Table of contents

Overview Page 3

Cybersecurity Risk Assessment Page 4

Vulnerability Matrix Page 12

Incident Response Plan Page 13

I. Roles and Responsibilities Page 14

II. Incident Response Reports Page 17

III. Incident Response Checklist Page 21

Service-Level Agreement Page 23

I. Operating System Protections Page 23

II. Service-Level Agreement (SLA) Page 25

III. Service Description Page 25

IV. Service Level Agreement (SLA) Evaluation Page 27

FVEY Indicator Sharing Report Page 30

I. Intrusion Detection and Prevention (IDS/IPS) Systems Page 32

II. Best Practices for Database Protection Page 36

Final Forensic Report Page 38

I. Network Attack Techniques Page 40

II. Computer Forensic Tools Page 42

References Page 44

Overview

Fifteen days ago, the United States reported, a successful data exfiltration had been detected in their intrusion detection system. As part of FVEY, Canada has conducted a comprehensive forensic analysis, and priority has been given to this data exfiltration because it has occurred on the nation's intrusion detection system that is hosting the international summit. Additionally, each nation's server at the summit is also at risk, with possibility of various attacks such as denial of service, and buffer overflows based on the United State's reported anomalous pattern of network traffic observed.

Although all members of FVEY who are at the Summit are regarded as allies, it is common knowledge amongst all FVEY partners that each nation is collecting intelligence and acquiring big data on the cyber-activity of each nation. Furthermore, some nations have been known to use this intelligence strategically to progress the individual nation's needs above the collective goal of the FVEY partners. In addition to Canada, all nations will be presenting to the CISO, a comprehensive analysis of their respective systems.

This deliverable will detail the identified vulnerabilities within Canada's respective systems, as well as possible risk mitigation policies and procedures that can be instated to minimize any further data breaches The Cybersecurity Risk Assessment will detail the possible attack vectors Canada and other summit nations have encountered, as well as the limitation both physically such as seven year old hardware, and lack of sufficient physical security on the premise to guard the servers, as well as systemic such as Linux operating systems that Canada does not maintain updates or the latest versions of. Additionally, this deliverable will present to the CISO, Canada's Service-Level Agreement (SLA), in order to determine what this attack's impact is to FVEY nation's cost and services rendered. In conclusion, a Final Forensic Report

has been included in this deliverable to display to the CISO the results of an end-to-end forensic investigation that analyzed all features and elements of the data exfiltration attack.

Cybersecurity Risk Assessment including Vulnerability Matrix




CURRENT SECURITY MEASURES AUTHENTICATION, AUTHORIZATION, & ACCESS CONTROL
1. People
Physical Security
Education/Training- Threat Awareness and Response
Network Monitoring
Device Accountability


CURRENT SECURITY MEASURES AUTHENTICATION, AUTHORIZATION, & ACCESS CONTROL
2. Technology
Hardware Security
Authentication Devices
Intrusion Detecting Software
Firewall
Network Monitoring

