



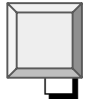
Introduction to Incident Response

Cybersecurity Boot Camp
Incident Response Day 1

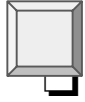


Class Objectives

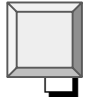
By the end of class today, students will be able to:



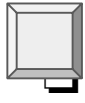
Define Incident Response and its purpose as it relates to cybersecurity.



Articulate typical Incident Response goals.



Define the purpose of a security operations center (SOC).



Evaluate whether or not to outsource an SOC depending on the specific needs of a company.

Introduction to Incident Response

Why do we need Incident Response

There are a lot of incidents out there...

Malware

DDoS and Botnet
attack

Phishing

Web Attacks

Data breach

Email Attacks

Attrition Attacks

Equipment Theft

Why do we need Incident Response

There are a lot of incidents out there...

Malware DDoS and Botnet attack Phishing Web Attacks

Data breach Email Attacks Attrition Attacks

Equipment Theft

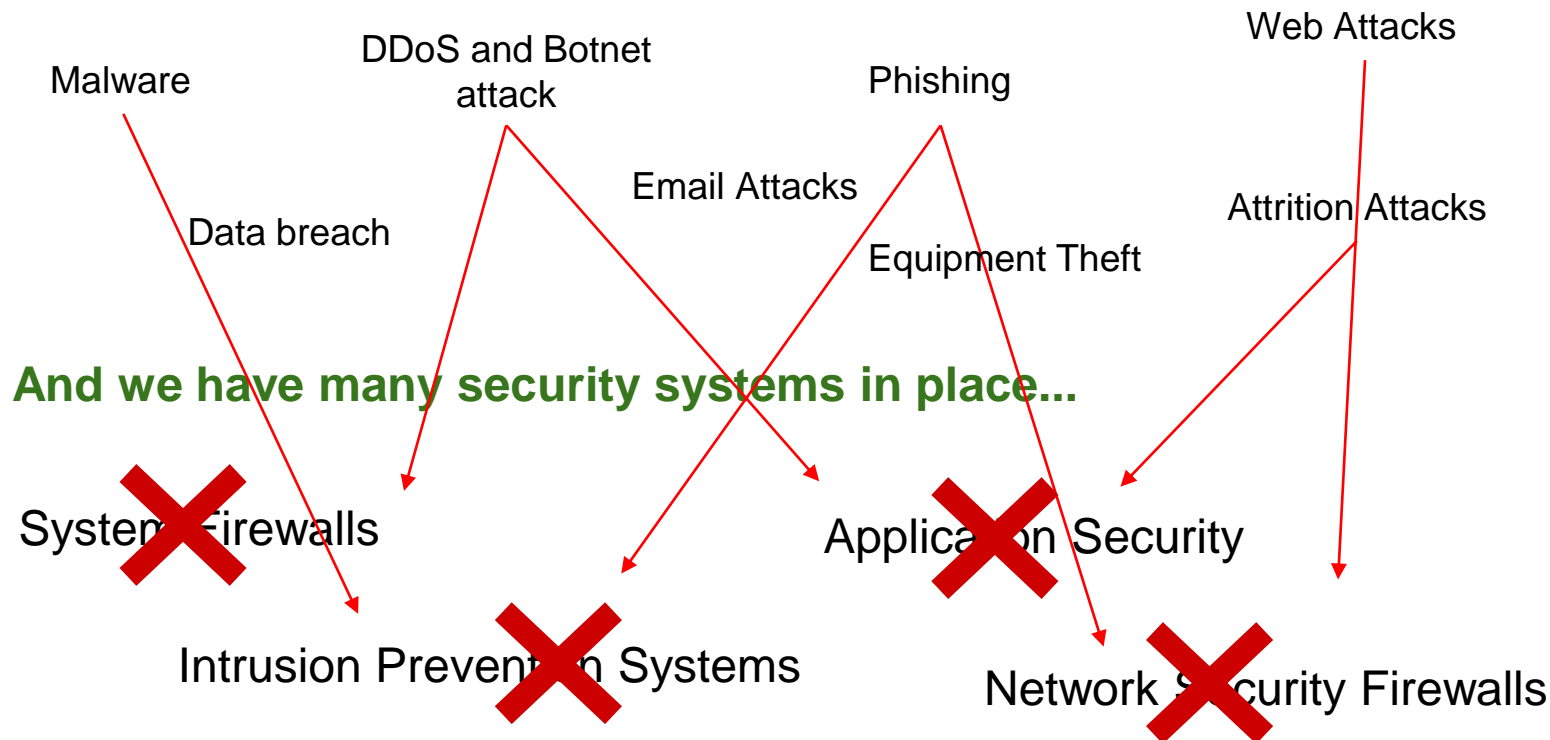
And we have many security systems in place...

