



Timetable

Time	Activity
09:00 - 09:10	Welcome & Introduction
09:10 - 09:30	Set-up
09:30 - 10:00	Workshop Kick-Off
10:00 - 10:15	Coffee Break
10:15 - 11:30	CTI Exercise
11:30 - 12:30	Emulation Phase 1: Start of Attack
12:30 - 13:30	Lunch Break
13:30 - 14:30	Blue Team Deep-Dive
14:30 - 15:00	Tabletop Phase 1
15:00 - 15:15	Coffee Break
15:15 - 16:00	Emulation Phase 2: Domain Compromise & Critical Impact
16:00 - 16:45	Tabletop Phase 2 + Deep-Dive
16:45 - 17:00	Closing Remarks
17:00 - ???	Apéro



SIGS Purple Team Workshop

Welcome & Introduction





Who are we?



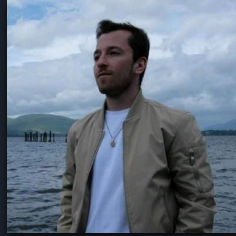
Thomas Spinnler

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



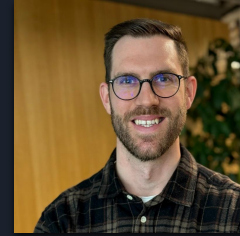
Olivier Lamotte

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 Tablemates



Logistics & Breaks





Timetable

Time	Activity
09:00 - 09:10	Welcome & Introduction
09:10 - 09:30	Set-up
09:30 - 10:00	Workshop Kick-Off
10:00 - 10:15	Coffee Break
10:15 - 11:30	CTI Exercise
11:30 - 12:30	Emulation Phase 1: Start of Attack
12:30 - 13:30	Lunch Break
13:30 - 14:30	Blue Team Deep-Dive
14:30 - 15:00	Tabletop Phase 1
15:00 - 15:15	Coffee Break
15:15 - 16:00	Emulation Phase 2: Domain Compromise & Critical Impact
16:00 - 16:45	Tabletop Phase 2 + Deep-Dive
16:45 - 17:00	Closing Remarks
17:00 - ???	Apéro

Introduction to the Workshop



Participants Set-Up



Tabletop Introduction





What we hope you get from the TTX

- Who has already conducted a Cyber Crisis Exercise?
- **Why do we do a TTX today?** Understand cross-functional collaboration under pressure. Reuse existing teams. Material cyber incidents are no longer only a CISO problem.
- **By the end of this exercise,** you'll understand the building blocks of an effective crisis response team and check your own readiness.

Take back ideas to your team / company to improve your preparedness.



Why Cyber Crisis readiness matters

Cyber incidents are no longer just a CISO's problem — they're a business-wide crisis

- Cyber attacks can escalate quickly with **global consequences** — unlike localized events (floods, terror, etc.).
- **Guaranteed media attention** can amplify damage if your response is not coordinated and professional.
- It's no longer a question of **IF**, but **WHEN** a cyber attack happens.
- Regulatory pressure is increasing: Know **who**, **when**, and **how** to notify.
- **Testing your response** is crucial — find weaknesses in communication and coordination before an actual breach.
- **Today's exercise** is a safe space to:
 - Explore what a material incident looks like.
 - Identify who communicates and when.
 - Take lessons home to improve your internal crisis playbooks.

- Do you have a Crisis Plan?
- Do the right people know their roles?
- Are your plans tested regularly?

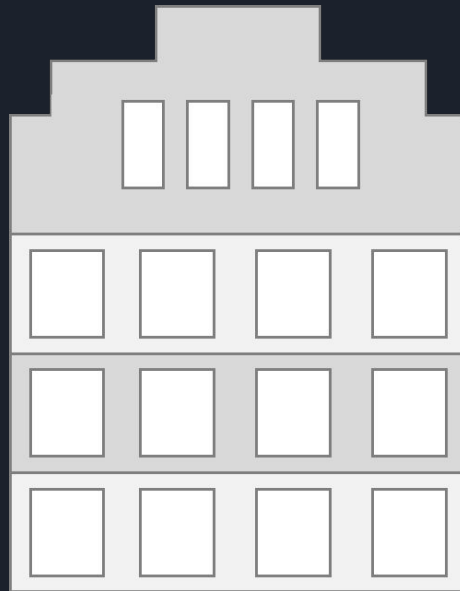


Use what you already have

You don't need to reinvent the wheel — just align and empower existing teams.