CURRENT SECURITY MEASURES AUTHENTICATION, AUTHORIZATION, & ACCESS CONTROL

3. Policy

Acceptable Use Policy

Password Management Policy

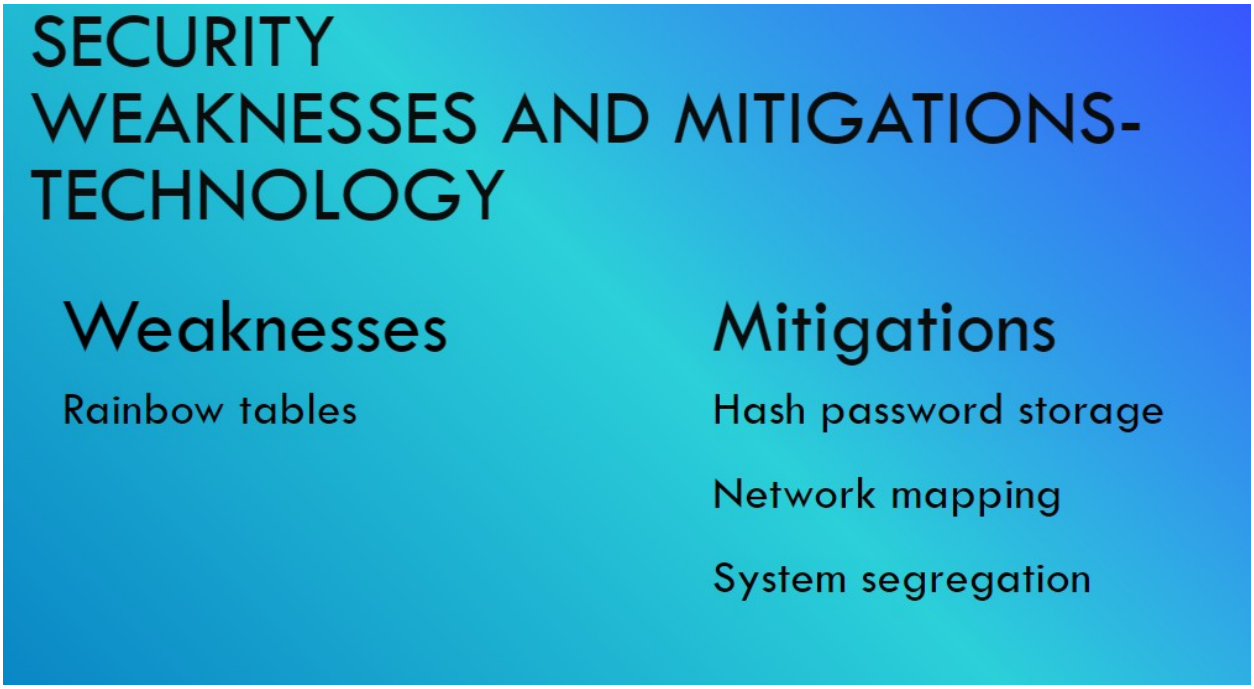
Access Control Policy

Remote Access Policy

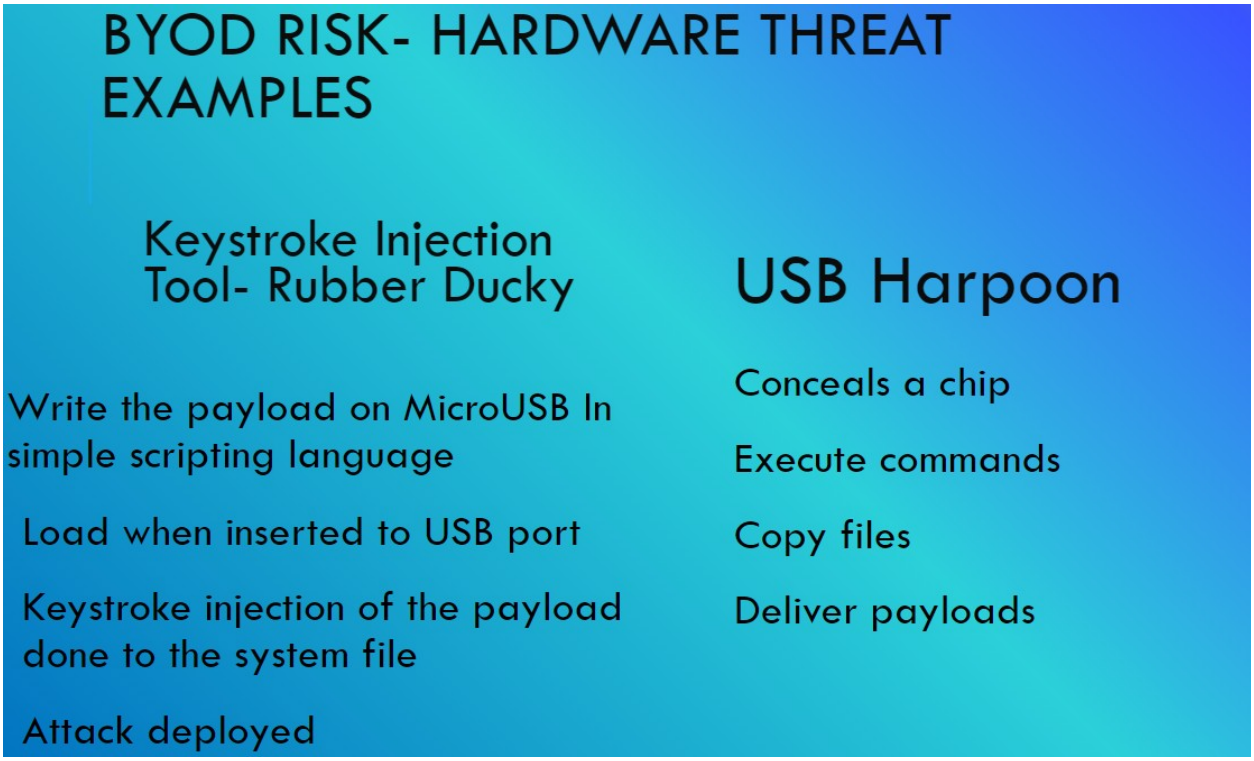
Email/Communication Policy

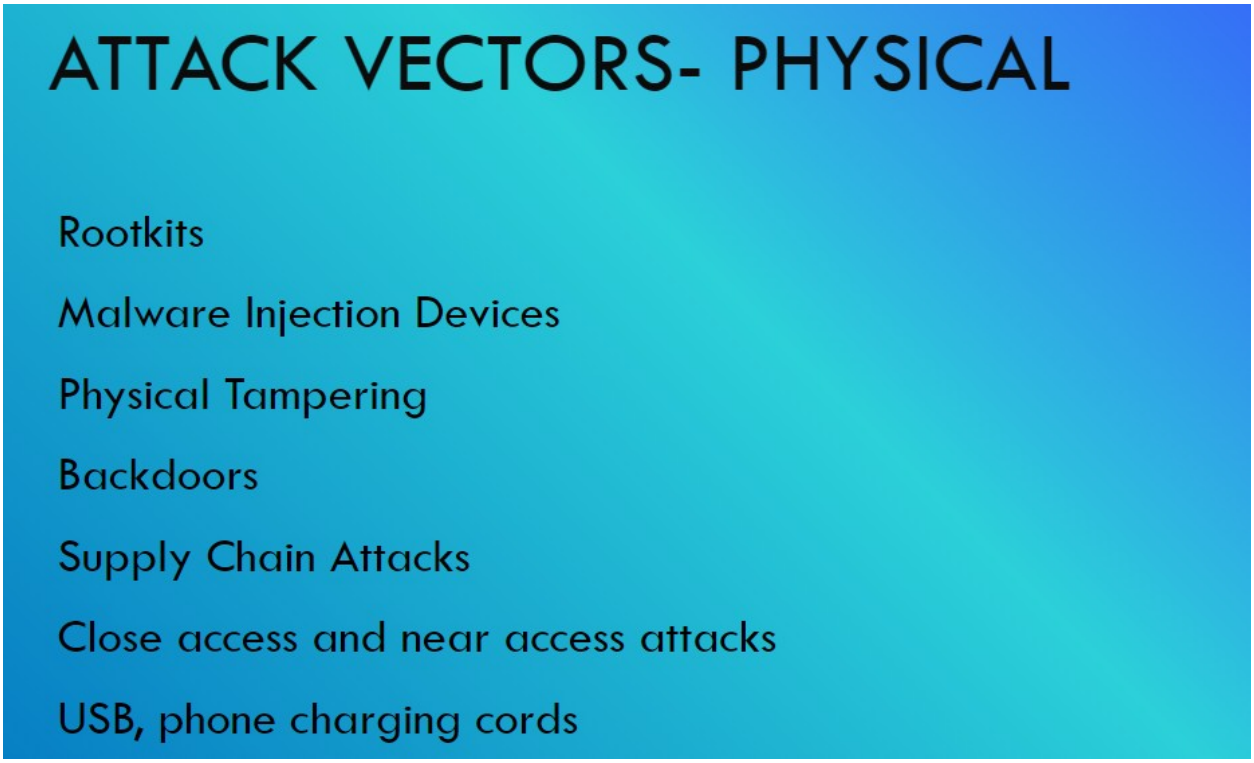
SECURITY WEAKNESSES AND MITIGATIONS- PEOPLE (HUMAN FACTOR)

Weaknesses	Mitigations
Poor password choices	➢ Password creation techniques and guidelines
Social engineering and phishing attacks (emails)	➢ Awareness training ➢ Teach users to think like an attacker


SECURITY WEAKNESSES AND MITIGATIONS-TECHNOLOGY
Weaknesses
Rainbow tables
Mitigations
Hash password storage
Network mapping
System segregation


SECURITY WEAKNESSES AND MITIGATIONS-HARDWARE
Weaknesses
Evolving Technology
Misconfiguration
BYOD
Malicious Devices
Mitigations
Firmware updates and vendor support
Sandboxing
Software Updates and vendor support
Software patch management
Penetration Testing


BYOD RISK- HARDWARE THREAT EXAMPLES
Keystroke Injection Tool- Rubber Ducky
Write the payload on MicroUSB In simple scripting language
Load when inserted to USB port
Keystroke injection of the payload done to the system file
Attack deployed
USB Harpoon
Conceals a chip
Execute commands
Copy files
Deliver payloads


ATTACK VECTORS- PHYSICAL
Rootkits
Malware Injection Devices
Physical Tampering
Backdoors
Supply Chain Attacks
Close access and near access attacks
USB, phone charging cords

ATTACK VECTORS- DIGITAL

Malware Proliferation

Email Attachments

Supply Chain Attacks

Backdoors

ATTACK VECTORS- PEOPLE

Social Engineering

Webpage

Poor Credential Management

POSSIBLE ATTACK VECTORS IN THE SUMMIT

Anomalous network activity was detected in the entire network of FVEY so all the team are affected.

Possible attack vector paths are considered.

SERVER

Canada`s hardware is 7 years old, so does not have the security construction of recent years.

Conventional Basic Input/Output System (BIOS)→ Is susceptible to attacks.

Uses HP Sure Start.

POSSIBLE ATTACK VECTORS IN THE SUMMIT

Using Linux operating system. Since it is open-source attackers can exploit easily.

C programming in Linux→ prone to buffer overflow.

Canada's server is 3 months behind the latest version.

Software: One application is prone to DoS attack. It needs to be patched.

Since all 5 teams are affected the server and software is not likely to be the cause.

POSSIBLE ATTACK VECTORS IN THE SUMMIT

HUMAN FACTOR is suspected.

Social engineering is most likely.

Uploaded malware via USB flash drives to all servers physically or an upload attacking the entire network by a member participating in the summit.

Trojan Attack that created a backdoor. Possibly from email phishing.