System Firewalls Application Security

Intrusion Prevention Systems Network Security Firewalls

But sometimes those systems **fail**

There are a lot of incidents out there...





When security systems fail and a company is negatively affected by attacks, we call in the **Incident Response Team**.

Incident Response Plan

An **Incident Response Plan** is a formal, high-level document detailing how an organization will respond to security incidents and mitigate any damage caused by the incident.

Incident Response kicks in when these security systems **fail**.

- There is always a way into a system. Anything can be hacked given enough time.
- Incident response isn't focused on blocking bad actors. Instead, it's focused on locating and extracting them.

Incident Response

Analogy:

If a company was a **bank**, and the preventative security systems in place were the bank's **alarm** and **security guards**, and the threats and bad actors were **bank robbers**, then **incident response** would be the **police** responding ***after*** the alarm goes off and the robbers broke in.

Security Operations Center

An organization's **Incident Response Team** is the first responder to a security incident.

- They are in charge of setting up and implementing response plans that we will be covering today.
- The team often has their own operating location called a **Security Operations Center (SOC)**.



SOC Team Tier Structure

Security operation centers commonly have a three tier structure of analysts:

Tier 1

Tier 1 “Junior” analysts are the first responders and the first line of defense.

They are in charge of monitoring alerts and verifying that they are not false positives before escalating to Tier 2.

They follow pre-planned procedures, perform an initial investigation, solve simple incidents and escalate as needed.

Tier 2

Tier 2 analysts are the first 'escalation' point for the Tier 1 Analysts.

In other words, they help get past any blockers that the Tier 1 analyst may have.

They will go off the path of written procedures if necessary.

They support Tier 3 as well as monitor and creates procedures for Tier 1.

Tier 3

Tier 3 analysts are the second point of escalation and can provide a forensic / deep investigative role.

Tier 3 often owns the tools used by the IR team.

They oversee complex incidents and mentor/monitor the performances of lower tiers.

SOC Team Tier Structure

SOC Managers and Incident Handlers are also included as part of the SOC team.

- SOC Managers can perform all Tier 3 duties, as well as manage the whole team and provide Human Resources responsibilities for growing and maintaining a team.
- Incident Handlers function as project managers for complex incidents ensuring that technical investigators have all the resources they need.

A Tier 1 Analyst is an entry-level role that can serve as a good starting point for students who want to pursue this career path.

Monitoring Vs. Response

A “philosophical” debate regarding Security Monitoring and Incident Response:

Some companies separate monitoring and responding into two different teams.

- When the monitoring team notices a problem, they will escalate the issue to another team.

Other companies have only one team that provides both the monitoring and responding.

- The Monitoring Team watches activity occur over the wire while the response team investigates and mitigates suspicious activity

Regardless of how many team there are, they only monitor systems that provide alerts, such as SIEMs.

- Setting up and maintaining these systems are usually completed by a different team like **Security Engineering**.

Why We Care about IR

Remember this chart for the beginning of the course?

Sample (Entry-Level) Cybersecurity Titles			
Security Analyst	Security Operations Center (SOC) Analyst	Security Analyst	Systems Engineer
Cyber Threat Analyst	Cyber Defense Analyst	Incident Response Analyst	Intelligence Analyst
Information Assurance Technician	Risk Analyst	Forensics Investigator	Systems Administrator
Network Engineer	IT Auditor	Application Security Engineer	Penetration Tester
Information Analyst	Systems Security Analyst	IT Specialist	Web Engineer Application Security

Incident Response and SOC Professional Context

Incident Response is a great stepping stone or entry-level role in the cybersecurity field.

