SIGS Purple Team Workshop

Welcome & Introduction

Who are we?

Thomas Spinnler
Senior Consultant at Pyopa GmbH & Lecturer Cyber Defence at Hochschule Luzern

Olivier Lamotte
Product Manager - Incident Response at Roche

Mihhail Sokolov
Information Security Analyst - Global Security at Roche

Jan Brons
Co-Founder & Cyber Security Expert at Kleeo GmbH

Marc Willaredt
Co-Founder at Kleeo GmbH

Introduce Yourself to Your Table Mates

Logistics & Breaks & Apero (Gabi)

Timetable

Time	Activity
09:00 - 09:10	Welcome and introduction to the workshop
09:10 - 09:30	Participants set-up (technical and tables/roles)
09:30 - 09:45	Kick-off from Table Top
09:45 - 10:00	Coffee break
10:00 - 11:15	CTI exercise
11:15 - 12:30	Phase 1: Start of the Attack
12:30 - 13:30	Lunch Break
13:30 - 14:45	Phase 2: Domain Compromise
14:45 - 15:00	Coffee Break
15:00 - 16:15	Phase 3: Critical Impact
16:15 - 16:45	Analyse results
16:45 - 17:00	Closing Remarks

Introduction to the Workshop

Participants Set-Up

Tabletop Introduction

Introduction to the company

You are part of Basel Financial Solutions AG, a medium sized digital bank in Switzerland providing innovative financial solutions for businesses and individuals.