RECOMMENDATIONS- ACCEPT RISK OR MITIGATE IMPACT

Policy- Mitigate

- Policy Risks can be mitigated
- Constant reassessment of threat environment
- A rule imposed is a rule opposed
- Enforcement





Vulnerability Matrix

VULNERABILITY MATRIX

Risk= (Vulnerability * Threat * Impact)	Vulnerability	Categorization	Threat	Date Published and Last Revised	Attack Vector	Impact and Assessment (Low, Medium, High)	Mitigation
Current Risks https://nvd.nist.gov/	Server Hardware: The server hardware is seven years old and thus does not have some of the newer hardware securities that have been introduced in recent years.	Technological Factor	This can impact the server's integrity if an attacker is able to reboot the machine.	2/5/21	DDoS	High	An effective way to ensure a secure start up that has gained popularity is HP Sure Start.
	TPM: A notable missing hardware component is a Trusted Platform Module.	Technological Factor	Without a TPM, important artifacts must be stored in software and can be obtained more easily by an attacker.	2/5/21	Malware	High	Installation of a TPM to ensure encrypted storage of important passwords and certificated.
	Canada's server at the summit is using a Linux operating system, an open-source OS that is commonly used on servers. While the operating system has become more robust over time due to community effort, there are still weaknesses found very often.	Technological Factor	Because the source code is available to the public, a resourceful attacker could potentially identify a weakness to exploit by observing how the operating system is designed to handle specific scenarios.	2/5/21	Malware/Ransomware	High	Canada's server is about three months behind the latest version of Linux, making it vulnerable to recently discovered exploits. The latest version of Linux must be installed and updated continuously to mitigate this risk.
	Unauthorized Device Use	Human Factor	Canadian government employees may inadvertantly open the secure network to malicious attackers without authorized device use policy	2/5/21	Malware	Medium	Instate proper use policy.
	Intrusion	Technological Factor	All servers are physically located at the Global Economic Summit and physical security has not been entirely reliable.	2/5/21	Trojan	High	Increase barrier to entry standards at Global Economic Summit to heighten security levels at server location.
	Backdoor identified on the server.	Technological Factor	A backdoor was found on the server which allows the attacker to gain access to the server whenever they like.	2/5/21	SQL Injection Attack	High	Frequent data backup procedure and security audit to identify possible backdoors created internally.
Emerging Risks	Regarding application software running on the server, security updates are also key to reducing vulnerabilities. Updates for third-party applications must be installed as soon as they become available.	Technological Factor	An assessment of custom software revealed that one application is susceptible to a Denial of Service (DoS) attack	2/5/21	DDoS	High	Patch update and regular vulnerability assessment on application software.
	Theft/Lost Device	Technological Factor	Unaccounted for device could contain stored access credentials which a malicious entity could then copy and use.	2/5/21	Physical Security	Medium	Instate physical access controles such as key pads that require scanning to enter and more importantly to leave any facility housing proprietary devices.
SECURITY ARCHITECTURES							
The Canadian Government has instated Bill C-59 which is an amalgamation of regulations that present a security framework/architecture for Canadian organization's to adhere to. Bill C-59 part 4 amends the Candadian Security Intelligence Service Act to enhance accountability, Bill C-59 part 5 amends the Security of Canada Information Sharing Act to clarify when information can be disclosed, and Bill C-59 part 2 enacts the Intelligence Commissioner Act which outlines the duties and functions of the Intelligence Commissioner (Parliament of Canada, 2019).							
References							
HP. (2019). HP Sure Start. Retrieved from http://h10032.www1.hp.com/ctg/Manual/c06216928 Malwarebytes. (2021). Backdoor computing attacks. Retrieved from https://www.malwarebytes.com/backdoor/							
Trusted Computing Group. (2021). Trusted Platform Module (TPM) Summary. Retrieved from https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/#:~:text=TPM%20(Trusted%20Platform%20Module)%20is,(your%20PC%20or%20laptop).							
Parliament of Canada. (2019, June 21). Bill C-59. Retrieved from https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent							

Incident Response Plan

With the world's advancing technologies and access to the globe via the internet, organizations should have a good Incident Response Plan (IRP), for detection, respond, eradicate, and recover from cybercrimes. The IRP is extremely important, due to the fact if an organization does not prepare for a cyber-attack, cyber threats have the potential to breach your organization and completely halt operations. A well-designed IRP will detect incidents, contain loss and damage, mitigate exploited vulnerabilities, and restore an organization's infrastructure, which is essential for survival. A network breach being large or small, organizations still need to react to the incident and take all incidents seriously. Incident response planning should focus and layout specific definitions of breaches, and the roles and responsibilities of the cybersecurity

team for handling the breach, and the next steps taken following the breach, to address a security incident.

Roles and Responsibilities

Is basically an IT cybersecurity group with the responsibility of preparing and resolving organizational emergencies from cyber-attacks. The IRT is responsible for developing a detailed incident response plan, constant testing, monitoring, and resolving system vulnerabilities, while following cybersecurity best practices and for all cyber incidents within the organization. The team members should always be updated on new or upcoming cyber threats and should inform the workforce of the mitigations involving these threats. The team lead should be highly trained in cybersecurity and focused on the IRP. He or she is responsible for following up with specific cyber incidents, and what is the potential impact to the organization. The IRT responsibilities would include, developing and delivering IRP, provide incident updates, stay up to date on current threats, create employee awareness training, and deliver final incident reports to leadership, among many other phases of the listed in the IRP. Some other responsibilities of the team lead are as follows: (Murphy, 2019)

- Help develop and deliver the initial Incident report to leadership.
- Interact with leadership on all updates of an incident investigation.
- Organize any Computer Forensics and Data Recovery during an incident investigation.

Phases of Incident Response

The IRP should be a written detailed plan with 6 specific phases guiding the cybersecurity team to recognize and respond to a cyber-attack or data breach. Each phase of the plan should be updated, and organized to brief leadership, and well as mitigating the threat to employees. The following are the 6 specific steps making up the IRP. (ELLIS, n.d.)

- **Preparation** - developing scenarios and periodically schedule mock data breaches to evaluate the IRP. Make sure training is done regularly, and funding has been planned.
- **Identification –** figure out where or if you have been breached.
- **Containment** - contain the breach so it does not spread and cause further damage and use the evidence to create a plan for this type of incident not to happen in the future.
- **Eradication/Mitigation –** find the root cause of the breach and eliminate it. Develop mitigations.
- **Recovery –** restoring effected devices after the attack.
- **Lessons Learned**

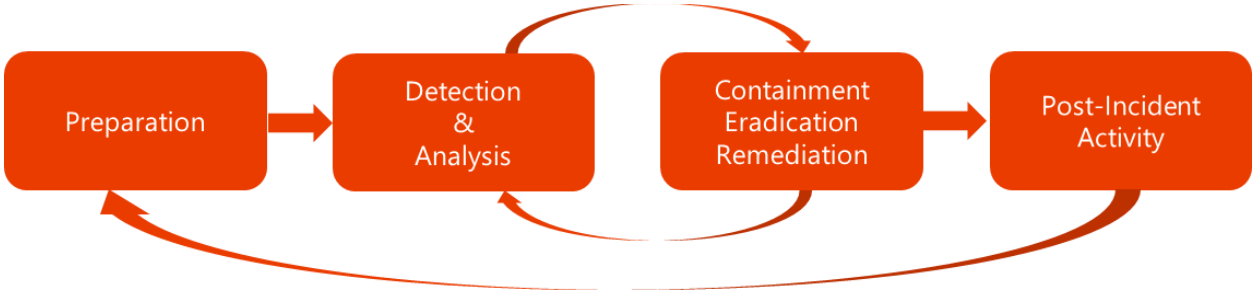


Figure 1- NIST Incident Response Lifecycle

Triggering Conditions for Actions

Protecting an organizational network, you must implement a robust set of policies and procedures that would contain threats. This can be accomplished through an Intrusion Detection and Prevention System (IDPS). An IDS generates alarms when it detects intrusive activity on the network, based on different types of network activity. The two most common triggering mechanisms are:

- Anomaly detection
- Misuse detection

When deciding which IDPS is needed, there are 4 typical types of IDPS as defined by NIST: (NIST, 2012)

- **Network-Based IDPS** - monitors network traffic for specific network segments and devices while analyzing the application protocol activity to identify suspicious and abnormal activity.
- **Wireless IDPS** - monitors wireless network traffic and analyzes it to identify suspicious activity involving networking protocols.
- **Network Behavior Analysis (NBA) System** - examine network traffic to identify threats that generate unusual traffic flows (e.g., malware, DDoS attacks, and policy violations).
- **Host-Based IDPS** - monitor a single host, and the events occurring within that host for suspicious activity.