Sample (Entry-Level) Cybersecurity Titles			
Security Analyst	Security Operations Center (SOC) Analyst	Security Analyst	Systems Engineer
Cyber Threat Analyst	Cyber Defense Analyst	Incident Response Analyst	Intelligence Analyst
Information Assurance Technician	Risk Analyst	Forensics Investigator	Systems Administrator
Network Engineer	IT Auditor	Application Security Engineer	Penetration Tester
Information Analyst	Systems Security Analyst	IT Specialist	Web Engineer Application Security

Incident response and SOC consume a large percentage of an organization's security budget.

Incident Response Plans

Putting a Plan in Place

Before any incident or a response occurs, there needs to be a **plan**.

Every company should have a plan that documents exactly when to respond, what to do, how to do it, and who is in charge. The following terms are parts of the planning process:

Incident Response Plan: A formal, high-level document detailing how the organization will respond to incidents.

Response Procedure: Step-by-step workflow of a response. Often organized as a flow chart. This is the document that a junior analysts would follow when responding to events.

Putting a Plan in Place (cont.)

Response Playbook: A collection of procedures for a given type of incident. Often segmented into various procedures under different aspects of a response: Detect & Analyze; Eradicate & Recover; Post-Incident, etc.

Post-Incident Report: Overview of analysts' findings and specific actions taken against the incidents.

Tabletop exercise: A common exercise or drill in which a security team will discuss the detailed steps of responding to any given incident scenario.

Simple and Complex Incidents

Incidents will vary in complexity:

Simple Incidents	Complex Incidents
Simple incidents are usually opportunistic attacks that can be solved by junior analysts.	Require a more coordinated effort and have a higher severity. Usually involves multiple IR team members and / or multiple IT teams.
Examples include phishing attacks and malware downloads.	Examples include attacks that affects multiple employees and/or servers.



An incident responder are not expected to be an expert at everything. It is very common to call in specific expertise to assist in the response effort.

Incident Response Example

These are questions an IR plan should answer for a production web server incident:

- ☐ Do you immediately take the server offline and send a notification?
- ☐ Who makes the decision to shut it down?
- ☐ Do you need management approval to shut systems down?
- ☐ Who needs to be notified?
- ☐ Will it affect company revenue or customer experience?
- ☐ At what point do you involve the Public Relations department?
- ☐ At what point do you involve the legal team?
- ☐ Who communicates the issue with the executive team?

Incident Response Planning

Many different technical teams may be involved in the process:

- IR
- Security Engineering
- Security Management
- Security Compliance
- Technical Staff
- Legal, Human Resources and Public Relations
- Law Enforcement

Incident Response Plan

After the plan is in place...

Security teams should have **regular, scheduled exercises** to test response plans efficiency on non-production systems.

Organizations should also have regular **tabletop exercises** throughout the year. With each incident and exercise, the response should be evaluated and documented.

The ability to effectively execute a plan and make these decisions can be critical to a company's **bottom line**.

UnderArmour vs. Uber

The ability to effectively execute a plan and make these decisions can be critical to a company's **bottom line**.

UnderArmour reported a breach within a week of it occurring, letting all of their affected users know and mitigating any further damage to their reputation.

Uber, on the other hand, had to pay \$148 million because they tried to cover up a breach.



Activity: Interpreting IR Plans

In this activity, you will compare and contrast four incident response plans from different companies.

Activites/IRPlans

Suggested Time:
15 Minutes



Interpreting IR Plans Review

What type of industry / institution did each organization belong to?

- Homeland Security:
- Carnegie Mellon:
- The State of Oregon:
- Virginia Tech:

Interpreting IR Plans Review

What type of industry / institution did each organization belong to?

- Homeland Security: National Government
- Carnegie Mellon: Private University
- The State of Oregon: State Government
- Virginia Tech: Public University

Interpreting IR Plans Review

Which sections do most of the documents have in common?

Interpreting IR Plans Review

Which sections do most of the documents have in common?

