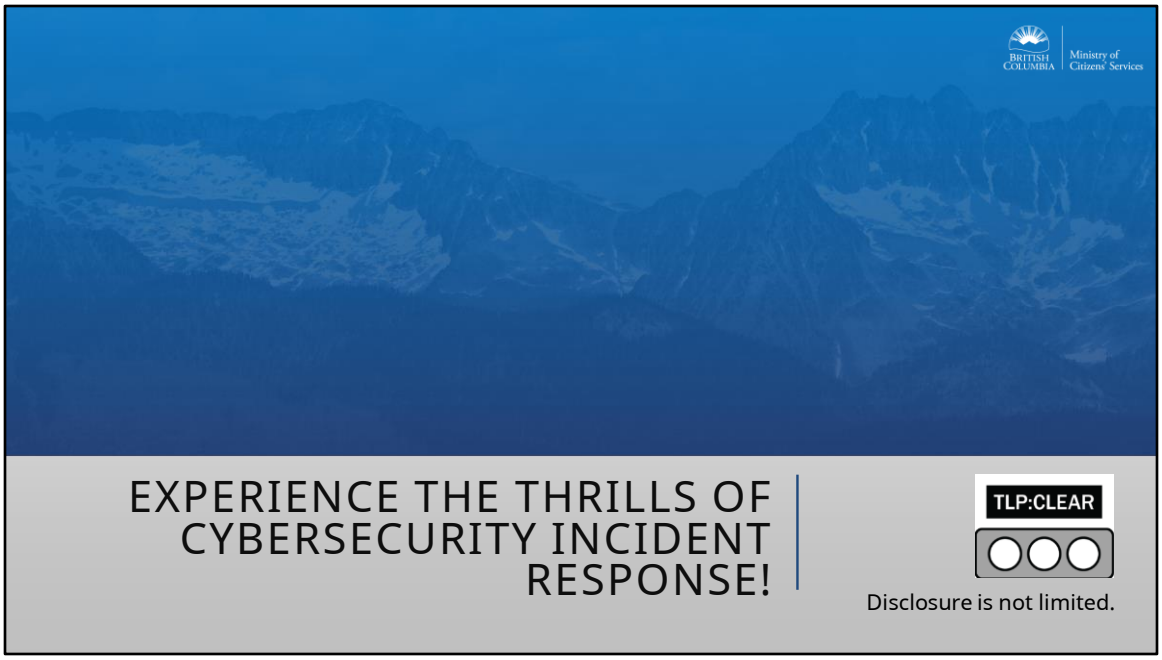
BRITISH COLUMBIA | Ministry of Citizens' Services

PICERL-Y CIRCUS

VIPSS March 11, 2025

Alex Loffler
James Argue

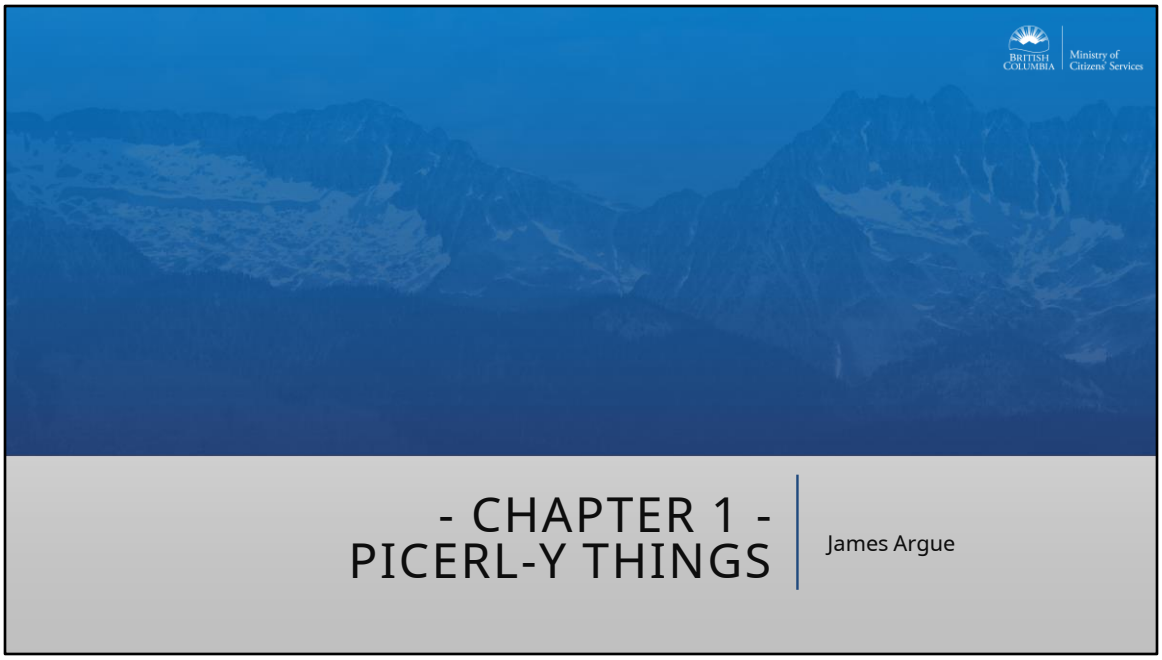


EXPERIENCE THE THRILLS OF CYBERSECURITY INCIDENT RESPONSE!

Disclosure is not limited.

AGENDA

Chapter 1 – PICERL-y things
Chapter 2 – PICERL adventures!
Chapter 3 – PICERL lightning round



- CHAPTER 1 - PICERL-Y THINGS

James Argue

THE PICERL PROCESS

BRITISH COLUMBIA Ministry of Citizens' Services

The Province of British Columbia follows the SANS PICERL Cyber Incident Response process, as described within the industry, including the SANS Institute.

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-security-incident-response-process

VOTING TEST: PICERL PICK A SQUIRREL

BRITISH COLUMBIA Ministry of Citizens' Services

Squirrel-San

Squeve

Squirleggo

YOU CHOSE: SQUIRREL-SAN

BRITISH COLUMBIA Ministry of Citizens' Services

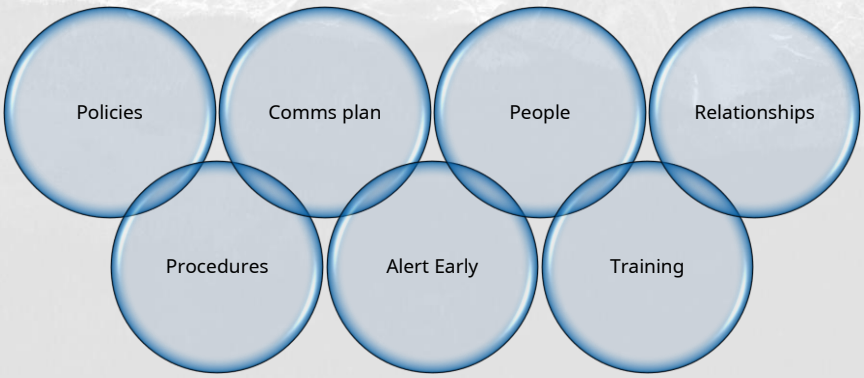
Squirrel-San

Squeve

Squirleggo

PREPARATION

Standardize responses, such as playbooks covering various cyber security event types including Phishing, Compromised Device, Compromised Credentials and more.