Triggering Conditions for Closure

Following an IDS detection, the incident response plan should support a strong emphasis on containment, eradication, and recovery from an incident. Containment after an incident is crucial before the incident increases damage to the network. This will provide time for developing tailored mitigation for the incident, as well as define acceptable risks when developing strategies. These strategies will differ depending on the type of incident, such as the with an email containing malware will be handled much different than a DDoS attack on the network. Organizations must develop and document distinct containment strategies for each major incident type.

After containment of an incident has been successful, eradication and recovery are the next steps. Eradication can be a simple has deleting malware/spyware or removing access to

certain user accounts. During this process, it is important you hit all the areas where the incident had occurred. In the recovery phase, the cybersecurity team must restore systems to normal operation, and then confirm that the systems are functioning normal. This phase can be the changing of a password, restoring systems from backup drives, or can be extensive as building affected systems from scratch. (NIST, 2012)

Incident Response Reports

A necessary aspect of the incident response is the documentation during and after the incident occurred. Documenting each incident can be beneficial for the future. These reports will provide a reference if this incident should occur again. Creating chronology of events along with times of events, are important for legal aspects, as well as damages costs. When documenting the incident, organizations must decide what incident data to collect based on reporting requirements and what and how to use the data in the future. Examples of what to document: (Johnson, 2020)

- Incidents Handled
- Time
- Objective Assessment of Each Incident
- Subjective Assessment of Each Incident

Tools, Techniques, and Technologies

There are many tools available, and many of these tools are open source. NIST has mentioned basic tools needed for incident assessments, but there is an extensive number of different tools to use, such as: (att, n.d.)

- **Log Analysis, Log Management, SIEM -** OSSIM (open-source security information management)
- **Intrusion Detection Systems (IDS)** – Snort, BroIDS
- **Netflow Analyzers** – Ntop, Nfdump

- **Vulnerability Scanners** – Qualys, OpenVAS
- **Monitoring** – Zeek, Nagios
- **Web Proxies** - Squid Proxy, IPFire
- **Asset Inventory** - OCS Inventory, SolarWinds

Communications and Parties Involved

During the incident response process, the cybersecurity team needs to communicate and notify the appropriate people who need to be involved. The Incident response policies should include these provisions and they must be followed. The communications will involve the initial incident and go to the final mitigations. Communication to the follow should occur:

- CIO
- Cybersecurity Team Lead
- Information security officer
- Incident response team members
- External incident response teams
- System owner
- Human resources
- Public affairs
- Legal department
- US-CERT (required for Federal agencies)
- Law enforcement

Security Controls and Tracking

In the NIST Special Publication 800-53, it lists the Incident Response Security and Privacy Controls for organizations. Some areas to focus on are: (Torino, n.d.)

- **IR-4**: Incident Handling
- **IR-8**: Incident Response Plan
- **PL-8**: Information Security Architecture
- **PM-16**: Threat Awareness Program
- **CA-2**: Security Assessments
- **CA-7**: Continuous Monitoring
- **SI-4**: Information System Monitoring
- **SI-5**: Security Alerts, Advisories, and Directives

No.	Control	Priority	Low	Moderate	High
IR-4	INCIDENT HANDLING	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-8	INCIDENT RESPONSE PLAN	P1	IR-8	IR-8	IR-8
PL-8	INFORMATION SECURITY ARCHITECTURE	P1		PL-8	PL-8
CA-2	SECURITY ASSESSMENTS	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-7	CONTINUOUS MONITORING	P2	CA-7	CA-7 (1)	CA-7 (1)
SI-4	INFORMATION SYSTEM MONITORING	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	P1	SI-5	SI-5	SI-5 (1)

Incident Response Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Figure 2 - NIST Incident Response Checklist

Network Protection and Integrity Checks

Implementing protection and integrity controls within the network ensures valid data and rejects invalid data inputs, unauthorized data outputs, protects data and programs from malicious attacks. The main purpose of integrity controls is to ensure transactions occur correctly and securely. A few simple preventative controls can be implemented:

- Strong cybersecurity policies

- Intrusion detection systems (IDS) / Firewalls
- Annual IRP training for employees
- Access Controls
- Hashing

It is the responsibility of leadership to ensure that these steps are taken and enforced. Cybersecurity personnel can safeguard company data by continually assessing system vulnerabilities, determining potential threats, and performing penetration testing, cyber forensics, and system audits. Cybersecurity is an emerging area, one that organizations should embrace as vital part to their core values of the organization. (Murphy G. , 2019)

Swimlane Diagram

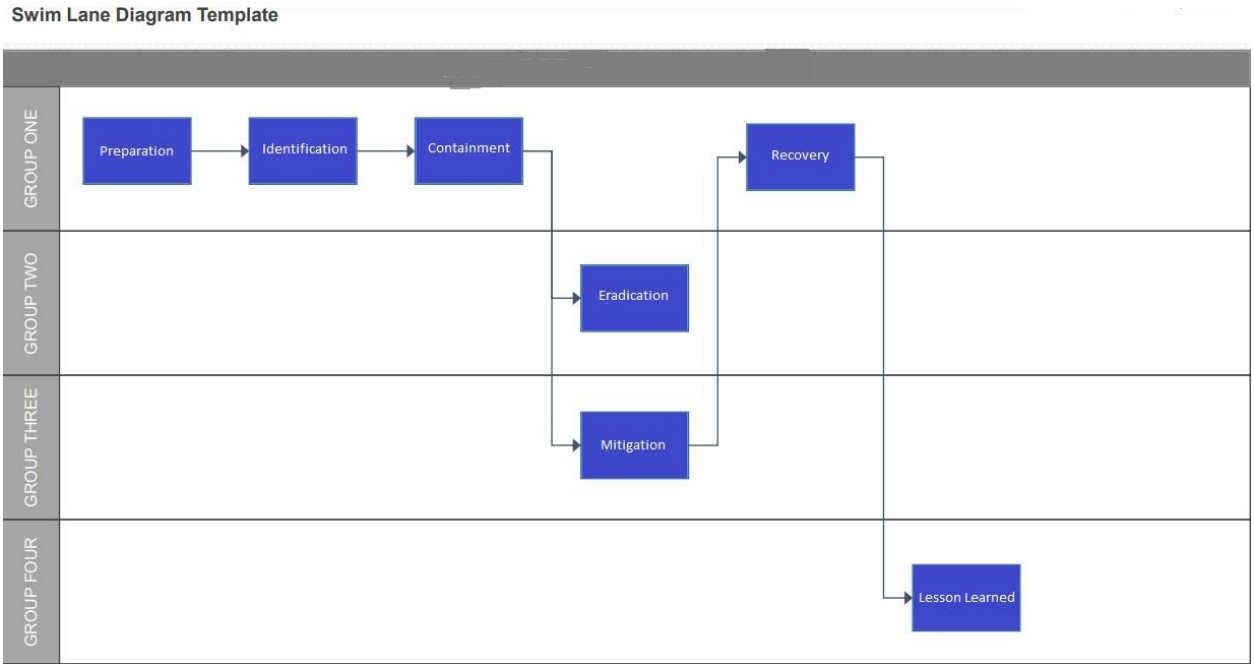


Figure 3 - Swimlane Diagram

Service-Level Agreement

Evaluate and Execute the Data Exfiltration Service-Level Agreement (SLA)

Our team transmitted the attack to other Five Eyes (FVEY) country team members, the team decided that all the nations in the summit were under the data exfiltration attack, and they retained their networks' latency or even unavailability. In fact, the new Service Level Agreement (SLA) for Canada will review the effect of the attack on cost and services.To ensure that the right security mechanisms are enforced to prevent vulnerabilities, the team analyzed DoS and Operating System (OS) risks and vulnerabilities. If there are ISP weaknesses, delays and disruptions to the network, the DoS mitigation services are to be provided. The team will also include solutions that are specified in this SLA's priorities, status monitoring and maintenance.

