  
Phone:  

<table>
<thead>
<tr>
<th>Item #</th>
<th>Item Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Manufacturer:  
Model #:  
Serial #:  

**Section 2: Chain of Custody** (TO BE COMPLETED BY ALL PARTIES INVOLVED WITH EACH TRANSFER)

- Print form before proceeding to complete this section
- Fill in each field entirely
- If a field does not apply, enter “N/A” and initial

<table>
<thead>
<tr>
<th>Tracking #</th>
<th>Date/Tim</th>
<th>FROM</th>
<th>TO</th>
<th>Reason for</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>
# Appendix E – Incident Response Chain of Custody Form

## Section 1: System/Hard Drive/Computer Details

<table>
<thead>
<tr>
<th>Incident #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Please complete as much of this section as possible.
- Each item taken into custody requires a new form.
- The IRT will assist as needed and assign an Incident Number.

<table>
<thead>
<tr>
<th>Original Acquirer</th>
<th>Department</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item #</th>
<th>Item Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model #</th>
<th>Serial #</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Section 2: Chain of Custody

<table>
<thead>
<tr>
<th>Tracking #</th>
<th>Date/Tim</th>
<th>FROM</th>
<th>TO</th>
<th>Reason for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Name/Organization</td>
<td>Name/Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Signature</td>
<td>Signature</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next). The book, "tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents."

Plenty of standards to draw from:
- ITIL framework incident management processes
- NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
- ISO 27035, "Security incident management"
- European Network and Information Security Agency (ENISA), "CSIRT Setting Up Guide"
- ISACA, "Incident Management and Response"

### Examples of information security incidents
- Computer system intrusion
- Unauthorized or inappropriate disclosure of sensitive institutional data
- Suspected or actual breaches, compromises, or other unauthorized access to systems, data, applications, or accounts
- Unauthorized changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for university work) used to store private or potentially sensitive information
- Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

### Important

**Do NOT attempt to respond** to an information security incident unless you feel comfortable doing so. Some incidents appear to be inconsequential at first glance, but turn out to be quite significant.

If you need assistance, contact someone who has been trained on your specific incident response plan and/or procedures.

**Do NOT panic.** An efficient incident response is important, not necessarily quick. When people feel
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next). The book, “tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents.”

Plenty of standards to draw from:
• ITIL framework incident management processes
• NIST Special Publication 800-61, “Computer Security Incident Handling Guide”
• ISO 27035, “Security incident management”
• European Network and Information Security Agency (ENISA), “CSIRT Setting Up Guide”
• ISACA, “Incident Management and Response”

Conduct Incident Management

Mission Before Money

Incident Classification

Incidents are classified by how impactful they might be to the organization. Incident classifications are based upon the type of incident, the criticality of the system(s) affected, and the sensitivity of the information involved. If you completed Step 2, then the incident has been classified*

There are three classifications; HIGH, MEDIUM, and LOW. Each classification has its own requirements for handling.

<table>
<thead>
<tr>
<th>Classifications</th>
<th>IRT Notification</th>
<th>Formal Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>LOW</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>

*Classifications are assigned automatically, using the Incident Log.

Two critical facets of incident response are mandated as part of the incident classification; IRT Notification and Formal Response.

IRT Notification

The IRT must be notified of all HIGH severity incidents. An incident owner may determine that a LOW or MEDIUM severity incident should be reported to the IRT, but such notification is not required.

Formal Response

All MEDIUM and HIGH severity incidents require a formal response. A formal response is one that is documented (using the Incident Response Form).

Notification and Incident Ownership

Initial incident notification rules and ownership responsibilities are assigned based upon the classification of the incident. The table below represents who must be notified within which timeframe, and who becomes the “owner” of the incident.

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>Help Desk</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>1 - 2 Hours</td>
<td>N/A</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Not Required</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>Infrastructure Team</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>Less than 1 hour</td>
<td>Infrastructure Team</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Not Required</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>N/A</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>Less than 10 minutes</td>
<td>N/A</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Less than 1 hour</td>
<td>IRT</td>
</tr>
</tbody>
</table>

Incidents that are classified as LOW and MEDIUM do not require notification beyond the Help Desk and the Infrastructure Team.

Only HIGH severity incidents require notification of the Incident Response Team (IRT). The IRT must be notified of any HIGH severity incident within the time denoted under “SLA”; less than one hour.

The incident owner is responsible for all facets of the incident response from Preparation to Recovery. Please refer to the incident response plan for additional guidance regarding specific incident response processes, including Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Post-Incident Activities.

IMPORTANT

The incident “owner” is responsible for the response to the incident beyond the steps identified here.
Incident Management Plan

Incidents are classified by how impactful they might be to the organization. Incident classifications are based upon the type of incident, the criticality of the system(s) affected, and the sensitivity of the information involved. If you completed Step 2, then the incident has been classified.

There are three classifications; HIGH, MEDIUM, and LOW. Each classification has its own requirements for handling.