B2B Services

- Finance Platform
- Easy Operations
- Asset Management

B2C Services

- Digital Banking
- No-Fee Payments
- Low-Fee Investment

350+
Employees

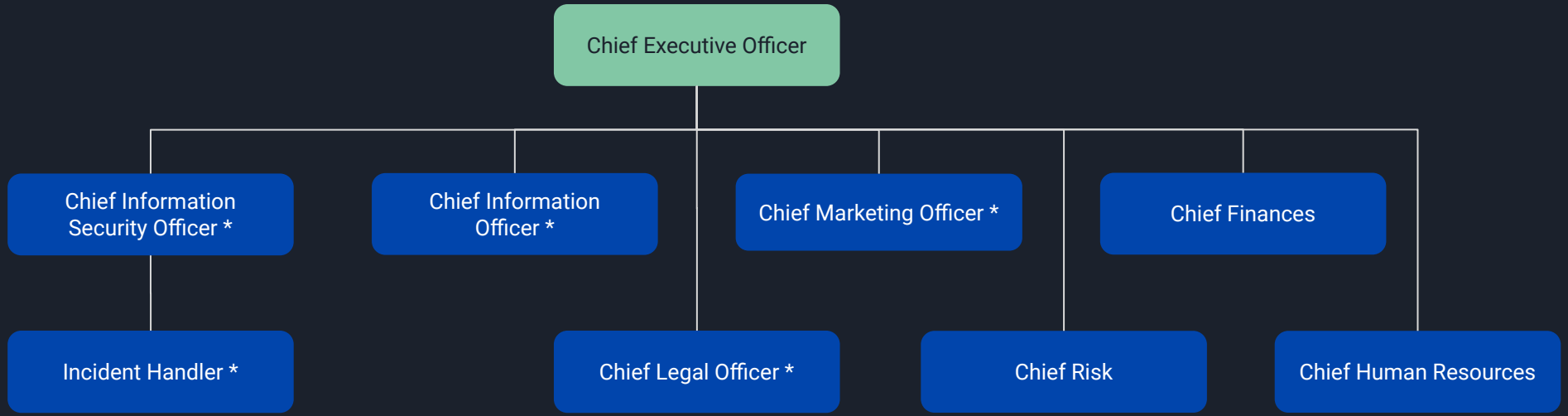
100m+
Yearly revenue

5bn+
Assets under management

500+
Endpoints

Organizational Chart

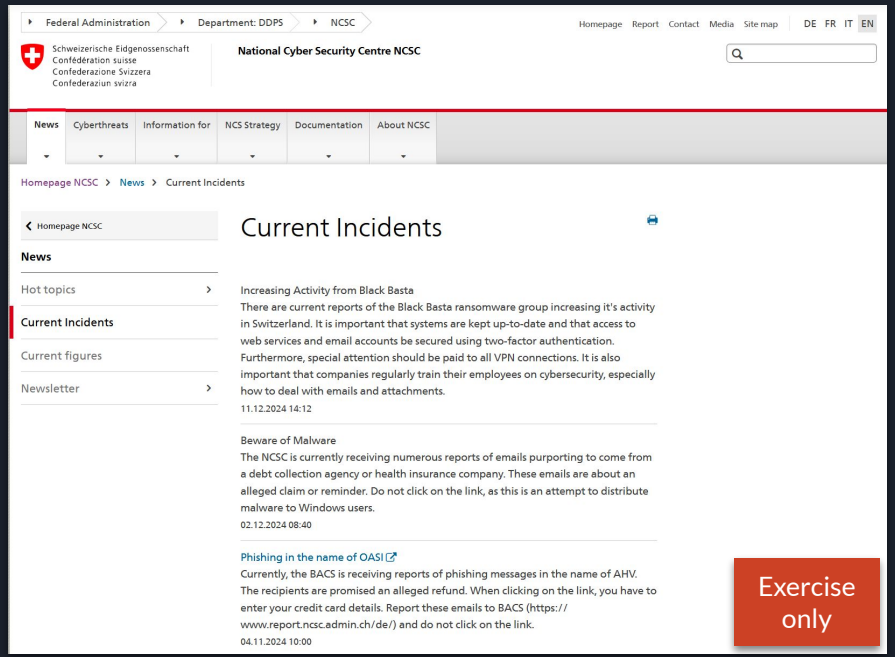
For this workshop, a simplified organizational chart for the imaginary bank will be used.



** roles represented during the tabletop exercise*

Setting the Scene

Earlier this week, the Swiss National Cyber Security Center (NCSC) issued a warning regarding the increased activities of the notorious cyber criminal group Black Basta.