SQUIRREL-SAN - PREPARATION

BRITISH COLUMBIA Ministry of Citizens' Services

IDENTIFICATION

Based on the reports and other available information, identify the type, scope and severity of the incident so we can mount the appropriate response. If the incident was reported by a person, vs automated alert, then ensure we have all the information from them and inform them with updates.

- Awareness
- Need to know
- Tools
- Jump Bag
- Use out-of-band comms
- Management notified
- Primary IR handler
- Unusual security events
- Unusual files
- Analyze logs
- Chain of custody
- Passive monitoring
- Odd scheduled tasks
- Rogue processes
- Unusual accounts / privileges

SQUIRREL-SAN - IDENTIFICATION

BRITISH COLUMBIA Ministry of Citizens' Services

CONTAINMENT

Once we have completed enough Identification, then start the response. Usually some steps to ensure the attack/problem is not getting worse or can be stopped completely.

- "Stop bleeding"
- Categorize
- Notify management
- Remove LAN cable
- Isolate host
- Memory captures

- Short-term
- Criticality
- FW/IDS filters
- Adjacent host logs
- Kill backdoors

- Change passwords
- Back-up
- Sensitivity
- Low profile
- ISP coordination
- Patch vuln(s)

- Long-term
- Document actions
- Infected VLAN
- Forensic images

SQUIRREL-SAN - CONTAINMENT

BRITISH COLUMBIA Ministry of Citizens' Services

ERADICATION

Once we have contained the problem from getting worse, completely remove the threat. Including finding all instances of the problem and eliminating it from our environment.

- Delete artifacts
- Apply all patches
- Black hole IP's
- SIEM alerts
- Root cause
- Restore back-up
- Black hole DNS
- Additional FW / IDS
- Other host footholds?
- Wipe/format/rebuild
- Remove malware
- Rescan network

SQUIRREL-SAN - ERADICATION

RECOVERY

Ministry of Citizens' Services

Returning all user access and equipment back to a normal operating condition.

Usually, the business areas affected by the cyber security event work with service delivery processes and staff.

It may include removing protective controls that were added during the containment phase if no longer required.


Return to operations


Test documented baseline


Monitor (signs/shells/artifacts/events)


Move to production (approval)


Script searches for attacker artifacts

SQUIRREL-SAN - RECOVERY

LESSONS LEARNED

Ministry of Citizens' Services

Review the incident and our response to ensure the best protocols are in place to address the situation efficiently and effectively.

- Update our Security Incident Response Plan and Playbooks as appropriate
- Close our cyber incident documentation
- Give completion notification to our reporter(s) and stakeholders

Document incident ASAP
Assign to on-scene IR Handler
All affected parties review draft
Finalize report
Provide exec summary

Seek required changes
Seek funding
Reach report consensus
Address process not people
Update procedures

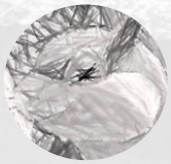
SQUIRREL-SAN – LESSONS LEARNED

BRITISH COLUMBIA Ministry of Citizens' Services

OFF TO CHAPTER 2

- CHAPTER 2 - PICERL ADVENTURES

YOU CHOSE: SQUEVE



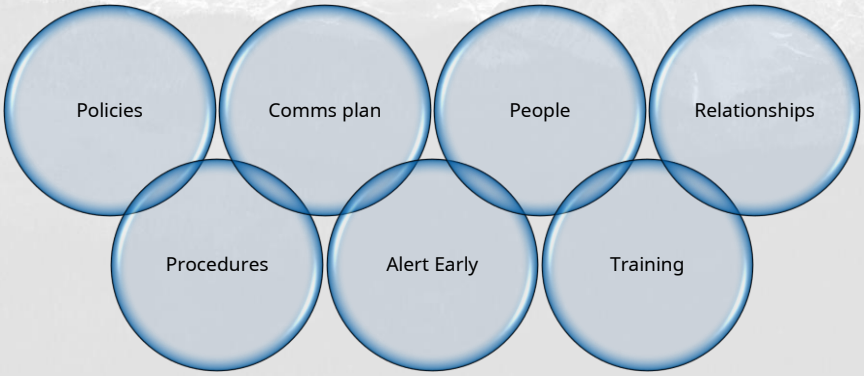
Squirrel-San

Squeve

Squirleggo

PREPARATION

Standardize responses, such as playbooks covering various cyber security event types including Phishing, Compromised Device, Compromised Credentials and more.



SQUEVE - PREPARATION

BRITISH COLUMBIA Ministry of Citizens' Services

IDENTIFICATION

Based on the reports and other available information, identify the type, scope and severity of the incident so we can mount the appropriate response. If the incident was reported by a person, vs automated alert, then ensure we have all the information from them and inform them with updates.

- Awareness
- Need to know
- Tools
- Jump Bag
- Use out-of-band comms
- Management notified
- Primary IR handler
- Unusual security events
- Unusual files
- Analyze logs
- Chain of custody
- Passive monitoring
- Odd scheduled tasks
- Rogue processes
- Unusual accounts / privileges

SQUEVE - IDENTIFICATION

CONTAINMENT

Once we have completed enough Identification, then start the response. Usually some steps to ensure the attack/problem is not getting worse or can be stopped completely.

- "Stop bleeding"
  - Categorize
  - Notify management
  - Remove LAN cable
  - Isolate host
  - Memory captures
- Short-term
  - Criticality
  - FW/IDS filters
  - Adjacent host logs
  - Kill backdoors
- Change passwords
  - Back-up
  - Sensitivity
  - Low profile
  - ISP coordination
  - Patch vuln(s)
- Long-term
  - Document actions
  - Infected VLAN
  - Forensic images

SQUEVE - CONTAINMENT

ERADICATION

Ministry of Citizens' Services

Once we have contained the problem from getting worse, completely remove the threat. Including finding all instances of the problem and eliminating it from our environment.