- Most organizations already have trained crisis personnel — **activate and connect** them
- SMBs benefit from flatter structures: **faster decision-making**
- Enterprises have deep expertise: **Clarify who decides and when** to avoid internal conflicts
- **Cross-functional alignment** is critical — security, legal, PR, execs, HR
- Define **roles and responsibilities** before the crisis, not during it

Global Crisis Response



Team	Responsibility	Members	Rhythm
Board of Directors (BoD)	<ul style="list-style-type: none"> Ultimate decision power and responsibility Protects shareholder 		Kept informed
Group Crisis Management Team	<ul style="list-style-type: none"> Speaks in front of media during global crisis Decides on global impact 	<ul style="list-style-type: none"> CRO CTO CFO CISO (sec. incident) 	Once a day when decision is required
Emergency Management Team	<ul style="list-style-type: none"> Ensures timely reporting to regulators globally Guides and coordinates local teams Takes more strategic decision 	<ul style="list-style-type: none"> Chief of Staff CISO Legal & Compliance Data Protection 	Mornings and evenings
Local Incident Management Team	<ul style="list-style-type: none"> Immediate response: People safety first Handles incidents locally Floods, terror attack Reporting locally in local language 	<ul style="list-style-type: none"> Local IT Compliance Officer Physical Security 	Hourly

Inform

Inform

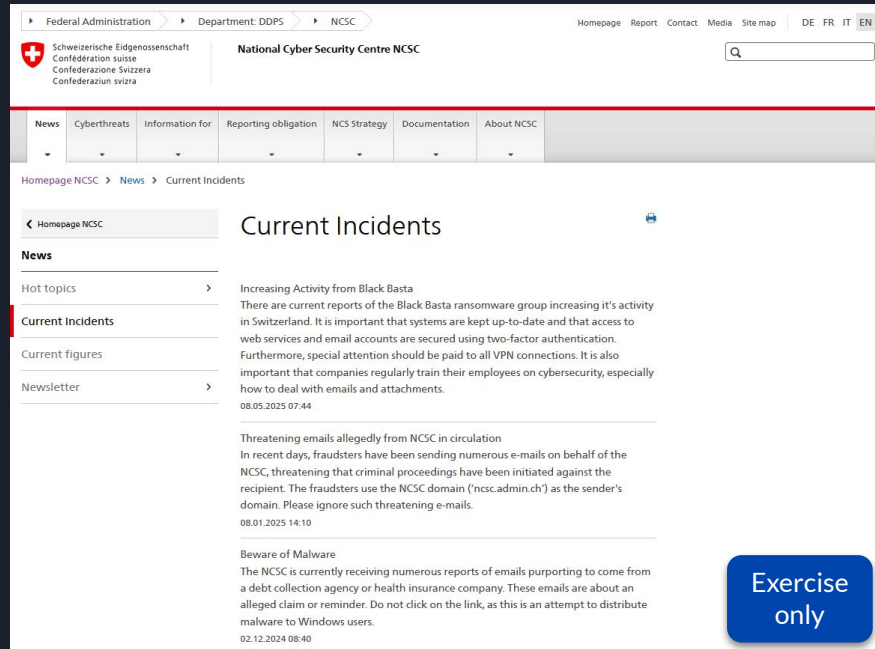
Inform

Coffee Break until 10:15



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.