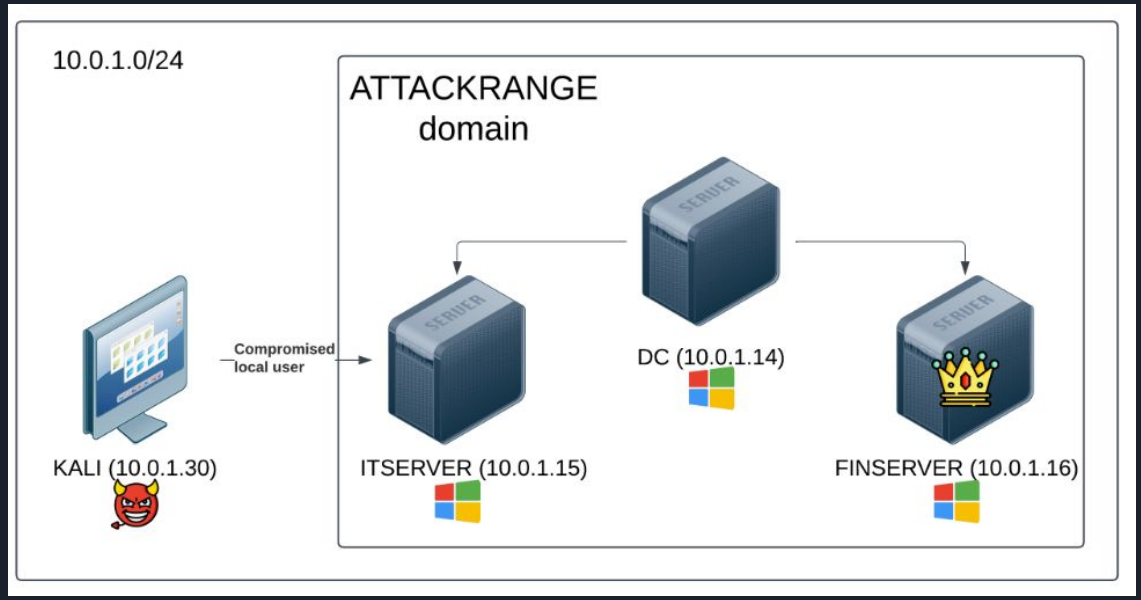
Cyber Threat Intelligence Introduction

Coffee Break until 10:15

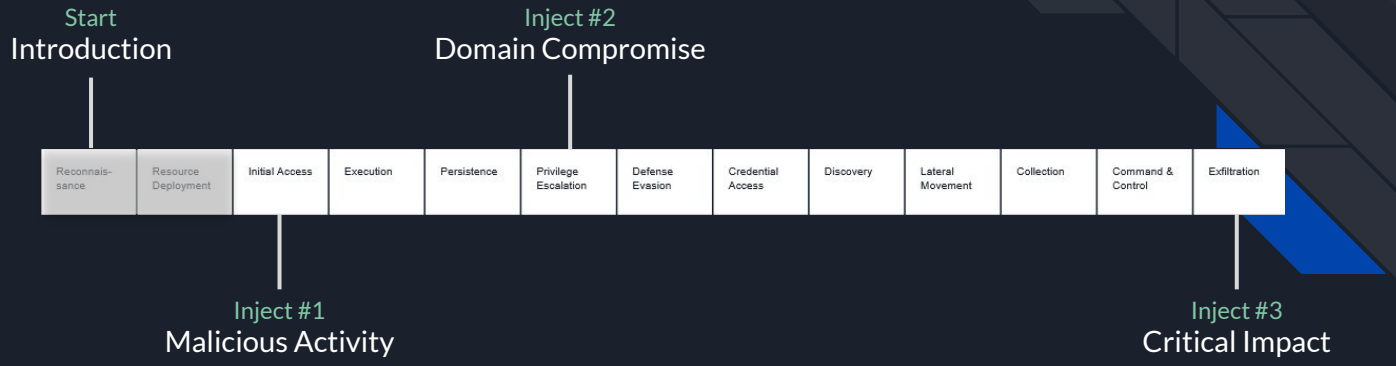
Cyber Threat Intelligence Exercise

Emulation Phase 1
Red & Blue Teaming & Tabletop Exercise

SAR Overview



Phase 1:
Malicious Activity



Red Emulation

Blue Team

Tabletop Exercise - Expectations

What you can expect

- Incident Scenario based on Red & Blue team actions
- Active discussion and decision-making
- Periodic injects to evolve the scenario

Rules of engagement

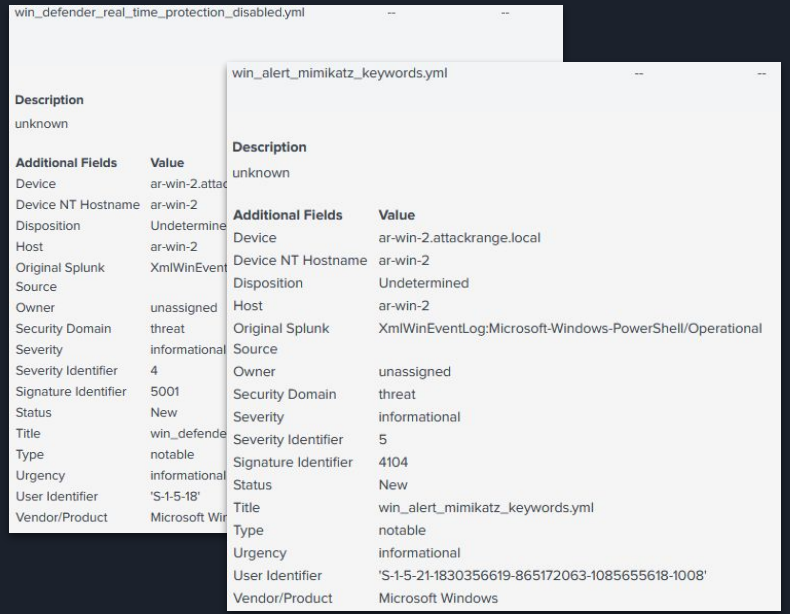
- Do not fight the scenario
- Actively engage in the discussions
- Read your role cards carefully and keep them in mind during discussions

TTX Inject #1: Malicious Activity

The Security Operations Center has observed activities on one of the bank's Windows machines. There are several related alerts correlated by the SOC indicating local escalation of privileges, evasion of defensive tooling and an attempt to gain access to further credentials in the company.