Operating System Fundamentals

Any modern computer system, from network servers, workstation desktops, to laptops and portable devices, has a central piece of software, called kernel or operating system, executed on the top of a bare machine of hardware that allocates the fundamental tools of the system and manages the execution of all programs within the system. Some prominent operating systems for commercial and open source are Microsoft Windows, various Unix, Mac OS, and Linux versions. Because of the operating system's vital function in the service of every Computer systems, operating system security (or lack of security) can have a significant effect on the general security of a computer system, and the security of all applications running within the system. (Yang, 2003).

Operating System Protections

An operating system must be present to control their resources and processes and take advantage of the functionality offered by different computing devices. Protecting the operating

system's functions from unauthorized access and use is very crucial.Operating systems, including viruses, ransomware, spoofing, and denial of service, are subject to many attacks. It is important to secure an Operating System because of the critical tasks performed by the Operating System. A main role in its security is to monitor the access of the operating system. Access can be extended only to users who have access privileges.

Access to the operating system must be regulated in order to secure the operating system. The concept of least privilege is based on the assertion that the minimum amount of access needed to accomplish their activities efficiently is given to software, users, and devices. This, in accordance with the "need to know principle," which specifies that the minimum degree of access needed for computer systems to perform activities over the minimum period of time required to do so, offers good techniques for minimizing and eliminating future violation occurrences. (UMGC, n.d.).

Operating System Security

Many attempts have been made to identify and build security models for trustworthy computing systems, protected operating systems specifications and architecture. The operating systems of today are more advanced and feature-rich than ever before, which makes them considerably more useful to the business, but also adds to the security vulnerability, unless the operating systems are appropriately designed, maintained and controlled. Organizations need to increase the protection of the operating system across their network, once in one location, provisioning of the servers on the network can be completed, requiring the approximately tens of different installations that most organizations require. (Krishna, 2014).

To monitor access to the network and to ensure that users have sufficient access to business services, account management has to be unified. In order to provide user systems with

correct IDs and authorizations, policies, rules and intelligence should be put in one location, not on each box, and pushed out from there. Also, the operating system should be designed so that it can be used to quickly and reliably track network behavior, exposing who connects and who does not connect, as well as pointing out possible security events emanating from the operating system. Security should not have to be a budget buster or compete with ordinary company tasks. Properly configured security for the operating system is a business enabler that saves money because it keeps the bad guys on the defensive where they belong. (Krishna, 2014).

Service-Level Agreement (SLA)

Theservice-level agreement (SLA) is an agreement between both the nation teams and the Internet Service Provider (ISP). As an internet connection subscriber, the Canada team decide what success level the ISP is supposed to attain. More significantly, by minimizing the DDoS threat, this checked agreement seeks to serve the security protections of the nation teams. In every outsourcing and technology vendor arrangement, SLAs are a vital part. Beyond listing service form and efficiency standards, an SLA offers solutions when specifications are not fulfilled.

Service Description

The aim of this Service Level Agreement (SLA) is to formulate the arrangements for the procurement of equipment and support facilities between the Canada team and the ISP at different support levels and at acceptable costs. With additional awareness of the consumer needs, as well as the integration of new products and facilities into the support portfolio offered by the vendor this SLA will grow over time. A comprehensive overview of each and every service offered by the ISP along with the length of time the service is available for use is the part of the SLA. Technical goals and limitations should be analyzed by the SLA. The best approachto

meet practical and sustainable technological goals is to learn of the different criteria and technological objectives that might increase the quality of operation over time. Once all the technical goals are established, it is time to look at the vulnerabilities and risks inherent in achieving the technical goal. Also, it is easier for the ISP to recognize and identify service level specifications and the network resources offered by the service provider by constructing an application profile. It also serves as a documented framework for funding for the network service which aligns the priorities of the network service with the business criteria. (Luenendonk, 2019).

The service requirements for a company are defined by ensuring conformity with standards of availability and performance. For various areas of a given program or network, this may be calculated. The team can now calculate the service efficiency in terms of latency, total scalability, and jitter, round-trip delay, and bandwidth commitments in many ways. Also, both constructive and reactive network operations and network management capabilities that can be applied to meet service level objectives are specified by the network service. In the last text of the arrangement, called an organizational support package, the network service concept is included. If all sides refuse to gather the metrics and track the efficiency of the service being offered, a service level concept on its own is absolutely meaningless. They should ensure that a clear description is provided when drafting a service level agreement as to how the service level will be calculated and recorded.(Luenendonk, 2019).

If the technical validation has been done by the ISP, DDoS Protection will verify the monitoring setup and plan to clean up traffic. The ISP will also enable traffic reports for prevention and detection available via the ISP portal. Daily reporting on available metrics in relation to goal results would be delivered by the ISP to the Canada team. The problem-ticket

method of the ISP, which will detail ticket management output against SLA goals in the case management phase of the ISP, is required to deliver these reports.

Best practices for implementing and operating SLAs

1. Document objectives and capabilities: In a set of Service Level Requirements, the Canada team can identify what it needs; criticality for users and the organization; hours of service availability; hours of service support; essential periods; maximum downtime; requirements for security and data protection; reporting requirements; and any mandated requirements for law, regulation or standards. (Freshservice, n.d.).
2. Gain mutual understanding: Before drafting the SLA, all parties should present and obtain a shared understanding of what is expected and what is possible. The Canada team facilitator should facilitate talks and find a compromise if there are disagreements that must be overcome. (Freshservice, n.d.).
3. Negotiate SLAs: In order to finalize the SLA, members of the Canada team and the ISP should meet, including discussing any unresolved things for a mutual agreement. An SLA must not be signed until all contents are decided by all parties. (Freshservice, n.d.).
4. Sign and communicate the agreement: The agreement should officially be signed by all parties. Within all sides, it must then be conveyed to anyone who wants to hear about it and made available for potential referral and analysis. (Freshservice, n.d.).
5. Use and review the SLA: As customer requirements and supplier capabilities can change, both parties should regularly review SLAs at least annually. (Freshservice, n.d.).

Service Level Agreement (SLA) Evaluation

The incident and SLA were reviewed to assess the ISP DDoS mitigation services. The Canada team was tasked with the creation of its own independent stable communications

network prior to the summit. Using the following parameters, the DDoS mitigation service offered by the provider will be evaluated. The requirements are based on practical knowledge in tested DDoS attack migration approaches.

1. Threat Intelligence: On a regular basis, the mitigation service provider can provide the team with detailed threat intelligence, gathered by a dedicated DDoS security specialist analysis team. Staying aware of the latest attack patterns, fresh development of toolkits and emerging cyber threats is so critical. (Akamai, 2015).
2. Front-Line Experience: The provider of mitigation services must be able to protect itself against all forms of cyberattacks. As a result of their combined experience in successful attack mitigation, seasoned DDoS mitigation service providers would have developed their network, making them much more equipped to deal with the unforeseen or zero-day form of DDoS incident. (Akamai, 2015).
3. Mitigation Capabilities: The team needs a very robust DDoS mitigation provider equipped to protect against all forms of existing and new attack vectors, including the greatest possible Internet attack scale. A time-to-mitigate SLA determines how fast and successful a DDoS attack can be stopped by the service provider. (Akamai, 2015).
4. Mitigation Capacity: Among DDoS mitigation service providers, mitigation capability is a crucial differentiator. The cost of bandwidth needed to tackle today's massive DDoS attacks is the largest cost item for trustworthy DDoS service providers. (Akamai, 2015).

Detection Category	**Strategy Used**	**Complexity**	**Detection Accuracy**	**Limitations**
Pattern Detection	Store the signature of the known attacks in the databases and monitor each communication for the presence of these pattern	Low	High	Novel attacks detection is not possible
Anomaly Detection	Compare the current state of the system with normal system behavior periodically	Medium	Medium	High rate of false positive/negatives, as normal system behavior and thresholds setting is difficult
Third Party Detection	Rely on a third party to signals the occurrence of attack.	High	Depend on detection approach used by third party	Economic Factor, Security prone.