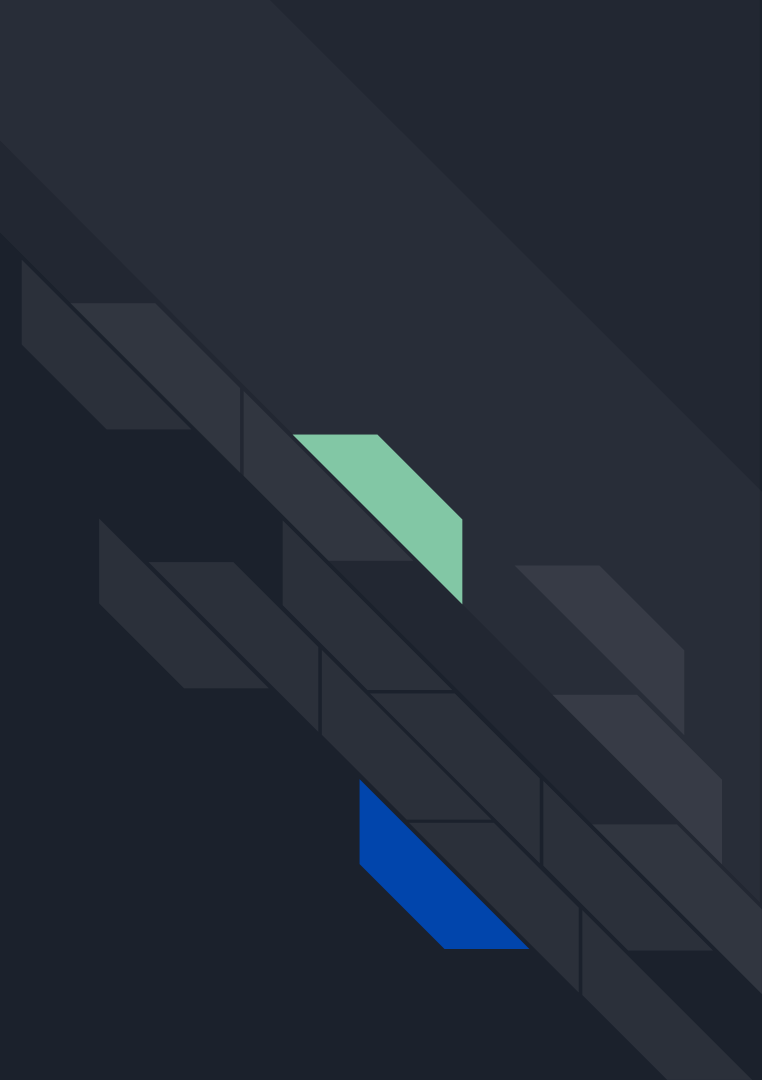


The screenshot shows the official website of the National Cyber Security Centre (NCSC) of Switzerland. The header includes navigation links for Federal Administration, Department: DDPS, and NCSC, along with language options (DE, FR, IT, EN) and a search bar. The main navigation menu lists News, Cyberthreats, Information for, Reporting obligation, NCS Strategy, Documentation, and About NCSC. The breadcrumb trail indicates the path: Homepage NCSC > News > Current Incidents. The left sidebar contains links to Homepage NCSC, News, Hot topics, Current Incidents (which is highlighted with a red bar), Current figures, and Newsletter. The main content area is titled 'Current Incidents' and features three news items:

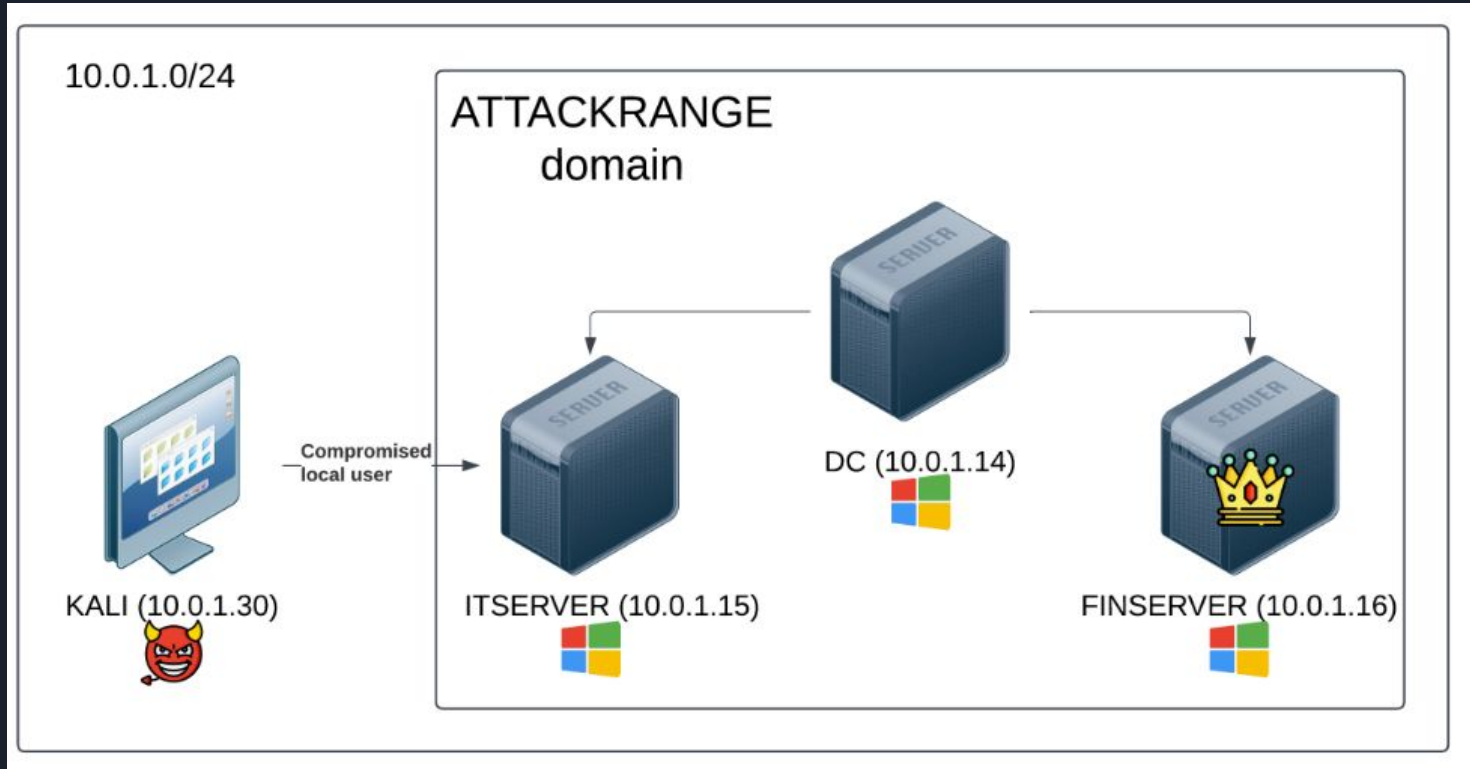
- Increasing Activity from Black Basta**
There are current reports of the Black Basta ransomware group increasing its activity in Switzerland. It is important that systems are kept up-to-date and that access to web services and email accounts are secured using two-factor authentication. Furthermore, special attention should be paid to all VPN connections. It is also important that companies regularly train their employees on cybersecurity, especially how to deal with emails and attachments.
08.05.2025 07:44
- Threatening emails allegedly from NCSC in circulation**
In recent days, fraudsters have been sending numerous e-mails on behalf of the NCSC, threatening that criminal proceedings have been initiated against the recipient. The fraudsters use the NCSC domain ('ncsc.admin.ch') as the sender's domain. Please ignore such threatening e-mails.
08.01.2025 14:10
- Beware of Malware**
The NCSC is currently receiving numerous reports of emails purporting to come from a debt collection agency or health insurance company. These emails are about an alleged claim or reminder. Do not click on the link, as this is an attempt to distribute malware to Windows users.
02.12.2024 08:40

