**Student Name:** Coleton Sanheim **Weight: 3%**

**Student ID:** 000862545 **Marks: /**

# Module 10

# Security Operations

Table of Contents

[Introduction 3](#_Toc110199417)

[Instructions 3](#_Toc110199418)

[Scenario 4](#_Toc110199419)

[Chain of Custody 4](#_Toc110199420)

[Citation 5](#_Toc110199421)

# Introduction

Security operations encompasses many areas, including incident response, security controls, security events analysis, monitoring, change management, backup strategy, BCP and DR. An operation plan must be developed for each of these areas to address the operational tasks associated with them.

# Instructions

Develop an operation plan to handle the collection of evidence in an investigation of a corporate user’s Internet access through the corporate Internet firewall. The HR department can also request an Internet usage profile on an individual if the necessity arises (e.g., for a performance evaluation).

Provide one answer to each of the questions in the chain of custody below.

1. Who is the appropriate person to collect the evidence from the Internet firewall?

**A Forensic Analyst/Incident Response Team with oversight from chief security officer.**

1. What kind of information from the firewall can serve as evidence?

**Firewall logs that are recorded, assuming that the firewall was configured properly then it should log every connection and packet that passes through the firewall and that should be the main source of information collected. This information can include IP/MAC addresses, ports, type of data transferred.**

1. When should the evidence be collected from the firewall?

**It should be collected immediately after an incident. If not responding from an incident, firewall logs should be archived regularly and able to be referenced should the need arise.**

1. Where should the evidence be collected (from which security device)?

**The information should be collected from every security device that was involved or potentially exposed from an incident.**

1. How should the evidence be collected to ensure its confidentiality and integrity?

**Evidence collection should adhere to all standard procedures outlined by company policy and rule of law, and these standards need to be upheld during every step in Chain of Custody.**

# Scenario

A medical supply company has been the target of a ransomware attack, the attackers managed to gain access via a phishing email that installed a worm into the internal servers and encrypted all of the company’s data.

# Chain of Custody

The Chain of Custody starts with asking 5 questions:

Who is taking the evidence?

* It is important that the right people with the right training and authority are the ones taking the evidence

What is being taken as evidence?

* It is important that relevant information is being taken and irrelevant information is not.

When was the evidence taken?

* Evidence should be taken immediately after an incident

Where was the evidence taken?

* Evidence should only be taken from the affected infrastructure

How was the evidence collected?

* Ensuring that evidence is properly collected will prevent potential legal issues

Once these 5 questions have satisfactory answers, the next step is conducting interviews of the suspects. Ensure that legal counsel is present and that you are recording when conducting interviews to avoid any potential legal problems. Ensure that all laws surrounding interviews are upheld so that no evidence is invalidated against the suspect.

Finally, Reporting and Documenting is the final, most important step. Whoever responded to the incident should immediately begin recording all information and every action taken. Ensure that all records are timestamped and signed by the investigator to ensure data authenticity. When reporting, the incident response team should propose based on what they found, suggestions to improve the infrastructure that was affected so to avoid a repeat incident in the future.

# Citation

ITSC308\_M10-LEC-R01 PowerPoint, as reviewed in class.