Comparison of various Detection Approaches (Gupta, Misra& Joshi, 2008).

Keeping the FVEY nations safe from cyber-attacks and other threats during the summit is one of the ISP's most influential security concerns. In the IDS (intrusion detection system), data exfiltration was detected, which is very difficult to mitigate correctly as these attacks allow the system to stop operating by resource exhaustion. The list evaluates the performance of the ISP (internet service provider) during the attack:

Was the attack detected by the ISP?	☒ Yes ☒ No
Did the ISP respond to the attack with the SLA?	☒ Yes ☐ No
Did the attack create downtime for the summit?	☒ Yes ☐ No
Was the attack recorded and a report sent to the FVEY nations?	☒ Yes ☐ No

Has the attack vector been remediated?	☐ Yes ☒ No
What is the financial loss to the FVEY nations?	$ 0

FVEY Indicator Sharing Report

We know, so far, that we've been attacked by DoS. In order to ascertain the origin of the attack on the database server, the team examined a captured packet (PCAP) file that was presented to them to review and evaluate this file. A Denial-of-Service attack and other highly malicious activities were detected through forensic investigation and incident response by the team. A denial-of-service (DoS) attack happens when, because of the actions of a malicious cyber threat agent, legitimate users are unable to access computer systems, computers, or other network services. Affected services may include email, blogs, online accounts (e.g., banking), or other services that depend on the device or network that is affected. By overwhelming the intended host or network with traffic until the target does not respond or simply fails, a denial-of-service situation is achieved blocking access for legitimate users. (CISA, 2019).

This report would include strategies, details on risk assessments and prevention of DoS in an FVEY Indicator Sharing report, it will also discuss causes that may have stopped the DoS attack and offer suggestions to stop this and related attacks in the coming years. There are guidelines that apply to data indicators, vulnerabilities, exfiltration, network security measures to bring the device (BYOD) settings, and multi-factor verification measures such as CAC and PIV card readers to meet the goal of securing the network.

Risk Analysis and Mitigation

Risks can involve vulnerabilities that are unpatched, human actions, or emerging threats. The next move after a threat is established is to implement preventive strategies to thwart or mitigate the threat's effect. Corrective measures include altering or hardening security modules, altering security protocols, or blocking access to the device. Organizations should consider the best strategies for avoiding and reacting to a DoS attack in order to successfully protect against

Denial-of-Service attacks. Testing and verification offers the ability to test system security and ensure that the efficiency of system security is appropriate. An example is penetration (pen) testing, which is used to verify the security of the system, detect vulnerabilities that could place the system at risk, and suggest vulnerability mitigation. Regression testing, which looks at software output following software modifications to ensure that it works as expected before the update, is another example. Also, acceptance testing is carried out to assess if it is compliant with standards and is carried out prior to practical use. (UMGC, n.d.).In addition, continuous control is necessary to minimize DoS threats, restricting and managing traffic within the system can maintain the network going when under threat, warning protocols, assigning priority levels, and eventually getting a reaction and escalation action in place can help protect the networks.

To mitigate DoS threats, Snort an intrusion detection and prevention device program that is free and open source was used. To decide whether to accept traffic through a network, the tool analyzes protocols and content. Developing these rules requires an appreciation of the measurement of vulnerabilities. The rules help to detect threats, including buffer overflows, port scans, and fingerprinting attempts on the operating system. In order to detect a DoS attack against the web server (192.168.10.101) based on the bad actor IP address that was previously detected, the team used the snort tool to prevent any attack by running the following alert rules against the collected network traffic (i.e.192.168.10.111). In order to run against the captured network traffic, the following Snort rules were used:

##

#SNORT rule for detecting Denial of Service attack has been performed against the web server.

##

alert tcp 192.168.10.111 any -> 192.168.10.101 any (msg:"DoS Attack"; flow:stateless; content:"GET"; content:"Not Found"; sid:2000000201;)

##

#SNORT rule for detecting possible Denial of Service attack activity against the web server.

##

alert tcp 192.168.10.111 any -> 192.168.10.101 any (msg:"Possible Attack"; flow:stateless; content:"HTTP"; content:"GET"; sid:2000000202;)

##

#SNORT rule for detecting Denial of Service attempts against the web server.

##

alert tcp 192.168.10.111 any -> 192.168.10.101 any (msg:"Attempted Attack"; flow:stateless; content:"HTTP"; content:"Not Found"; detection_filter:trackby_dst, count 5000, seconds 5; sid:2000000203;)

##

Intrusion Detection and Prevention (IDS/IPS) Systems

Attendees at this summit, as well as the representatives from Canada, are advised to use network security systems like Instruction Detection Systems (IDS) or Intrusion Prevention Systems (IPS). Network traffic is analyzed by Intrusion Detection Systems (IDS) for signatures that complement documented cyberattacks. Packets are also processed by Intrusion Prevention Systems (IPS), but the packet can also be stopped from being sent depending on what kind of attacks it detects, helping to stop the attack. Both IDS/IPS read network packets and compare the content with a known threat database. The main contrast is what comes next to them. IDS are

instruments of monitoring and tracking but may not take action on their own. IPS is a mechanism of control that approves or rejects a packet depending on a series of rules. (Petters, 2020).

Like their cyber-attack databases, IDS/IPS is reliable. If a new attack breaks out in the wild and/or the attack signature is not in the database, it keeps them updated and be ready to make manual changes. Several organizations end up choosing an IDS to an IPS, since an IPS will stop the operations and interrupt the business in the case of false positives, but an IDS will just report and not impact the company.

It must do more than hire network security equipment for an organization to successfully defend itself against a cyber threat. An organization should always defend its endpoints efficiently. Any physical wireless system that is attached to a network is an endpoint. Endpoint defense is the defense from disruptive attacks by endpoints such as desktops, computers, and handheld devices.Endpoint security or endpoint defense is an approach to safeguarding data networks that are bridged to client computers remotely. The connection to business networks of notebooks, tablets, cell phones and other portable gadgets provides attack paths for security threats. Endpoint authentication aims to ensure that all devices meet with requirements at a definite stage. (Kantarci, 2020).

Organizations would be safe from most cyber-attacks if they preserve their networks and make sure it stays up to date. If they use a solution that helps them to remotely control both the distribution of anti-virus and operating system upgrades, companies can do this more efficiently. To detect blind spots that attackers might aim, companies should examine the existing endpoints. In order to provide a security approach by exploiting personal firewall, port and system access, and anti-malware features, endpoint defense platforms are implemented on endpoint devices. Using encryption is a vital consideration for securing endpoints. If an attacker

can get through the network and host-based protection and exfiltrate data successfully, it is possible that strong encryption would prohibit a hacker from using the information. Sensitive networks and specific systems need to be encrypted by an organization. (Kantarci, 2020).

Data Exfiltration Indicators

Usually, data exfiltration attacks imitate normal behavior, that is why, until any component of the data has already been moved, it is impossible to identify data exfiltration attacks in time. Organizations need to differentiate between illegal and permitted data transfer to detect data exfiltration efficiently. As part of an automatic attack, data exfiltration can occur or can be done manually and can occur on-site or over an internet connection. When this happens, confidential or important information is usually part of a planned attack. Although it is possible to track data exfiltration, it mostly does not happen until at least some data has been destroyed. This is because it looks very close to legal transactions to the illegal transfer of data. You ought to know that the customer or provider does not transfer information to identify it, that the data being transferred is suspicious, or that the transfer scale is suspicious. (Gonzalez, 2020).