A blue button with the text 'Exercise only' is located in the bottom right corner of the screenshot.

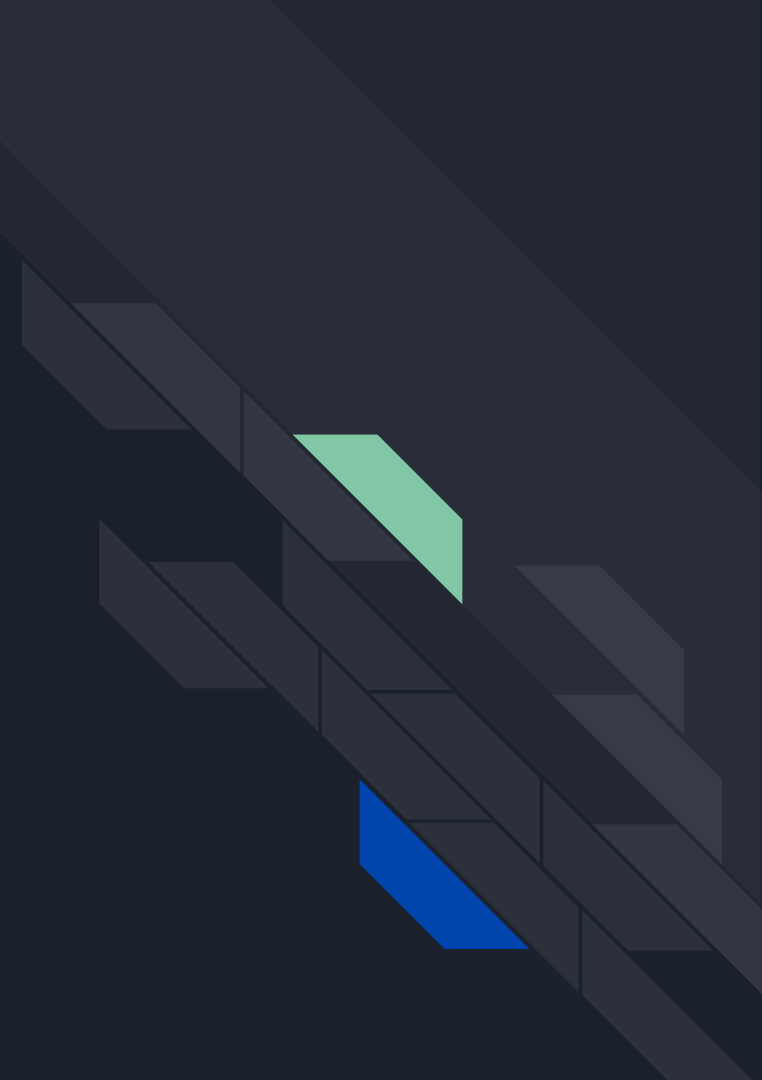
Cyber Threat Intelligence Introduction



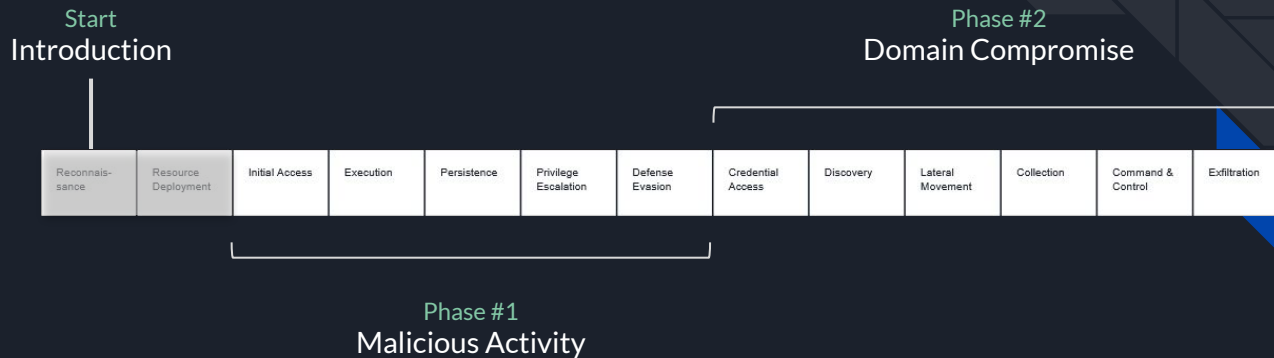
Attack Range Overview



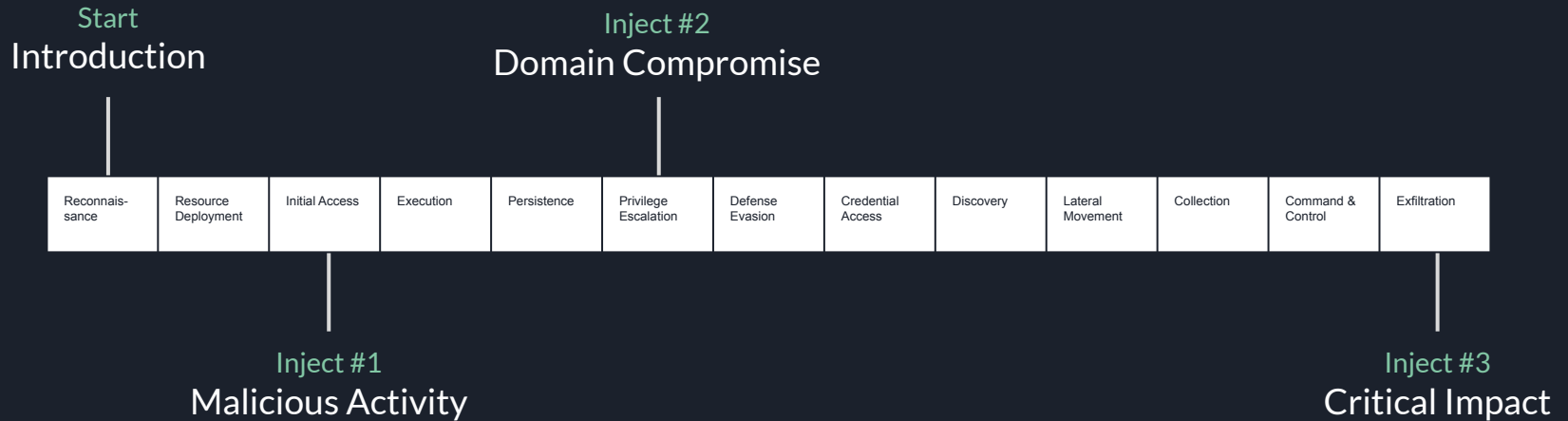
Cyber Threat Intelligence Deep-Dive



Phase 1: Malicious Activity



Tabletop Exercise - Overview



Phase 1: Red Emulation



Lunch Break





Timetable

Time	Activity
09:00 - 09:10	Welcome & Introduction
09:10 - 09:30	Set-up
09:30 - 10:00	Workshop Kick-Off
10:00 - 10:15	Coffee Break
10:15 - 11:30	CTI Exercise
11:30 - 12:30	Emulation Phase 1: Start of Attack
12:30 - 13:30	Lunch Break
13:30 - 14:30	Blue Team Deep-Dive
14:30 - 15:00	Tabletop Phase 1
15:00 - 15:15	Coffee Break
15:15 - 16:00	Emulation Phase 2: Domain Compromise & Critical Impact
16:00 - 16:45	Tabletop Phase 2 + Deep-Dive
16:45 - 17:00	Closing Remarks
17:00 - ???	Apéro

Phase 1: Blue Team Deep-Dive





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



Introduction to the company

You are part of Zurich 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

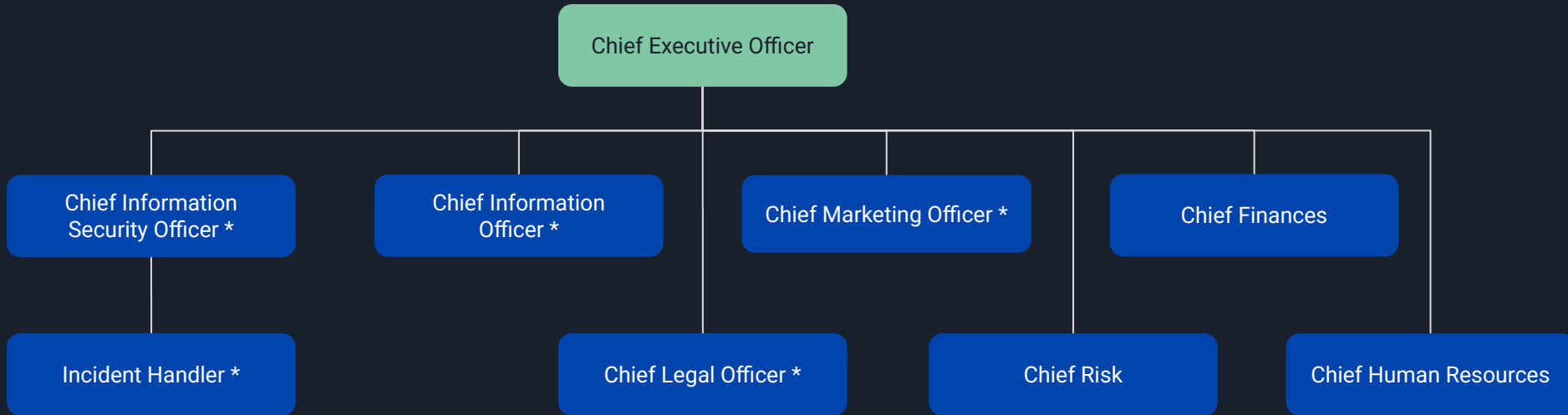
100m+
Yearly revenue

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*



Now it's your turn!

These are your TTX functions for today...

- **Chief Information Security Officer**
 - Is on top of the investigation. Gathers latest analysis information and informs the management / crisis team in an understandable way
- **Chief Information / Technology Officer**
 - Advises on technical implications and takes decision to shutdown services on CISO's demand
- **Chief Legal Officer**
 - Takes decision on legal actions such as acting on employee misbehavior, ransomware payment, incident reporting to police and regulators
- **Chief Marketing and Communication Officer**
 - Internal and external crisis communication according to predefined and pre-approved holding statements
- **Incident Handler**
 - Spokesperson to the CISO. Provides updates on investigation and analysis regularly.

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.

Team Exercise Guidelines

1. You are in a team of 5, each with an assigned role
2. Discuss how to respond to the situation using the questions on your role cards
3. Feel free to address any other relevant steps you identify
4. Write down your key decisions and agreed actions
5. Be ready to briefly present your results if selected. 2-3 tables will be asked to share their outcomes with the group

win_defender_real_time_protection_disabled.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	4
Signature Identifier	5001
Status	New
Title	win_defender_real_time_protection_disabled.yml
Type	notable
Urgency	informational
User Identifier	'S-1-5-18'
Vendor/Product	Microsoft Windows