- Introduction, Purpose and Scope
- Authority, Training, and Definitions
- Preparation, Detection and Containment

Interpreting IR Plans Review

While there are several common sections amongst the documents, these plans are quite distinct, each with unique topics to fit their specific needs:

Interpreting IR Plans Review

While there are several common sections amongst the documents, these plans are quite distinct, each with unique topics to fit their specific needs:

Themes where content differs for each organization:

- Executive Summary, Document Structure, Audience
- Insider Threats, Communications, Private Sector
- Access Control, Forensics, Escalation

Interpreting IR Plans Review

Did you find anything particularly interesting or useful?

Answers will vary.

Interpreting IR Plans Review

Homeland Security (National Government)

- This document is meant to be a framework, not a tactical or operational plan.
- Many departments follow this plan, including the Department of Justice, the FBI, the NCIJTF, and the DHS.
- This plan has a “Guiding Principles” section that affected parties should follow.
- This plan also distinguishes between “Cyber Incident” and “Significant Cyber Incident”.

Interpreting IR Plans Review

Carnegie Mellon (Private University)

- Carnegie Mellon has an entire “office” that is responsible for handling this document.
- Describes an “Event” as an exception outside normal operations.
- Mentions both personally identifiable information and protected health information.
- Carnegie Mellon calls their analysts “Incident Response Handlers”.

Interpreting IR Plans Review

The State of Oregon (State Government)

- The Oregon state plan seems less official than the National plan.
- There is a CISO position for the state of Oregon who is responsible for statewide information security.
- Oregon also has a position called an “Incident Commander” that seems to resemble an SOC Analyst role.
- Oregon keeps a full-time “Enterprise Security Office” (ESO) on staff whose primary focus is to analyze, but not detect incidents.

Interpreting IR Plans Review

Virginia Tech (Public University)

- VT has a checklist to follow Incident Handling.
- Addresses very specific attacks, like botnet DDoS attacks and ransom attacks.
- Includes a chart of the changes that occurred to the document.

Creating a Playbook

Class Activity: Creating a Playbook

Your outline should cover each of the following steps:

01

Preparation

02

Detection and Analysis

03

Containment, Eradication and Recovery

04

Post-Incident



Class Activity: Creating a Playbook

In this activity, we will create a playbook for a specific scenario and then compare it to the IR plans from the previous exercise.

Suggested Time:
20 Minutes



Creating a Playbook

Get creative setting up the scenario!

01

What type of company are we making a plan for?

02

What should we name the company?

03

What incident should we have the playbook address?

Creating a Playbook Example Review

1. Prepare

- Determine how to handle hardware and software
- System Documentation, network diagrams, baselines
- Clean OS and application images
- Specify who is monitoring and who is responding
- Specify the key stakeholders and their contact info

Creating a Playbook Example Review

2. Detect and Analyze

- Determine if an incident occurred
 - System logs and IDS / IPS system alerts
 - Anti-virus software alerts
 - Host-based monitor detecting configuration changes
 - Network traffic anomalies
- Document the characteristics and indicators of threats
- Determine the business impact
- Determine the incident priority

Creating a Playbook Example Review

3. Contain, Eradicate, and Recover

- System Isolation
- Disable breached user accounts
- Replace compromised files
- Determine which systems were affected
- Identify attack tools, methods, vectors, vulnerabilities
- Communicate with relevant teams
- Verify incident is removed with updated monitoring
- Recover affected systems or restore from backup

Creating a Playbook Example Review

4. Post-Incident

- Learn and improve
- Post-Incident meeting
- Review detailed time-stamp
- Re-evaluate IR plan
- Update system alert to make more accurate
- Review changes applied
- Update response workflow
- Document report

Take a Break!



The NIST Guide for Incident Response

The NIST Guide for Computer Security Incident Handling

The **NIST Guide** is the industry standard for Incident Response.

- It contains very detailed descriptions of plans and processes for specific incidents.
- Companies can also use the NIST standard as a framework for building out their own plans, only incorporating the items that make sense for them.
- Incident Response plans must be continually executed, assessed and updated in order to keep up with current threats.



Activity: The NIST Template

In this activity, you will use the NIST plan to assess the incident response plans we reviewed in the previous activity.