<table>
<thead>
<tr>
<th>Classifications</th>
<th>IRT Notification</th>
<th>Formal Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>LOW</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>

Classification is assigned automatically, using the Incident Log.

Two critical facets of incident response are mandated as part of the incident classification: IRT Notification and Formal Response.

IRT Notification

The IRT must be notified of MEDIUM severity incident.

Formal Response

All MEDIUM and HIGH severity incidents require a formal response. A formal response is one that is documented (using the Incident Response Form).

Notification and Incident Ownership

Initial incident notification rules and ownership responsibilities are assigned based upon the classification of the incident. The table below represents who must be notified within which timeframe, and who becomes the "owner" of the incident.

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>Help Desk</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>1 - 2 Hours</td>
<td>N/A</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Not Required</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**LOW**

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>N/A</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>Less than 1 hour</td>
<td>Infrastructure Team</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Not Required</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**MEDIUM**

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>N/A</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>Less than 10 minutes</td>
<td>N/A</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Less than 1 hour</td>
<td>IRT</td>
</tr>
</tbody>
</table>

**HIGH**

<table>
<thead>
<tr>
<th>Notification</th>
<th>SLA</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Immediate</td>
<td>N/A</td>
</tr>
<tr>
<td>Infrastructure Team</td>
<td>Less than 10 minutes</td>
<td>N/A</td>
</tr>
<tr>
<td>IRT Members</td>
<td>Less than 1 hour</td>
<td>IRT</td>
</tr>
</tbody>
</table>

Incidents that are classified as LOW and MEDIUM do not require notification beyond the Help Desk and the Infrastructure Team.


**IMPORTANT**

The incident "owner" is responsible for the response to the incident beyond the steps identified here.
Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, "tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents." Plenty of standards to draw from:

• ITIL framework incident management processes
• NIST Special Publication 800-61, "Computer Security Incident Handling Guide"
• ISO 27035, "Security incident management"
• European Network and Information Security Agency (ENISA), "CSIRT Setting Up Guide"
• ISACA, "Incident Management and Response"

Let me know if you want a copy of this…

AGENDA

• Introduction
• Justify With Logic
• Most Common Incident Response Myths
• Most Common Incident Response Mistakes
• Most Common Incident Response Questions
• The Best Laid Plans
Testing is mandatory.
Excellent training opportunities.
Improves response.
Can be used to integrate with other plans.
Incident Response - Reporting

Two messages, one internal and the other external.
Step 2: Incident Communications

There are two categories for incident communications: internal communications and external communications. To the greatest extent possible, all communications must be controlled and follow the need-to-know principle.

Internal Communications

Handled by the CIO, with backup support provided by the Legal Officer (LO).

Internal communications include the coordination and communication with other teams internal to %ORGANIZATION%, regionally and globally (if necessary). Use the information contained in Appendix D of this plan for contact methods and details.

Internal communications include, but may not be limited to:

- Executive management; regionally and globally.
- Information security management; regionally and globally.
- Service desk and support personnel; regionally and globally.
- Employees and contractors; regionally and globally.
External Communications

All external communications MUST be coordinated by and through the Public Relations/Marketing representative and the LO.

No personnel, including members of the IRT, are permitted to communicate with anyone outside the organization regarding any details of an information security incident without explicit authorization from the Public Relations/Marketing representative and the LO.

External communications include, but may not be limited to:

- Customers
- Media
- Other incident response teams external to the %ORGANIZATION%
- Software and support vendors
- Internet service providers
- Law enforcement
- Regulatory authorities and/or data protection agencies

The contact information for the various third-parties, or external entities, that may need to be contacted during or after the incident response should be maintained or compiled by the IRT as needed. At this point in the incident response process, external communications may not necessarily need to be established; however, an external communications plan should be initialized.

The IRT should discuss information sharing before an incident occurs to establish policies and procedures regarding information sharing. A failure in external communications could lead to additional disruption and loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes.

Media handling

All media communications MUST be coordinated by and through the Public Relations/Marketing representative and the LO.

The Public Relations/Marketing representative and/or LO should establish media communications procedures. The following actions should be considered:
CISSP® MENTOR PROGRAM – SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES
Defense-in-depth where controls are layered to serve both preventative and detective functions.
Defense - in-depth where controls are layered to serve both preventative and detective functions.

CISSP® MENTOR PROGRAM

DOMAIN 7 - SECURITY OPERATIONS

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Mission Before Money
Defense-in-depth where controls are layered to serve both preventative and detective functions.
Firewalls (review)

- **Static packet inspection** (stateless)
- **Stateful packet inspection**

- **Web application firewall (WAF) and API gateway** - Specialized network access control devices designed to handle specific types of traffic, unlike a generic firewall that handles all network traffic. WAFs and API gateways analyze traffic destined specifically for a web application or an application's API.

- **Host-based firewalls** - These are installed on a specific endpoint and use a ruleset specific to that endpoint.
Firewalls (review)

• **Next-generation firewalls (NGFW)** - These are more of a marketing term than a unique type of firewall. Combines network security services into a single device/system. Lower overhead and cost (maybe), but higher complexity in a single device (point of failure).