- Delete artifacts
- Apply all patches
- Black hole IP's
- SIEM alerts
- Root cause
- Restore back-up
- Black hole DNS
- Additional FW / IDS
- Other host footholds?
- Wipe/format/rebuild
- Remove malware
- Rescan network

SQUEVE - ERADICATION

RECOVERY

Ministry of Citizens' Services

Returning all user access and equipment back to a normal operating condition.

Usually, the business areas affected by the cyber security event work with service delivery processes and staff.

It may include removing protective controls that were added during the containment phase if no longer required.


Return to operations


Test documented baseline


Monitor (signs/shells/artifacts/events)


Move to production (approval)


Script searches for attacker artifacts

SQUEVE - RECOVERY

LESSONS LEARNED

Ministry of Citizens' Services

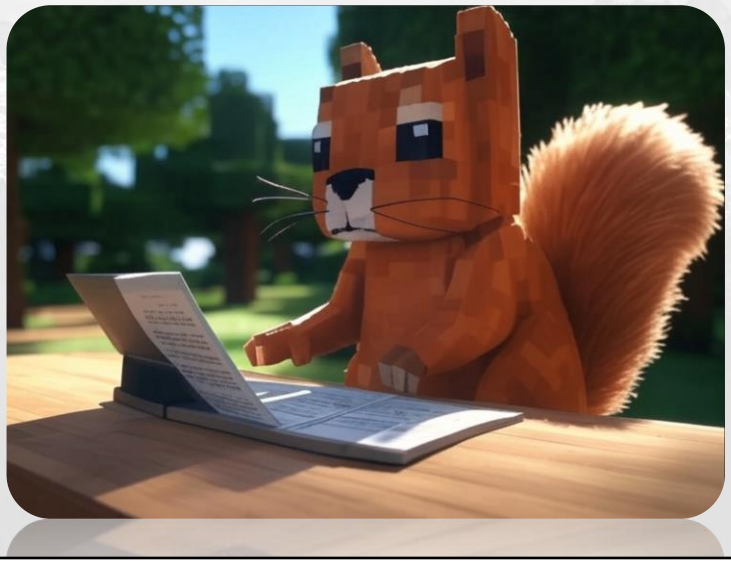
Review the incident and our response to ensure the best protocols are in place to address the situation efficiently and effectively.

- Update our Security Incident Response Plan and Playbooks as appropriate
- Close our cyber incident documentation
- Give completion notification to our reporter(s) and stakeholders

Document incident ASAP
Assign to on-scene IR Handler
All affected parties review draft
Finalize report
Provide exec summary

Seek required changes
Seek funding
Reach report consensus
Address process not people
Update procedures

SQUEVE - LESSONS LEARNED

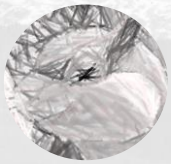


OFF TO CHAPTER 2

- CHAPTER 2 - PICERL ADVENTURES

YOU CHOSE: SQUIRLEGGO

BRITISH COLUMBIA Ministry of Citizens' Services



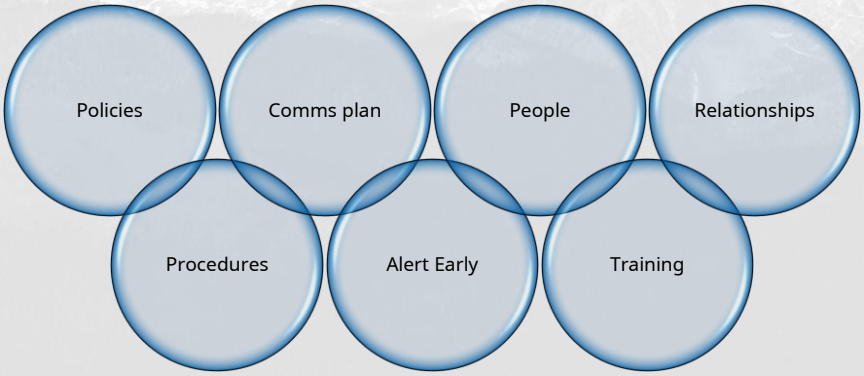
Squirrel-San

Squeve

Squirleggo

PREPARATION

Standardize responses, such as playbooks covering various cyber security event types including Phishing, Compromised Device, Compromised Credentials and more.



SQUIRLEGGO - PREPARATION

IDENTIFICATION

Based on the reports and other available information, identify the type, scope and severity of the incident so we can mount the appropriate response. If the incident was reported by a person, vs automated alert, then ensure we have all the information from them and inform them with updates.

- Awareness
- Need to know
- Tools
- Jump Bag
- Use out-of-band comms
- Management notified
- Primary IR handler
- Unusual security events
- Unusual files
- Analyze logs
- Chain of custody
- Passive monitoring
- Odd scheduled tasks
- Rogue processes
- Unusual accounts / privileges

SQUIRLEGGO - IDENTIFICATION

BRITISH COLUMBIA Ministry of Citizens' Services

CONTAINMENT

Once we have completed enough Identification, then start the response. Usually some steps to ensure the attack/problem is not getting worse or can be stopped completely.

- "Stop bleeding"
  - Categorize
  - Notify management
  - Remove LAN cable
  - Isolate host
  - Memory captures
- Short-term
  - Criticality
  - FW/IDS filters
  - Adjacent host logs
  - Kill backdoors
- Change passwords
  - Back-up
  - Sensitivity
  - Low profile
  - ISP coordination
  - Patch vuln(s)
- Long-term
  - Document actions
  - Infected VLAN
  - Forensic images

SQUIRLEGGO - CONTAINMENT

ERADICATION

Ministry of Citizens' Services

Once we have contained the problem from getting worse, completely remove the threat. Including finding all instances of the problem and eliminating it from our environment.

- Delete artifacts
- Apply all patches
- Black hole IP's
- SIEM alerts
- Root cause
- Restore back-up
- Black hole DNS
- Additional FW / IDS
- Other host footholds?
- Wipe/format/rebuild
- Remove malware
- Rescan network

SQUIRLEGGO - ERADICATION

RECOVERY

Ministry of Citizens' Services

Returning all user access and equipment back to a normal operating condition.

Usually, the business areas affected by the cyber security event work with service delivery processes and staff.

It may include removing protective controls that were added during the containment phase if no longer required.