Discussion Guidelines

1. **Assemble:** Who are the roles required to overcome this situation?
2. **Information Gathering**: What happened? How severe is this incident based on the presented information?
3. **Responsibility:** Who should pick up this information and further follow-up? Who is in the lead?
4. **Communication**: Decide who is informed about these developments. What would you communicate? Adjustments for non-technical roles?
5. **Risk Assessment**: What are the dangers posed by the situation? How can these risks be quantified and addressed?



win_defender_real_time_protection_disabled.yml -- --

Description

unknown

Additional Fields	Value
Device	ar-win-2.attac
Device NT Hostname	ar-win-2
Disposition	Undetermine
Host	ar-win-2
Original Splunk Source	XmlWinEvent
Owner	unassigned
Security Domain	threat
Severity	informational
Severity Identifier	4
Signature Identifier	5001
Status	New
Title	win_defende
Type	notable
Urgency	informational
User Identifier	'S-1-5-18'
Vendor/Product	Microsoft Wi

win_alert_mimikatz_keywords.yml -- --

Description

unknown

Additional Fields	Value
Device	ar-win-2.attackrange.local
Device NT Hostname	ar-win-2
Disposition	Undetermined
Host	ar-win-2
Original Splunk Source	XmlWinEventLog:Microsoft-Windows-PowerShell/Operational
Owner	unassigned
Security Domain	threat
Severity	informational
Severity Identifier	5
Signature Identifier	4104
Status	New
Title	win_alert_mimikatz_keywords.yml
Type	notable
Urgency	informational
User Identifier	'S-1-5-21-1830356619-865172063-1085655618-1008'
Vendor/Product	Microsoft Windows

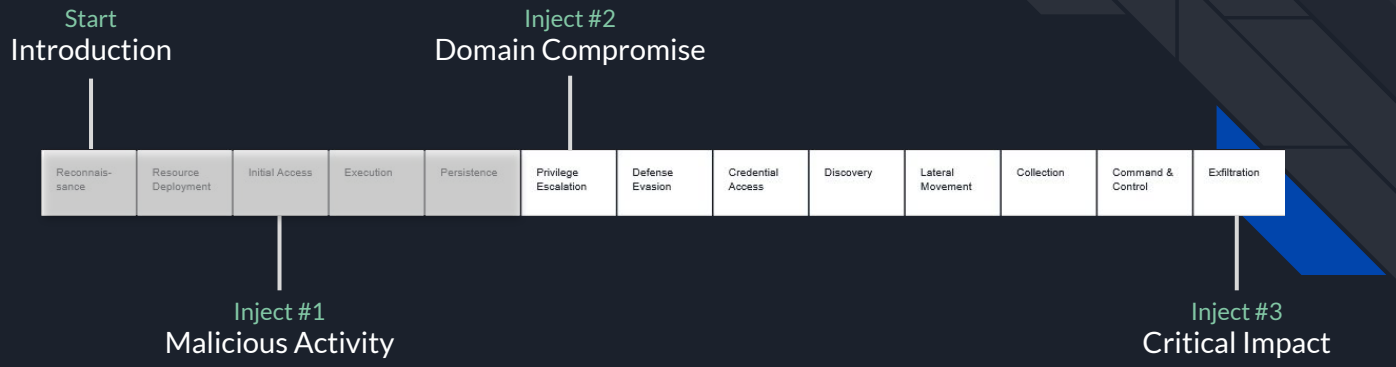
Lunch Break

Refresher: Timetable

Time	Activity
09:00 - 09:10	Welcome and introduction to the workshop
09:10 - 09:30	Participants set-up (technical and tables/roles)
09:30 - 09:45	Kick-off from Table Top
09:45 - 10:00	Coffee break
10:00 - 11:15	CTI exercise
11:15 - 12:30	Phase 1: Start of the Attack
12:30 - 13:30	Lunch Break
13:30 - 14:45	Phase 2: Domain Compromise
14:45 - 15:00	Coffee Break
15:00 - 16:15	Phase 3: Critical Impact
16:15 - 16:45	Analyse results
16:45 - 17:00	Closing Remarks