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

Phase 2: Domain Compromise & Critical Impact



Phase 2 :Red Emulation



Phase 2 :Blue Team



Phase 2 : Tabletop Deep-Dive



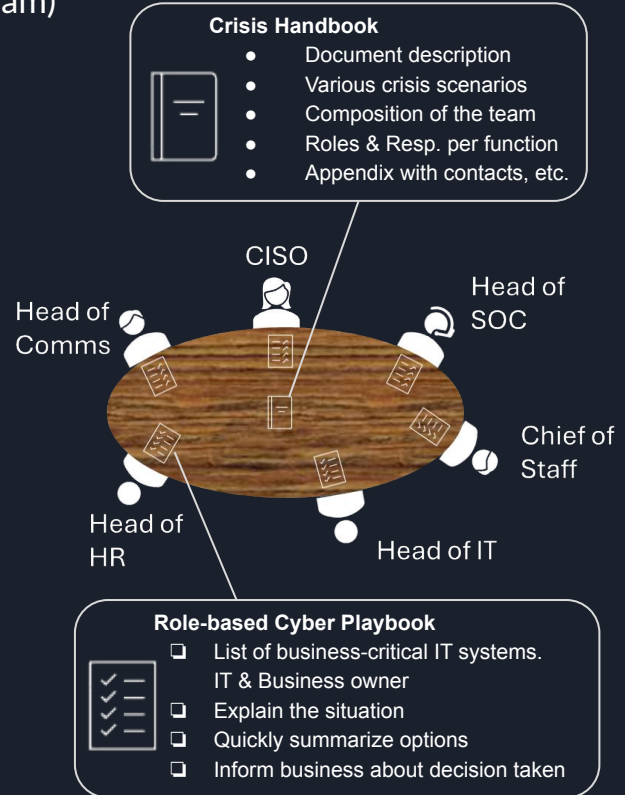
Recap: Global Crisis Response



Cross-functional team

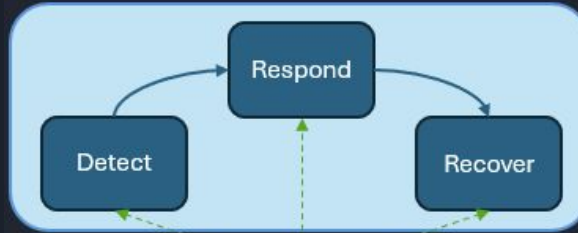
(Example could relate to the Emergency Management Team)

- Role playbooks as part of overall Crisis Handbook: **Clear roles & responsibilities** must be assigned
- Checklist with most **critical points** to consider for first **24-48 hours**
- **Important:** Appoint **deputies** for each function! There is nothing more disturbing than a (h)angry Head of IT, trust me!
- **Physical war room** with printed Crisis Handbook, R&R checklists, most important contacts (mail + phone number), maybe also bank account information, etc.



Incident Response: NIST SP 800-61r3

Incident Response



Help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications.

Lessons Learned

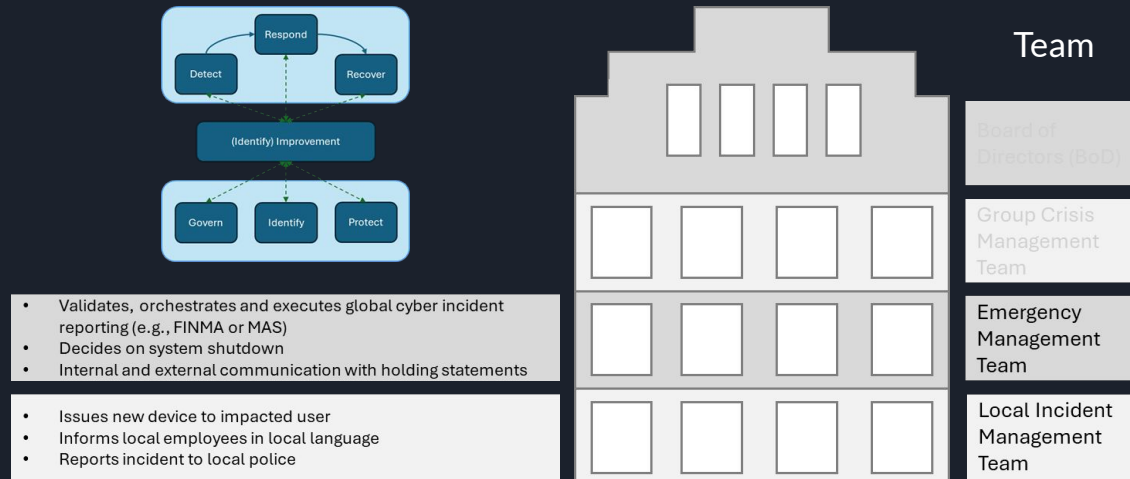


Preparation



Help organizations prevent some incidents, prepare to handle incidents that do occur, reduce the impact of those incidents, and improve incident response and cybersecurity risk management practices based on lessons learned.