Return to operations


Test documented baseline


Monitor (signs/shells/artifacts/events)


Move to production (approval)


Script searches for attacker artifacts

SQUIRLEGGO - RECOVERY

LESSONS LEARNED

Ministry of Citizens' Services

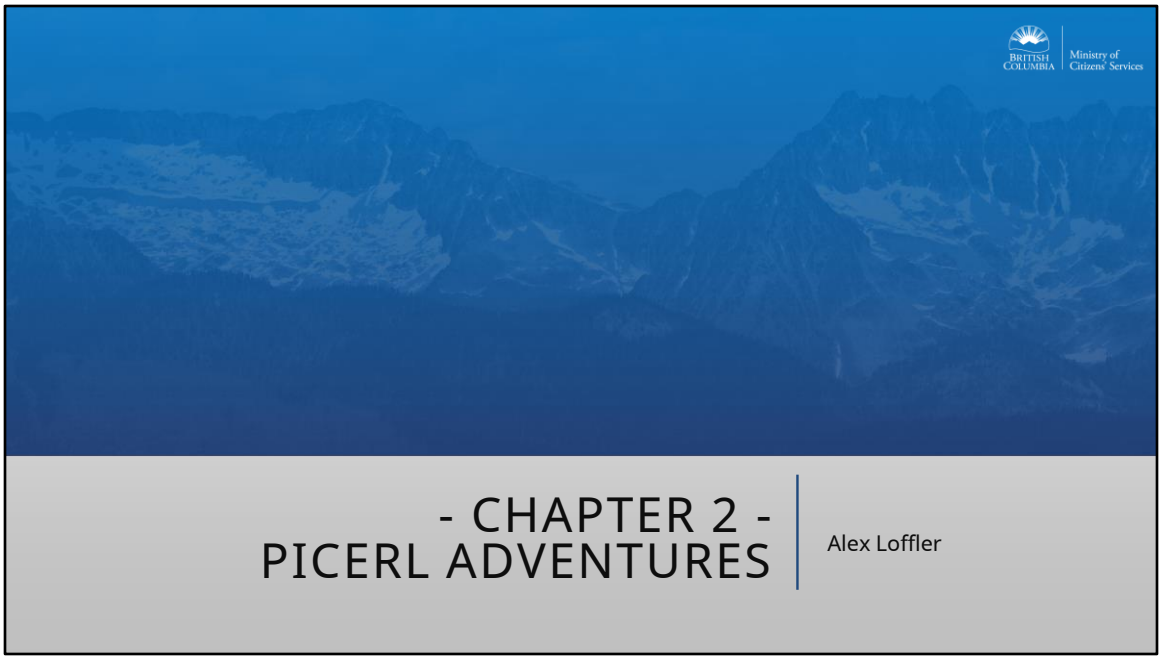
Review the incident and our response to ensure the best protocols are in place to address the situation efficiently and effectively.

- Update our Security Incident Response Plan and Playbooks as appropriate
- Close our cyber incident documentation
- Give completion notification to our reporter(s) and stakeholders

Document incident ASAP
Assign to on-scene IR Handler
All affected parties review draft
Finalize report
Provide exec summary

Seek required changes
Seek funding
Reach report consensus
Address process not people
Update procedures

SQUIRLEGGO – LESSONS LEARNED



We are going to walk through a Fictitious Incident Scenario.

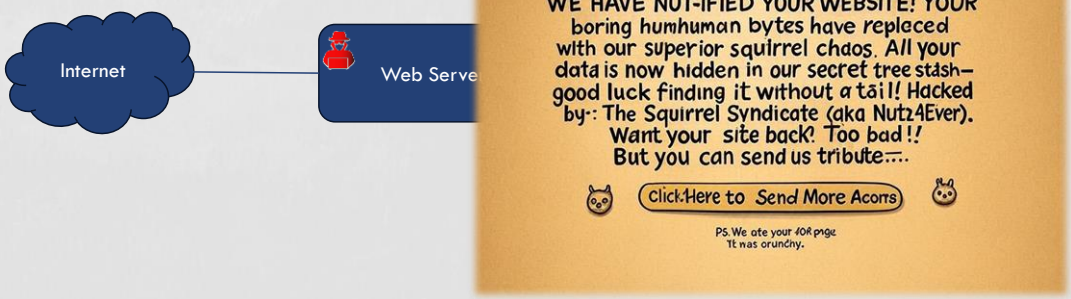
There are four parts to the scenario, in each part we will explore the findings and walk though some questions.

PART 1 – WEB DEFACEMENT

Your citizen facing website has been defaced!

A member of your team notices the defacement and alerts you.

What do you do?



PREPARATION

BRITISH COLUMBIA Ministry of Citizens' Services

This is happening right now, so we don't have time to prepare.

But if we had a time machine, some things to consider would be:

- Develop an Incident Response Plan / Runbook
- Ensure Backups of the system (and validate those backups)
- Patch Management
- Baseline Configuration – file hashes, user accounts, configurations, etc.
- Documentation – Architectural Diagrams, Support Contracts, RACI

QUESTION

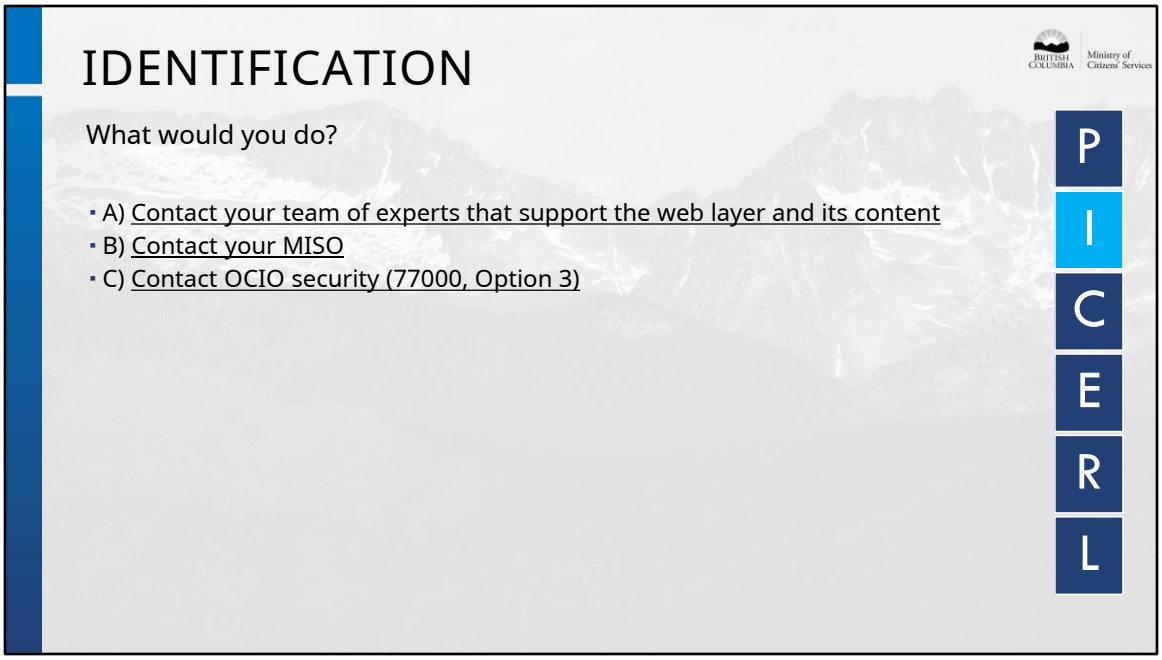
BRITISH COLUMBIA Ministry of Citizens' Services

Who is typically involved in the Prepare phase?