Activities/NIST

Suggested Time:
20 Minutes



NIST Template Review

A good IR Plan should include the following:

- ☐ Statement of management commitment
- ☐ Purpose and objectives of the policy
- ☐ Scope of the policy
- ☐ Definition of computer security incidents and related terms
- ☐ Organizational structure and definition of roles, responsibilities and levels of authority.
- ☐ Prioritization or severity ratings of incidents
- ☐ Performance measures
- ☐ Reporting contact forms



NIST Review

National Government (Homeland Security)

- Clear purpose (summary) and scope sections
- Includes definitions of incidents only (no related terms)
- A lot of organizational structure
- Includes a incident severity section
- No specific performance measures or KPIs

NIST Review

University (Carnegie Mellon)

- Clear Purpose, Scope and Definitions sections
- Organizational breakdown included
- No specific performance metrics mentioned

NIST Review

State Government (Oregon)

- Seems to jump right to organizational structure
- No specific “Scope” section
- Strong definitions section
- Good threat level chart

NIST Review

University (Virginia Tech)

- Has no “Purpose and Scope” sections
- Good organizational structure
- Includes some severity ratings of incidents
- No performance metrics mentioned.

SOC Team Metrics

SOC Team Metrics


Performance monitoring is very important in order to judge if a team is effective and to make any policy adjustment when necessary.

- Organizations call this measurement **metrics** or **Key Performance Indicators (KPIs)**.
- Metrics can assess the efficiency of the IR team as a whole, a particular tier, or even each specific member.
- The more metrics that an IR team keeps track of, the more they can drive improvements.

SOC Team Metrics

Some Common SOC team metrics:

- Mean time to respond to an incident (MTTR)
- Time from detection to resolution by analyst
- Time from detection to resolution by shift
- Percentage of incidents escalated to Tier 2 analysts
- Percentage of incidents escalated to Tier 3 or forensics analysts
- Percentage of false positives by system
- Percentage of recurring incidents by system
- Number of incidents handled by week/month/year



Is outsourcing an SOC to a third party
provider a valid security plan?

Is outsourcing an SOC to a third party provider a valid security plan?

Option 1: No Outsourcing

- Companies that have very complex monitoring and incident response teams will usually keep all SOC operations **in-house**.

Is outsourcing an SOC to a third party provider a valid security plan?

Option 1: No Outsourcing

- Companies that have very complex monitoring and incident response teams will usually keep all SOC operations in-house.

Option 2: Some Outsourcing

- Most common. Monitoring is outsourced by a Managed Security Service Provider (MSSP).
- Or some teams will only outsource complex incidents.
- What is outsourced is varied.

Is outsourcing an SOC to a third party provider a valid security plan?

Option 1: No Outsourcing

- Companies that have very complex monitoring and incident response teams will usually keep all SOC operations in-house.

Option 2: Some Outsourcing

- Most common. Monitoring is outsourced by a Managed Security Service Provider (MSSP).
- Or some teams will only outsource complex incidents.
- What is outsourced is varied

Option 3: All Outsourcing

- Full outsourcing is common for companies that prioritize security spending at the expense of robust monitoring, IR and SOC **facilities**.



Activity: To Outsource or not to Outsource

In this activity, you will work in groups to evaluate the pros and cons of outsourcing.

Your groups will invent a company and decide to which degree you will outsource its security operations.

Activities/ToOutsourceOrNot

Suggested Time:
20 Minutes



To Outsource or Not to Outsource Review

What company did you create? What was the budget? Which outsourcing option did you choose?

Option 1: No Outsourcing

- Do you need 24/7 coverage?
- How big is your SOC team?
- Does it make sense to have multiple tiers of teams?

Option 2: Some Outsourcing

- What will be outsourced and why?
- What will you keep in-house and why?
- Do you need 24/7 coverage?
- What teams will you have covering each aspect of security operations?

Option 3: All Outsourcing

- Is the budget your main reason for outsourcing?
- Will you outsource to another company, or just build an overseas team?
- Who will be in-charge or monitoring quality of outsourced services?

Class Objectives

By the end of class today, students will be able to:



Define Incident Response and its purpose as it relates to cybersecurity.



Articulate typical Incident Response goals.



Define the purpose of a security operations center (SOC).



Evaluate whether or not to outsource an SOC depending on the specific needs of a company.