Emulation Phase 2
Red & Blue Teaming & Tabletop Exercise

Phase 2:
Domain Compromise



Red Emulation

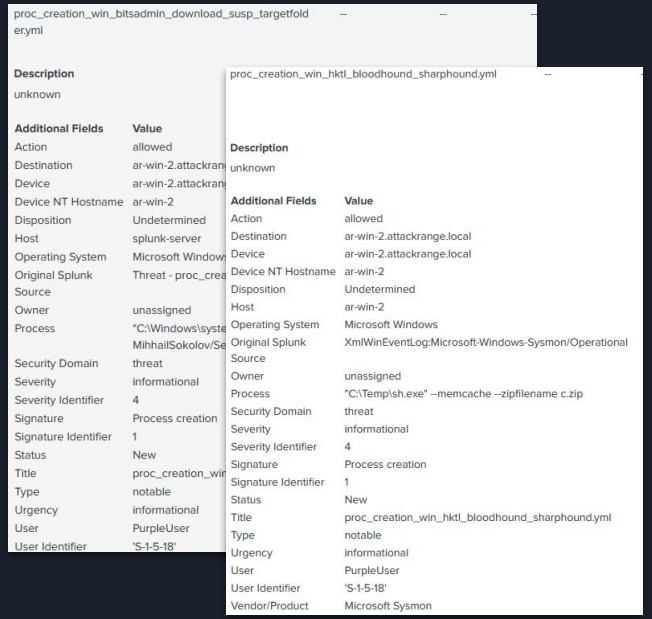
Blue Team

TTX Inject #2: Domain Compromise

The attack has further evolved and the adversaries gained access to the domain by abusing locally stored hashed credentials. This allowed the attacker to gain information about the environment and reset domain administrator passwords giving them full control of the domain.

Discussion Guidelines

1. **Risk & Impact:** How would you assess the situation in terms of risk to business continuity? What are the immediate and long-term impacts?
2. **Regulatory**: What must be considered at this stage when it comes to informing regulatory bodies?
3. **Containment & Recovery**: How can an attack at this stage be contained and recovered? Who would you engage in this situation?
4. **Communications**: Which internal and external stakeholders should be informed? What information is shared?



proc_creation_win_bitsadmin_download_susp_targetfolder.yml

Description
unknown

Additional Fields	Value
Action	allowed
Destination	ar-win-2.attackran
Device	ar-win-2.attackran
Device NT Hostname	ar-win-2
Disposition	Undetermined
Host	splunk-server
Operating System	Microsoft Window
Original Splunk Source	Threat - proc_crea
Owner	unassigned
Process	"C:\Windows\syste MihhailSokolov/Se
Security Domain	threat
Severity	informational
Severity Identifier	4
Signature	Process creation
Signature Identifier	1
Status	New
Title	proc_creation_wi
Type	notable
Urgency	informational
User	PurpleUser
User Identifier	'S-1-5-18'