For any organization, preventing data exfiltration should be a priority, especially those with sensitive data. One of the most common techniques attackers use to obtain access to a device is unreliable passwords. These may involve default passwords that have not been updated, passwords that have been poor or reused, or passwords that have been exchanged by phishing unintentionally.You can ensure that password policies require some flexibility and that passwords are rotated regularly in order to avoid password misuse. The introduction of multi-factor authentication (MFA) that uses a secondary approach to validate the identity of a user should also be considered. At-rest and in-transit data protection means that it can be reached only by anyone with the required key. Encryption is also a requirement of many legal enforcement and industry

practices. To keep information secure, wherever possible, organizations must ensure that all information is encrypted. Additional security measures can be added where there are occasions when encryption is not feasible, for example, in paper documents. (Gonzalez, 2020).

Bring Your Own Device (BYOD) Protection Method

Many organizations are introducing policies to allow employees to bring to work personal computers or mobile devices. This strategy makes it easier for companies to cut costs and offers workers the independence, accessibility and comfort to use one computer for both personal and company use. Although the implementation of a bring your own device (BYOD) approach may have certain advantages, there are also security risks. Safeguarding endpoints in a setting whereby the bring your own device (BYOD) is part of the network infrastructure brings an added layer of sophistication to the capacity of an organization to protect itself against attack. (UMGC, n.d.).

BYOD security solutions must be considered by organizations to have continuing employee education on the significance of appropriate usage and simple data security hygiene is essential for the effectiveness of BYOD. There are some components that are often used as part of a robust BYOD protection program that should be explored. For instance, antivirus software which is installed on individual devices is also a feature of such security programs. Monitoring, though with mixed views, is another component often used as part of a BYOD protection program. Encryption is another security mechanism which can be used as part of a robust BYOD security program. And even in the worst-case situation, such as a stolen device or traffic being detected over an unsecured network, encryption means that the contents of confidential files are secured. (Brook, 2020).

Importance of Authorization and Authentication Mechanisms like CAC-PIV Card Readers

Traditional authentication methods provide only a single authentication element, such as username/password combinations: something the user knows. On the other hand, common access cards (CAC) have two things: something that the user knows (the PIN) and something that the user has (the card). Through their multi-factor authentication of preference, government agencies and related contractors have implemented Common Access Card (CAC) / Personal Identity Verification (PIV) authentication. In these conditions, authentication allows the user to have a physical card with a corresponding password/PIN. With a username and password, in order to achieve network access, the hacker simply has to obtain the password. With a CAC, the hacker must physically acquire the CAC and also obtain the card's PIN. (Keiser & Edwards, 2016).

The common access cards (CAC) can protect user credentials, including identification certificates. The data is encrypted on the card it can only be provided for verification if opened with the security code of the user. This authentication technique is classified much simpler than basic password authentication even if an attacker breaches a password, without the actual card in hand, he/she is also unable to log in.In order to provide better security against more advanced threats authentication has to be more comprehensive, the physical form factor of the CAC and policies regulating its use provide the greatest strength of the card as an authentication mechanism. (Keiser & Edwards, 2016).

Best Practices for Database Protection

Security of databases is a complicated and challenging endeavor involving all aspects of technologies and practices in information security. It is also naturally at odds with the usability of databases. The more accessible and usable the database, the more vulnerable it is to security

threats; the more invulnerable the database is to threats, the more difficult it is to access and use. Since databases are almost always network-accessible, any security threat to any component within or portion of the network infrastructure is also a database threat, and the database can be threatened by any attack affecting the device or workstation of a user. Database security must therefore extend well beyond the confines of the database alone. (IBM, 2019).

Database protection allows an entity to develop the correct controls and policies for database access and data masking, also referred to as data obfuscation, which is a defense-in-depth technique that prevents attackers from reading critical data by covering original data using changed information. One of the most complex data obfuscation techniques is encryption. The use of a "key" to access data based on user rights and privileges is allowed by a special encryption mechanism. Database security policies, such as protection of critical intellectual property and cybersecurity policies and cloud security policies, should be integrated with and support the organization's overall business objectives. In support of formal security policies, security controls, security awareness training and education programs, and penetration testing, and vulnerability assessment strategies should all be developed. (IBM, 2019).

Final Forensic Report

Digital forensics has grown expediently as technology advances, and the field will continue to broaden as new types of digital data are created. With the onset of cybercrime, collection and tracking of malicious online activity has become critical. This will allow investigators to connect digitally stored information to physical evidence. There are five steps for computer forensics, which will allow a thorough investigation: (Lyle, 2008)

- **Identification** – identifying potential sources of evidence/digital data relating to an attack.
- **Preservation** –preserving digital data stored information, by protecting the crime or incident scene, capturing images, and documenting all evidence acquired.
- **Collection** – collecting digital data pertinent to the investigation. Collection may involve removing the electronic devices from the incident scene.
- **Analysis** – in depth search of evidence relating to the incident being investigated, to draw conclusions based on the evidence.
- **Reporting** – reports are based on proven techniques and methodologies of the evidence.

When performing digital forensics investigations, there are currently three major resource groups to assist the digital forensic examiner with an investigation. The three groups with the support of NIST, the U.S. Department of Justice's National Institute of Justice (NIJ), and the National Institute of Standards and Technology Office of Law Enforcement Standards (OLES) help advocate the efficient and effective use of technology in the investigation of cybercrimes.

- National Software Reference Library (NSRL)
- Computer Forensic Tool Testing (CFTT)

- Computer Forensic Reference Data Sets (CFReDS)

NSRL

The NSRL was developed to collect software from numerous sources and create profiles computed from software into a Reference Data Set (RDS), such as hashes created when software is installed on network computers. The NSRL main objective is to advice computer forensics examiners during their investigations with a library comprising of:

- collection of over 9,000 original software packages.
- database containing detailed information about the files in those software packages.
- public NSRL Reference Data Set (RDS) which contains a subset of the metadata held in the database. The RDS is published and updated quarterly, as NIST Special Database 28.

CFTT

The CFTT group's intention, is to create a functionality driven methodology for testing computer forensic software tools through general tool specifications, test procedures, test criteria, test sets, and test hardware. The outcome provides the allows the toolmakers to improve tools that support forensic investigations. Each facet of a digital forensic investigation is separated into distinct actions, such as hard disk drive (HDD) write protection, disk imaging, etc. For each action, a test methodology is then developed for each category. After a test methodology is developed it is posted to the online for the public and help forensic examiners test specified actions within a computer forensic tool.

CFReDS

The CFReDS is a repository of images to provide an investigator with simulated digital evidence for an examination. This type of evidence will allow investigators the ability to compare the results of searches for the target strings with the known placement of the strings. CFReDS can also help investigators in several other ways including validating software tools, equipment checks, training investigators, and proficiency testing for laboratory accreditation. The CFReDS web site is **http://www.cfreds.nist.gov**. (Lyle, 2008)

Network Attack Techniques

Cyberattacks are any type of attack to gain unauthorized access to a computer network system for the purpose of theft, extortion, disruption infrastructures, computer network or personal computer devices, using various attack techniques. Some most common attacks are: (Rapid7, n.d.)

Denial-of-service (DoS) - overwhelms a system's resources so that it cannot respond to service requests.

Man-in-the-middle (MitM) - hacker inserts itself between the communications of a client and a server.

Phishing - emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.

Password attack - obtaining user passwords e.g., Brute Force attack

SQL injection - SQL query to the database by inputting data from the client to server. A successful attack, hackers could read, modify, update, or delete sensitive data from the database.

Eavesdropping - interception of network traffic.

Malware attack - software installed in your system without your consent collection data.

Attack Vectors

When discussing cyber-attacks, there are many ways an attacker can expose, modify, delete, steal, or gain unauthorized access to network systems. Attack vectors can be divided into two type of attacks: (Balbix, n.d.)

- **Passive attack** - attempts to gain access or make use of information from the system but does not affect system resources, such as phishing and social engineering attacks.
- **Active attacks** - attempts to modify a network system, such as malware, exploiting vulnerabilities, email spoofing, man-in-the-middle attacks, and ransomware.