• **Security groups**: These exist in software defined networks (SDNs) and cloud environments and serve many of the same functions as a firewall.

Firewalls, security groups, and microsegmentation are useful access control devices in a zero-trust network architecture, where no part of the network is implicitly trusted.
Intrusion Detection Systems and Intrusion Prevention Systems

Nothing new to cover here.
Intrusion Detection Systems and Intrusion Prevention Systems

Nothing new to cover here.

IDS vs IPS

An IDS is for detecting and monitoring intrusions. It won’t take action on its own.

An IPS can decide whether to accept/reject packets (based on rules).

An IDS needs help from human being or automated system to interpret the results and decide whether to take action.

Both IDS and IPS analyze traffic and compare it to known threats.

An IPS needs to be updated to recognize the latest threats.

CISSP® MENTOR PROGRAM – SESSION NINE

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
**Whitelisting/Blacklisting**

Mostly changed to allowlisting and blocklisting.

<table>
<thead>
<tr>
<th></th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blacklists</strong></td>
<td>• Scale</td>
<td>• Quickly out of date</td>
</tr>
<tr>
<td></td>
<td>• Quick to deploy</td>
<td>• Resource intensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Will eventually fail to protect</td>
</tr>
<tr>
<td><strong>Whitelists</strong></td>
<td>• Every site is vetted</td>
<td>• Every site needs to be vetted</td>
</tr>
<tr>
<td></td>
<td>• Safer</td>
<td>• Scale</td>
</tr>
<tr>
<td></td>
<td>• Less frequent updates</td>
<td></td>
</tr>
</tbody>
</table>

#MissionBeforeMoney
Third-Party-Provided Security Services

• Pros and Cons

**Common services:**

• **Security Operations Center (SOC):** Full or partial SOC outsourcing can be useful to deal with the cost and complexity of building and running a 24x7 SOC operation.

• **Digital Forensics and Incident Response (DFIR):** look for orgs without bias.

• **Threat intelligence:** can provide useful information about threats that could target the organization and are often industry- or technology-specific.
Sandboxing

• Run code, observe and analyze and code in a safe, isolated environment on a network that mimics end-user operating environments.
• Designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code.

Honeypots/Honeynets

• Network-attached system as a decoy to lure cyber attackers.
• Used to detect, deflect and study hacking attempts to gain unauthorized access to information systems.
• A honeynet is a collection of honeypots.
Be careful with honeypots, entrapment versus enticement.

- Designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code.

**Honeypots/Honeynets**

- Network-attached system as a decoy to lure cyber attackers.
- Used to detect, deflect and study hacking attempts to gain unauthorized access to information systems.
- A honeynet is a collection of honeypots.
DOMAIN 7 – SECURITY OPERATIONS
IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT
Five crazy facts on exactly how much time is spent on debugging and code fixing in the software industry:

1. On average, a developer creates 70 bugs per 1000 lines of code (!)
2. 15 bugs per 1,000 lines of code find their way to the customers
3. Fixing a bug takes 30 times longer than writing a line of code
4. 75% of a developer’s time is spent on debugging (1500 hours a year!)
5. In the US alone, $113B is spent annually on identifying & fixing product defects
Five crazy facts on exactly how much time is spent on debugging and code fixing in the software industry:

1. On average, a developer creates 70 bugs per 1000 lines of code (!)
2. 15 bugs per 1,000 lines of code find their way to the customers
3. Fixing a bug takes 30 times longer than writing a line of code
4. 75% of a developer’s time is spent on debugging (1500 hours a year!)
5. In the US alone, $113B is spent annually on identifying & fixing product defects

Windows 10, 50MM LOC, 75,000 Bugs?!

The average car, according to KPMG, has over 150 Million lines of code in it.
A generic security patch process incorporating all stakeholders must include the following:

**Vulnerability detection** – Scanning, researcher, user reporting a bug, etc.

**Patch publication** - By the vendor or development team, once the vulnerability is verified and relevant code is written to address it.

**Evaluation** - Patch applicability by each organization's administrative personnel to determine if the patch is needed in each environment.

**Testing** - Ensure the patch won't introduce problems.

**Apply and Track** - Ensure the patch doesn't have a negative impact on functionality.

**Rollback** - If issues are encountered.

**Documentation** - Of the system including the patch, which becomes the
This is where we’ll stop for the night...
This is where we’ll stop for the night...

UNDERSTAND AND PARTICIPATE IN CHANGE MANAGEMENT PROCESSES

#MissionBeforeMoney
Homework:

• Catch up in your reading. You should be through (or at least beginning) Domain 7 soon.
• Take practice tests.
• Review at least two of the references we provided in this class (download for later use).
• Post at least one question/answer in the Discorder Channel.

See you Wednesday!
FRSecure CISSP Mentor Program

2023

Class #10 – Domain 7 (Part 2)

Ron Woerner