proc_creation_win_hktl_bloodhound_sharphound.yml

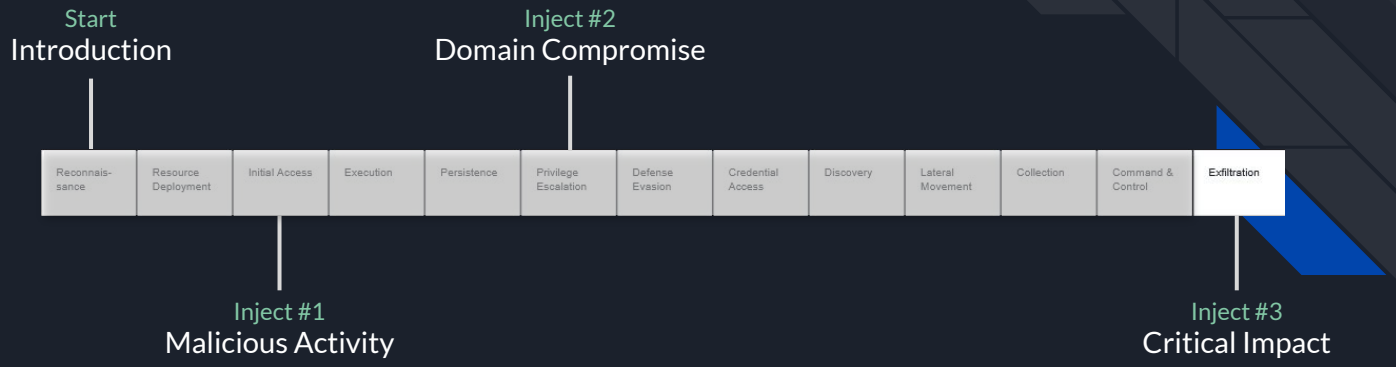
Description
unknown

Additional Fields	Value
Action	allowed
Destination	ar-win-2.attackrange.local
Device	ar-win-2.attackrange.local
Device NT Hostname	ar-win-2
Disposition	Undetermined
Host	ar-win-2
Operating System	Microsoft Windows
Original Splunk Source	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Owner	unassigned
Process	"C:\Temp\sh.exe" --memcache --zipfilename c.zip
Security Domain	threat
Severity	informational
Severity Identifier	4
Signature	Process creation
Signature Identifier	1
Status	New
Title	proc_creation_win_hktl_bloodhound_sharphound.yml
Type	notable
Urgency	informational
User	PurpleUser
User Identifier	'S-1-5-18'
Vendor/Product	Microsoft Sysmon

Coffee Break until 15:00

Emulation Phase 3
Red & Blue Teaming & Tabletop Exercise

Phase 3:
Critical Impact



Red Emulation

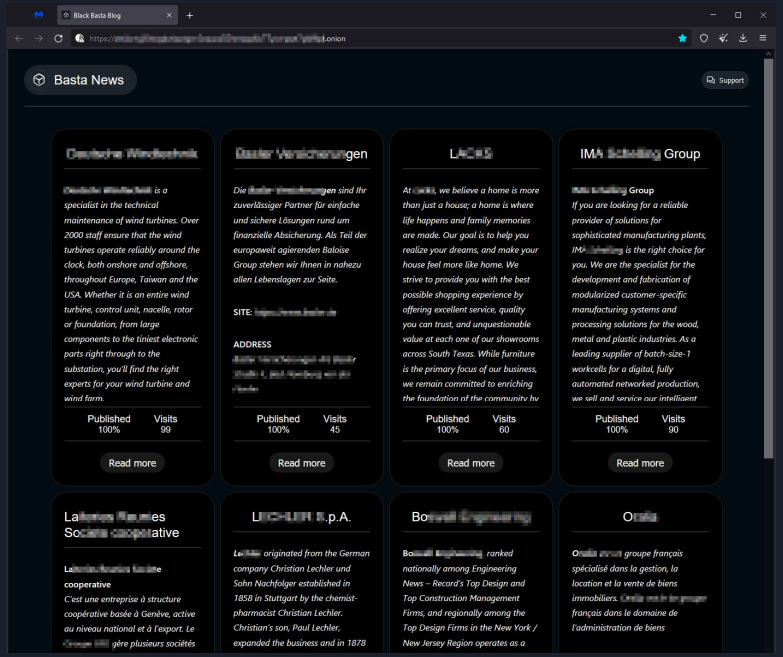
Blue Team

TTX Inject #3: Critical Impact

Critical data has been exfiltrated by the adversary and a threat to publish the data was posted on Basta News. In parallel, Basel Financial Solutions AG was contacted by the threat group demanding a ransom of 60 BTC, further threatening to encrypt all domain data.

Discussion Guidelines

1. **Assessment:** How would you go about assessing the affected data? How to determine it's criticality?
2. **Regulatory Disclosure**: Who and how must regulatory bodies be involved at this point?
3. **Customer Communication**: Would you inform customers at this point in the attack?
4. **Ransom**: How many systems are encrypted? Do you negotiate with the threat actor and consider paying the ransom?
5. **Recovery**: What could an approach to start recovery look like? Which aspects would you consider?



Results & Improvements Analysis

TTX: Key Considerations

Things we would like you to take with you from the TTX….

- Clearly aligned roles & responsibilities
- Crisis Playbooks per function with most critical questions and duties listed including checklists per role for quick access
- Have a crisis team to support technical teams with managerial, legal, and communication matters
- Closely align tech and crisis team
- Incident Response Playbooks for plausible scenarios
- Legally signed off holding statements for internal communication
- Offline list with key contacts for customers, regulators, internal employees (key people), and external partners (forensic experts, etc.)
- Train and work together with your external media agency, IT forensics experts, etc.
- Conduct table-top exercises to train muscle memory, strengthen teamwork, and understand each other's strengths and roles & responsibilities.

Closing Remarks

Thank You!