Most common types of attack vectors: (OpenLearn, n.d.)

- **Compromised credentials** - usernames and passwords.
- **Weak credentials** - weak passwords and reused passwords.
- **Malicious insiders** - disgruntled employees
- **Missing or poor encryption** – missing common encryption methods like SSL.
- **Misconfiguration** - misconfiguration of cloud services, like Google Cloud Platform, Microsoft Azure or AWS.
- **Ransomware** - extortion where data is deleted or encrypted unless a ransom is paid.
- **Vulnerabilities** - vulnerabilities are added to CVE every day and zero-day vulnerabilities are found just as often.
- **Brute force** - attacks are based on trial and error.
- **Trojans** - malware that misleads users to be a legitimate program.
- **Third and fourth-party vendors** - risk to your customers data and your proprietary data.

Computer Forensics Tools

When starting a computer forensics investigation, there are many tools at the fingertips of an investigator, with some being costly, and other open source. Digital evidence can be found in many different forms, and on a variety of platforms. Digital investigation go through thorough analysis of different files, emails, and network activity, to find and collect evidence to find the impact and attribution of an incident. Due to the extensive amounts of data sources during an investigation, digital forensics tools often have different specialties. Here are some of the most common used tools for achieving different parts of a computer forensics investigation: (guru99, n.d.)

Autopsy/The Sleuth Kit - Sleuth Kit is a command-line tool, whereas Autopsy is a GUI-based system, that performs forensic analysis of forensic images of hard drives and smartphones.

FTK Imager - analyzing an image (rather than a live drive) is that the use of an image allows the investigator to prove that they have not made any modifications to the drive.

Volatility – analyzes RAM because forensic information can be stored in RAM, and this volatile memory must be collected quickly and carefully to be forensically valid and useful.

Registry Recon – analyzes Windows Registry. The registry acts as a database of configuration information for the Windows OS and the applications running on it, and one of the common locations where malware deploys.

Cellebrite UFED – analyzes mobile devices, which will work with either BYOD or corporate-owned devices.

Wireshark – network traffic analyzer, because cyberattacks occur over the network, and analysis of network traffic captures can help with the identification of malware and provide access to data that may have already been deleted and overwritten on the endpoint.

References

Akamai. (2015). How to evaluate DDoS mitigation providers: Four critical criteria. Retrieved from https://www.ten-inc.com/presentations/Akamai_DDOS.pdf

att. (n.d.). Incident Response Tools. Retrieved from cybersecurity.att: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools

Binus. (2017, May 8). DESIGNING INTEGRITY CONTROLS. Retrieved from Binus University: https://sis.binus.ac.id/2017/05/08/designing-integrity-controls/

Balbix. (n.d.). 8 common cyber attack vectors and how to avoid it. Retrieved from Balbix: https://www.balbix.com/insights/attack-vectors-and-breach-methods/

Burgett, A. (2020, March 5). Stay Secure With These Intrusion Detection and Protection Techniques. Retrieved from kirkpatrickprice: https://kirkpatrickprice.com/blog/idps-techniques/

Brook, C. (2020). The ultimate guide to BYOD security: Overcoming challenges, creating

effective policies, and mitigating risks to maximize benefits. Retrieved from https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

CISA. (2019). Understanding Denial-of-Service attacks. Retrieved from

https://us-cert.cisa.gov/ncas/tips/ST04-015

ELLIS, D. (n.d.). 6 Phases in the Incident Response Plan. Retrieved from Security Metrics: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

Freshservice. (n.d.). SLA 101. Retrieved from https://freshservice.com/sla

Gupta, B., Misra, M., & Joshi, R. (2008). An ISP level solution to combat DDoS attacks using combined statistical based approach. Retrieved from https://www.researchgate.net/profile/B_B_Gupta/publication/221677207_An_ISP_level_Solution_to_Combat_DDoS_attacks_using_Combined_Statistical_Based_Approach/links/0046351761840e0607000000/An-ISP-level-Solution-to-Combat-DDoS-attacks-using-Combined-Statistical-Based-Approach.pdf

Gonzalez, C. (2020). Data exfiltration threats and prevention techniques you should know. Retrieved from https://www.exabeam.com/dlp/data-exfiltration/

guru99. (n.d.). 15 BEST Digital Forensic Tools in 2021. Retrieved from guru99: https://www.guru99.com/computer-forensics-tools.html

HP. (2019). HP Sure Start. Retrieved from http://h10032.www1.hp.com/ctg/Manual/c06216928

IBM. (2019). Database security. Retrieved from https://www.ibm.com/cloud/learn/database-security

Johnson, L. (2020). Incident Response Process. Retrieved from sciencedirect: https://www.sciencedirect.com/topics/computer-science/incident-response-process

Kantarci, A. (2020). Endpoint security: What it is, why it matters & best practices. Retrieved

from https://research.aimultiple.com/endpoint-security/

Keiser, E. & Edwards, J. (2016). The pros and cons of common access cards. Retrieved from

https://www.c4isrnet.com/2016/04/11/the-pros-and-cons-of-common-access-cards/

Krishna, A. (2014). Steps to a secure operating system. Retrieved from https://www.computerworld.com/article/2571939/steps-to-a-secure-operating-system.html

Lyle, J. R. (2008, April). Digital Forensics at the National Institute of Standards and Technology. Retrieved from NIST: Nist.gov

Luenendonk, M. (2019). Understanding and managing service level agreements. Retrieved from https://www.cleverism.com/understanding-managing-service-level-agreements/

Malwarebytes. (2021). Backdoor computing attacks. Retrieved from

https://www.malwarebytes.com/backdoor/

Murphy, G. (2019). Standards, Policies, and Guidelines Definition. UMUC.

Murphy, G. (2019, March 19). Vulnerability Assessment. Vulnerability Assessment.

NIST. (2012, Aug). Computer Security Incident Handling Guide. Retrieved from NIST: www.nist.giv

OpenLearn. (n.d.). Digital forensics. Retrieved from Open.edu: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/

Petters, J. (2020). IDS vs. IPS: What is the difference? Retrieved from https://www.varonis.com/blog/ids-vs-ips/#:~:text=Intrusion%20Detection%20Systems%20(IDS)%20analyze,detects%20%E2%80%94%20helping%20stop%20the%20attack.

Parliament of Canada. (2019, June 21). Bill C-59. Retrieved from https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent

Rapid7. (n.d.). Common Types of Cybersecurity Attacks. Retrieved from Rapid7: https://www.rapid7.com/fundamentals/types-of-attacks/

Trusted Computing Group. (2021). Trusted Platform Module (TPM) Summary. Retrieved from https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/#:~:text=TPM%20(Trusted%20Platform%20Module)%20is,(your%20PC%20or%20laptop).

Torino, S. (n.d.). 8 NIST Security Controls to Focus on During, and After, a Crisis. Retrieved from cybersaint: https://www.cybersaint.io/blog/8-nist-security-controls-to-focus-on-during-and-after-a-crisis

UMGC. (n.d.). Nations behaving badly. Retrieved from UMGC: https://leocontent.umgc.edu/content/umuc/tgs/cyb/cyb670/2211/learning-topic-list/operating-system-protections.html?ou=541402

UMGC. (n.d.). Nations behaving badly. Retrieved from UMGC: https://leocontent.umgc.edu/content/umuc/tgs/cyb/cyb670/2211/learning-topic-list/risk-analysis-and-mitigation.html?ou=541402

UMGC. (n.d.). Nations behaving badly. Retrieved from UMGC: https://leocontent.umgc.edu/content/umuc/tgs/cyb/cyb670/2211/learning-topic-list/bring-your-own-device--byod-.html?ou=541402

Yang, C. (2003). Operating system security and secure operating systems. Retrieved from https://www.giac.org/paper/gsec/2776/operating-system-security-secure-operating-systems/104723