A) Only IT staff
B) Only external consultants
C) A cross-functional team
D) Only senior management

P
I
C
E
R
L

Answer: C



Discussion Prompt: Ask the audience how their chosen measure could have stopped the initial breach or limited its impact (e.g., patching the vulnerability or protecting the admin's credentials).

IDENTIFICATION – APP TEAM

Ministry of Citizens' Services

Your team finds a backup with accurate content from one month ago.

The team logs onto the server to restore the web application (avoiding a server restore from datacenter backups).

The web server returns to service with its regular content.

But your group does not feel that they have identified the root cause of the defacement, and decide they need more resources to attack the problem.

You contact your MISO for advice.

It is important to note, that by making changes to the server, the team has destroyed or at altered forensic evidence that could be vital to determining the root cause of the compromise and activity of the threat actor.

IDENTIFICATION - MISO

Ministry of Citizens' Services

P
I
C
E
R
L

Your MISO is concerned that we need more information to determine the root cause and feels the need to follow process and engage OCIO's SIIRT team.

The MISO calls 77000, Option 3 for support.

Cybersecurity Incident Response Process - Province of British Columbia

If you believe you have an ongoing Cyber Security Incident (i.e., signs that unauthorized agents have access and are using a computing device), please report your concern to the **OCIO Customer Service Centre at 7-7000 option 3 (1-250-387-7000).**

IDENTIFICATION - OCIO

The OCIO Security Investigations and Incident Response Team (SIIRT) meets with you, your application team and your MISO.

After assessing the situation. SIIRT engages DXC Advanced Solutions' datacenter personnel.

We discover that the web server was compromised through a known vulnerability existing in the web tier.

SIIRT requests:

- Application architecture diagrams and ops & admin contacts.
- List of all user, admin and service accounts with access to the affected server.
- A list of any other assets that the above accounts are able to access.

SIIRT activity:

- Forensic analysis of the server snapshot images.
- Identify similar applications elsewhere in the organisation.
- Attempt to identity the threat actor activity at the organisation perimeter.

P
I
C
E
R
L

QUESTION

Ministry of Citizens' Services

P
I
C
E
R
L

Which tool is most likely used in the Identify phase?

A) A backup system
B) A malware removal tool
C) A log analytics system (SIEM)
D) A project management app

Answer: C

CONTAINMENT

Ministry of Citizens' Services

P
I
C
E
R
L

SIIRT Recommends:

- Isolating the server and any related systems.
- Disabling the related admin, service and user accounts.
- Block & log any threat actor traffic (e.g. IP's) from all govt systems.

SIIRT Actions:

- Initiate Incident Response process with other ministries/platform teams based on discovery of similar application instances or as indicated by threat actor activity.

QUESTION

BRITISH COLUMBIA Ministry of Citizens' Services

P
I
C
E
R
L

What should be avoided during containment?

A) Documenting actions
B) Acting too quickly
C) Tipping off attackers unnecessarily
D) Using automated tools

Answer: C

ERADICATION

SIIRT recommends:

- Restoring from a known good server backup (server image)
- Scanning for vulnerabilities once the restore has completed
- Resetting all affected credentials (admin, service, web-admin and web application user accounts)
- Review file & directory permissions
- Review application and OS configurations

P
I
C
E
R
L

QUESTION

What must be confirmed *before* moving past eradication?

A) The incident is fully contained
B) The CEO approves
C) New software is installed
D) The team takes a break

P
I
C
E
R
L

Answer: A

RECOVERY

Ministry of Citizens' Services

Recovery tasks:

- Test functionality of restored service
- Verify patches have been applied
- Restore network connectivity
- Monitor for signs of re-compromise
- Notify stakeholders and end users about the resolution and any required actions

QUESTION

Who should verify systems are fully recovered?

A) Only the IT team
B) Affected stakeholders and IT
C) External auditors only
D) The marketing team

Answer: B

LESSONS LEARNED

Ministry of Citizens' Services

Conduct a debrief: What happened, what worked and what didn't.

Document findings.

- Create a detailed timeline of events.
- Document the chain of events and gaps that led to the incident.
- Capture total cost of the incident i.e. reputation damage, downtime, labour, etc.

Update Incident Response Plan / Playbooks.

Review patch cycles.

Separate administrative functions and accounts.

Share findings with relevant partners (e.g. CCCS, other ministries, etc.).

Review and implement additional controls (MFA, WAF, improved logging/monitoring, etc.).

P
I
C
E
R
L

QUESTION

What is a key outcome of Lessons Learned?

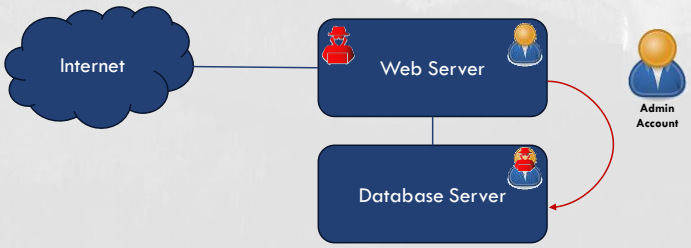
A) A fancy report no one reads
B) Stronger defenses against future incidents
C) A new team mascot
D) More paperwork for fun

Answer: B

PART 2 – STOLEN CREDENTIALS

As the incident unfolds, analysis of the web server image discovers that the admin credentials for the webserver may have been stolen.

This has allowed the attacker to move laterally to the database server containing sensitive citizen data.



<anim>
Once the attacker established a foothold on the webserver, they modified the SSH daemon to gather any usernames and passwords used to access the server.

<anim>
At this point, any user logging into the asset, would have their credentials harvested.

<anim>
This allowed the attacker to move laterally and access the DB server with the same admin credentials.

STOLEN CREDENTIALS

The organization had basic security measures like firewalls and antivirus in place.