Integrating Cyber Incident Response to Crisis Management



Clearly **define what a material cyber incident is**. Then, use your cross-functional crisis team in solving the cyber incident. As a CISO / Security function, you can **focus on what you do best**: Incident investigation and improving your protection capabilities. Let external communication, regulatory reporting, HR discussions, etc. be done by your experts in your firm! This is not you.

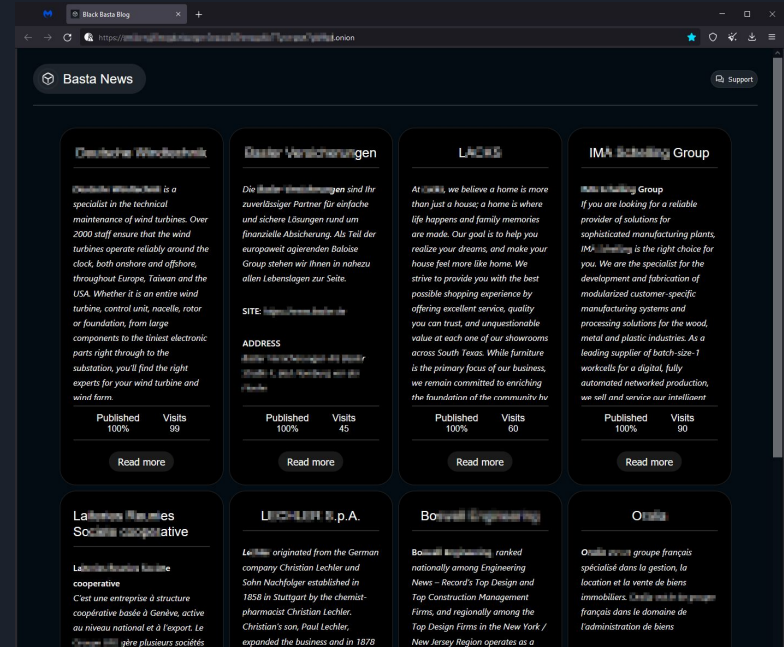


TTX Inject #2: Domain Compromise

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

Team Exercise Guidelines

1. You are in a team of 5, each with an assigned role
2. Discuss how to respond to the situation using the questions on your role cards
3. Feel free to address any other relevant steps you identify
4. Write down your key decisions and agreed actions
5. Be ready to briefly present your results if selected. 2–3 tables will be asked to share their outcomes with the group



Tabletop Results Presentation





Key learnings for participants

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

1. **Build & Structure Your Crisis Team**
 - Establish and train a cross-functional crisis team
 - Clearly define roles & responsibilities (R&R) for each member
 - Create one playbook per role with a clear, step-by-step guide
 - Integrate your Cyber Incident Response Plan into the broader Crisis Management Plan
2. **Practice & Prepare**
 - Regularly educate and test your teams — simulations provide the most effective learning
 - Involve key external partners in exercises to test real-world coordination
 - Ensure technical readiness (e.g., pre-authorized accounts/access for external experts, SIEM access)
3. **Communication Strategy**
 - Decide early on: proactive vs. reactive communication approach
 - Draft and maintain pre-approved holding statements
 - Define who is authorized to speak — internally and externally (media, website, regulators)
4. **Regulatory & Legal Preparedness**
 - Know your obligations: who to notify, what to report, and when (e.g., FINMA or global equivalents)
 - Identify and document reporting timelines across jurisdictions
 - Establish contact with law enforcement/regulators before a crisis
5. **Case Study Insight**
 - Learn from recent real-world responses (e.g., Brack.ch proactively informed customers of a potential breach, which was later ruled out — showing the value of transparency and preparedness)



Learnings from previous tabletops

Things we learned from conducting TTX with companies....

- **Have a backup:** Assign and empower a deputy — CRO's get tired, too.
- **Expect uncertainty:** Act decisively with limited information; don't wait for perfect clarity.
- **Break stalemates:** Leadership can (and must) emerge regardless of formal roles.
- **Communication strategy matters:** Proactive vs. reactive approaches shape perception (e.g., Brack case).
- **Test external support:** An IR retainer is useless if onboarding fails during a real crisis.
- **Keep critical info offline:** Store holding statements, contacts, and comms plans in secure offline locations.

Closing Remarks



Thank You!