Which additional security control would have most effectively prevented this server compromise?

A) Regular patch management
B) Enabling MFA for admin accounts
C) Network segmentation
D) Endpoint detection and response (EDR) tools

Although all of these options are valuable, the initial attack vector was a web server vulnerability.

So, in this scenario the

Answer: A

STOLEN CREDENTIALS

The IT team notices unusual outbound traffic from the web server and sees failed login attempts on the database server.

What is the best way to identify that credential theft and lateral movement are occurring?

A) Check server logs for admin login activity
B) Investigate failed login attempts on other systems
C) Scan the web server for malware
D) Monitor network traffic for anomalies

Discuss why correlating logs and failed logins across systems is key to spotting lateral movement, rather than focusing solely on the initial compromise.

Answer: A

It is important to note that an attacker can delete logs from a server.

Using a centralized log analytics platform, that moves the logs off the monitored systems helps protect against log tampering.

It also makes log search across multiple systems more efficient.

STOLEN CREDENTIALS

The compromise is traced to a vulnerability on the web server. Forensic analysis reveals that some of the attacker's tools (i.e. a modified SSH daemon) are still present on the asset.

What is the top priority to eradicate the threat?

A) Isolate and reimage the compromised server
B) Reset all admin credentials
C) Patch the web server vulnerability
D) All of the above

Is patching alone enough? or are reimaging and credential resets also necessary to ensure the attacker is fully removed.

Answer: D

STOLEN CREDENTIALS

The attacker has been using the stolen credentials to access the database server, but the web server is still operational.

What immediate containment action could be used to stop this lateral movement?

A) Disable the admin account
B) Disconnect the affected servers from the network
C) Block all outbound traffic from the web server
D) Shut down the web server

Explore the trade-offs—disabling the account stops the attacker but disrupts admin access, while isolating the server might buy time without fully containing the threat.

This really depends on the criticality and nature of the service in question.

Sometimes taking the service down is just not an option. And in these cases I would hope a DRP is in place, with a secondary instance of the platform ready to be put into production.

But in most cases the

Answer: B

STOLEN CREDENTIALS

The web server has been recovered from a known good backup, but the database server was accessed by the threat actor, and trust in the admin credentials for both servers is compromised.

What is the most critical recovery step to safely restore operations?

A) Restore the web server from a known good backup
B) Implement MFA for all admin accounts
C) Monitor systems for unusual activity post-recovery
D) Validate the integrity of the database server

Highlight why MFA and monitoring are essential to prevent recurrence, but this question focuses on service recovery.

The most important aspect to bringing the service back up would be to ensure that no data was tampered with.

Answer: D

STOLEN CREDENTIALS

The incident exposed weak patching practices and lack of credential protections, costing our organization downtime and potential data loss.

What key control(s) should be implemented to prevent this type of incident occurring in the future?

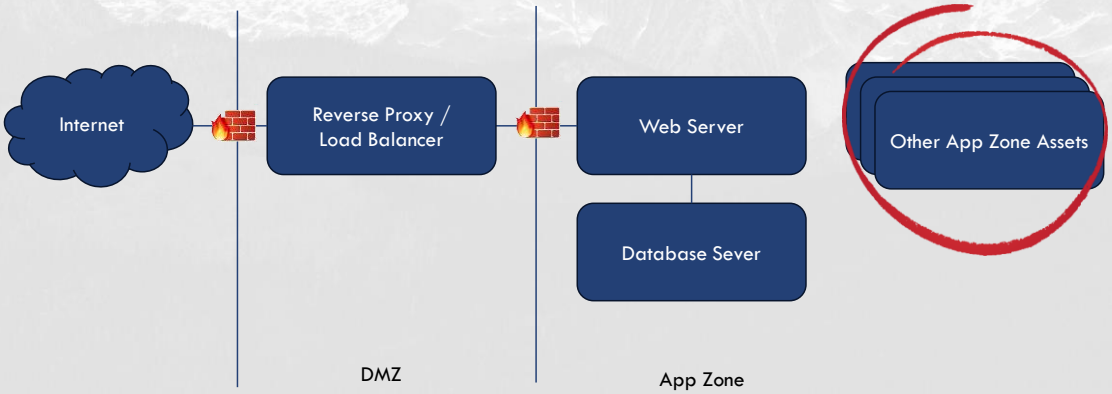
A) Enforce regular vulnerability scanning and patching
B) Require MFA for all privileged accounts
C) Segment critical servers from each other
D) All of the above

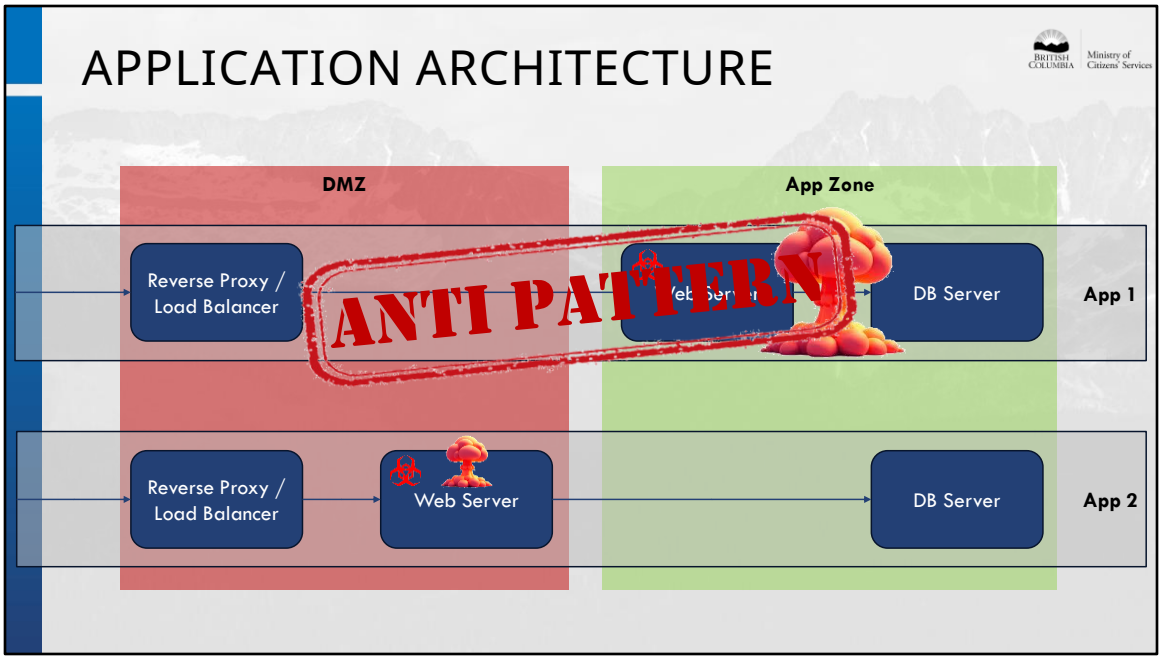
Tie our choice back to how it strengthens the preparation phase, preventing both the initial breach and the lateral spread.

Answer: D

PART 3 – LATERAL MOVEMENT

On closer examination of the application architecture. The webserver is hosted in the application zone, along with multiple other ministry assets. The compromised admin account is also used to manage these unrelated systems/services, forcing the scope of the investigation to be expanded.





App 1 – we have a reverse proxy in the datacenter's DMZ zone, and a web server and associated DB server in the application zone.

Quick show of hands, who owns or admins an application that follows this general pattern?

A reverse proxy or load balancer is not a security control. It will blindly forward web traffic to its web server(s).

<anim>
This means that if a malicious payload is aimed at the site, the attack will flow straight through the reverse proxy and the first port of call is the web server.
This is bad news if your webserver is one of many in the app zone.
Because if the attack is successful, the attacker is dropped straight into this network, alongside other servers!
Your blast radius now becomes everything in the zone that this server can talk to.
This risks the compromise of IDIR credentials, making lateral movement to other more critical networks, much easier.

<anim>
In short your blast radius is large!

<anim>
Instead, let's move the webserver from the application zone to the DMZ, where it belongs.

<anim>
In app2 the same webserver compromise keeps the attacker in the DMZ. The credentials for DMZ assets are not organization wide, IDIR credentials, and access from the DMZ to any of the other zones is much more restrictive.
Now the only way for an attacker to get a foothold in the app zone, would be to compromise the webserver and then to find another vulnerability in the DB Server, greatly reducing their probability of success.

<anim>
So with this architecture, in the event of a webserver compromise, the blast radius is contained within the DMZ, which is what the DMZ is for.

<anim>
So in summary, this first app architecture is an anti-pattern. It negates the zoning model in our datacenter and ultimately turns the app zone into a DMZ. This erodes the security posture of our organization.
We know that this architecture exists in our environment, and we are actively looking for and working with application owners to remediate this legacy anti-pattern.

LATERAL MOVEMENT

BRITISH COLUMBIA Ministry of Citizens' Services

Today it is common practice to use the same single-factor admin or service credential administer multiple systems/services.

In addition, of these systems can be accessed from, or have access to, other networks.

Given an admin account compromise on a single system, how many other systems could be accessed in your organization?

This one is rhetorical, but in all probability the answer to this question is not zero.

PART 4 – DATA EXFILTRATION

A cyber security partner informs us that sensitive citizen data (e.g. names, account numbers, and transaction histories) is being auctioned on the deep-web. The breach likely occurred weeks ago, pre-dating the web defacement.

This was likely an attempt to distract the response teams and cover up the theft.

This final part of our scenario escalates the impact of the incident by introducing a data breach event.

DATA EXFILTRATION

A cybersecurity partner alerts us after spotting our data on a deep-web auction site. Additional log analysis reveals unusual database queries starting approximately a month ago.

What's the first step to identify how the data was exfiltrated?

A) Analyze database access logs for anomalies
B) Scan all systems for malware or backdoors
C) Trace the deep-web auction to the attacker
D) Interview IT staff about recent changes

Historical log analysis and log retention is critical when the breach isn't active, versus focusing on current system scans or external clues.

Answer: A

DATA EXFILTRATION

The investigation reveals that the attacker used the compromised admin credentials to extract and modify data, months prior to the defacement.

How would you eradicate the root cause of this breach?

A) Change the DB credentials
B) Audit the integrity of the information in the DB
C) Conduct full system reimages
D) A and C

We could debate whether changing the DB credentials alone is sufficient or if broader audits and reimaging are needed to ensure no lingering access remains.

This question focuses on eradication so validating of the integrity of our data will be performed during the recovery phase.

Answer: D

DATA EXFILTRATION

The organization has firewalls, antivirus, and basic logging in place, but no data loss prevention (DLP) tools or dark web monitoring services were implemented.

Which other preparation measures could have most effectively prevented or detected this data exfiltration earlier?

A) Deploying DLP software to monitor data outflows
B) Subscription to a dark web monitoring service
C) Encrypting all sensitive customer data at rest
D) Conducting regular security audits

Consider how proactive monitoring (DLP or dark web services) versus encryption could have changed the timeline or impact of the breach.

B) Doesn't help us with detecting or preventing the exfiltration.
C) Encryption at rest only helps us in the event of e.g. physical theft of the databases hard drives. If the data is online, it is available in its cleartext form.
D) Regular security audits *may* have picked something up, but this is an after the fact detection control, and would not prevent the exfiltration.

Answer: A

DATA EXFILTRATION

The source of the data breach, while suspected, isn't yet confirmed, but the data is already exposed, and the attacker might still have access to internal systems.

What is the best immediate containment action given the uncertainty?

A) Lock down all database access
B) Reset all admin and user credentials
C) Block all outbound network traffic
D) Take all systems offline temporarily

Again this one is tricky as we need to strike a balance between slowing the attacker down (if they're still inside) and maintaining business operations, given the data has already left the building.

A) Doesn't buy us much as the data has already been stolen
B) This doesn't address containment – what if the attacker has created additional users?
C) Web traffic is only one method of communication.

All things being equal, the best response in this case is

Answer: D

DATA EXFILTRATION

The breach is contained, but citizen trust is damaged. The service must resume operations while addressing the exposed data.

What is the most critical recovery step to regain control and trust?

A) Verify system and data integrity before restoring service
B) Deploy DLP tools to prevent future data exfiltration
C) Notify affected citizens
D) A and C

We must weigh the importance of client communication and preventive measures against technical restoration, especially with the data already on the dark web.

Answer: D

DATA EXFILTRATION

In addition to reputational damage the breach has also incurred significant disruption and cost.

What would you do to prevent future breaches of this application?

A) Implement real-time data egress monitoring
B) Regularly audit DB and web access logs
C) Train staff on secure configuration practices
D) Invest in dark web threat intelligence

This one really ties back to preparation - Given what we now know, which choice will most likely allow us to avoid another incident?

Answer: Trick question! A case can be made for any and all of these options.

A) If your application handles highly structured data, such as financial information, real-time data egress monitoring may be the first thing to focus on.
B) If you have a small but highly privileged user base, regular auditing of DB and web logs may be your first stop.
C) If your application is built inhouse, and your team does not have a lot of security experience, training would be a great way to increase the overall security posture of your application.
D) If your application handles highly sensitive or valuable data, monitoring the dark web through threat intel feeds could give you an early warning system for potential breaches.

But only you can truly understand your domain, your teams' skillsets, the nature of your application, and last but not least, your real-world constraints.

So, based on all of these factors, what would *you* start with?

WHY PICERL MATTERS

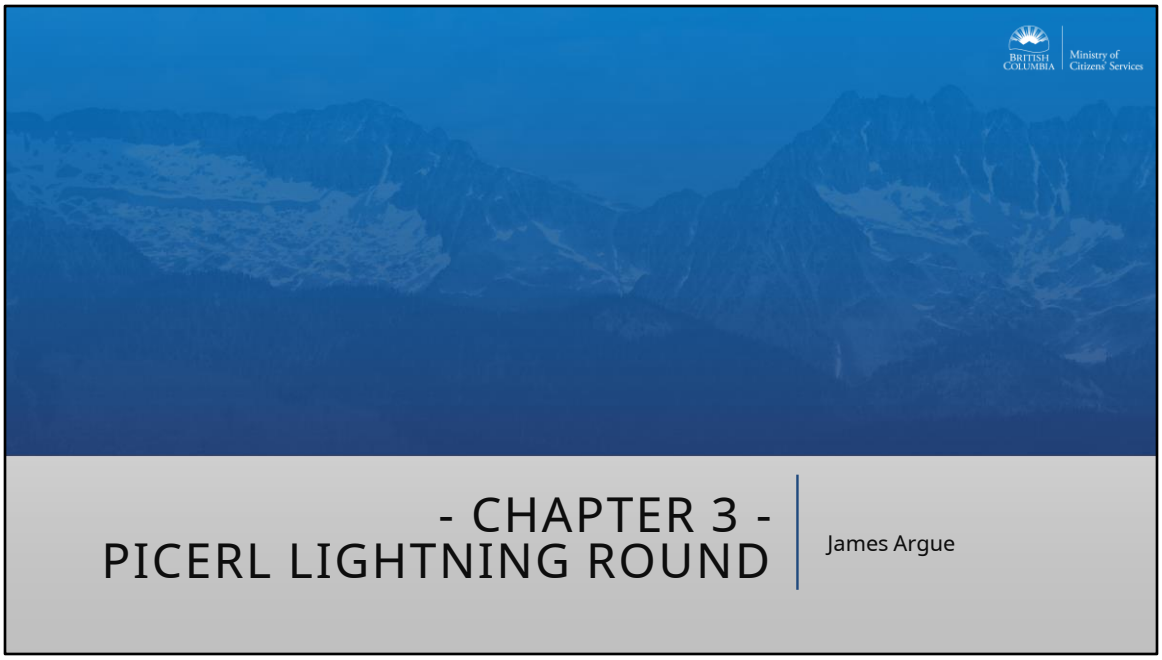
BRITISH COLUMBIA Ministry of Citizens' Services

The PICERL process is vital as it provides a clear, structured framework for tackling cyber incidents.

From preparation to lessons learned, it ensures rapid detection, effective containment, and full recovery while minimizing damage.

Following the PICERL process ensures consistency of response, strengthens defenses and drives continuous improvement—making it an essential tool in the fight against our adversaries.

In conclusion.



- CHAPTER 3 - PICERL LIGHTNING ROUND

James Argue

S3 Q1

Shutting down an affected server

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q2

Contracting a third-party company for forensic and IR services

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q3

Requesting logs to help confirm an attack occurred

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q4

Tabletop exercise

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q5

Review phishing playbook

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q6

Review improvements for phishing playbook

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q7

Scan datacenters for vulnerabilities

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q8

Find vulnerable application that is suspected to have been exploited

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q9

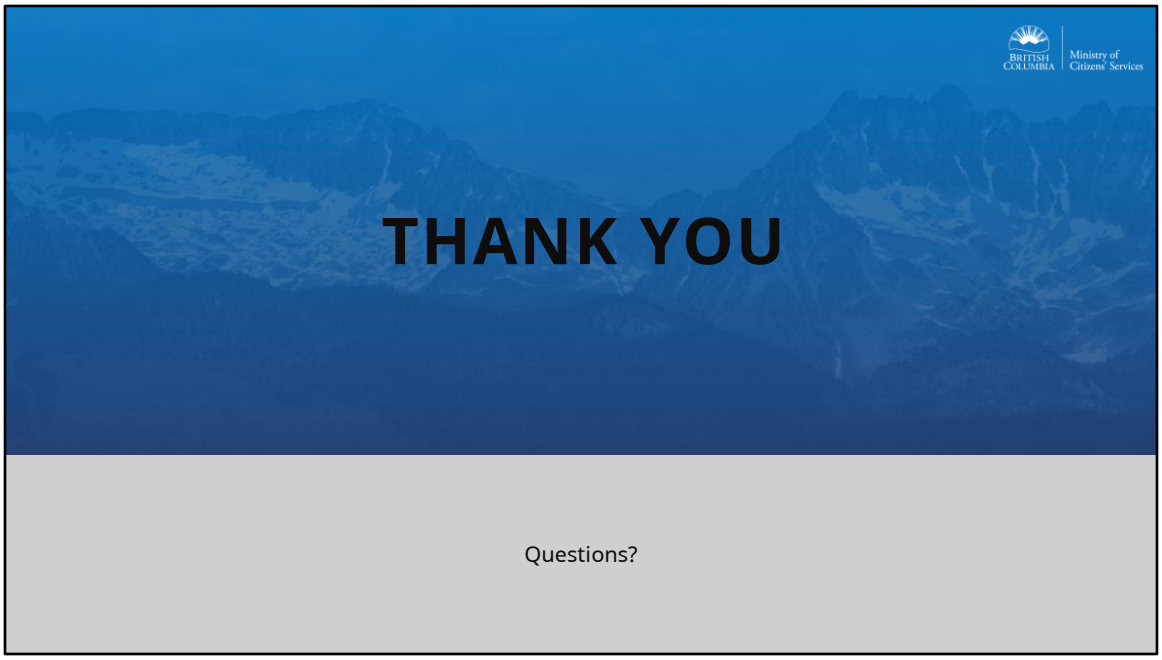
Meet with executive about improving log analysis skills and technology

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

S3 Q10

Check access logs of servers around suspected compromised server

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned


BRITISH COLUMBIA
Ministry of Citizens' Services
THANK YOU
Questions?