Microsoft - 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

Logistics & Breaks

Timetable

Time	Activity
09:00 - 09:30	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	Table-top Phase 1
15:00 - 15:15	Coffee Break
15:15 - 15:45	Emulation Phase 2: Domain Compromise & Critical Impact
15:45 - 16:30	Table-top Phase 2 + Detection Engineering Deep-Dive
16:30 - 16:45	Closing Remarks

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.

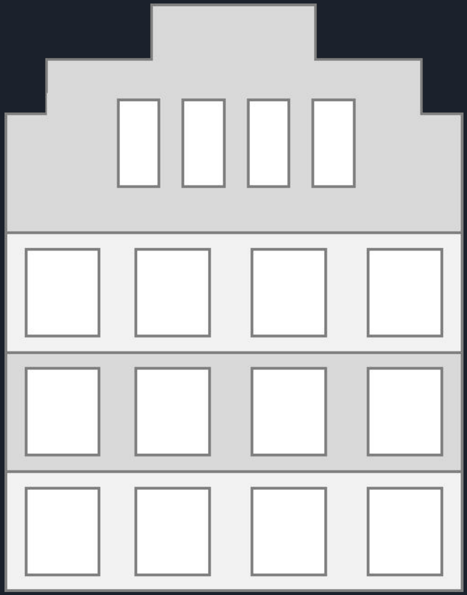
- Do you have a Crisis Plan?
- Do the right people know their roles?
- Are your plans tested regularly?

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)	- Ultimate decision power and responsibility - Protects shareholder		Kept informed
Group Crisis Management Team	- Speaks in front of media during global crisis - Decides on global impact	- CRO - CTO - CFO - CISO (sec. incident)	Once a day when decision is required
Emergency Management Team	- Ensures timely reporting to regulators globally - Guides and coordinates local teams - Takes more strategic decision	- Chief of Staff - CISO - Legal & Compliance - Data Protection	Mornings and evenings
Local Incident Management Team	- Immediate response: People safety first - Handles incidents locally - Floods, terror attack - Reporting locally in local language	- Local IT - Compliance Officer - Physical Security	Hourly

Inform

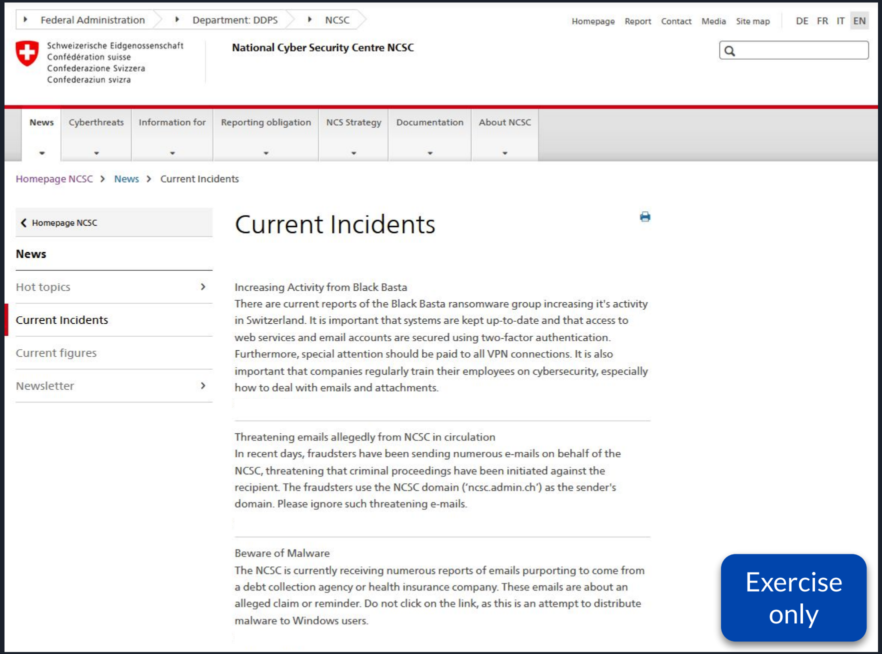
Inform

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.



Current Incidents

Increasing Activity from Black Basta
There are current reports of the Black Basta ransomware group increasing it's 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.

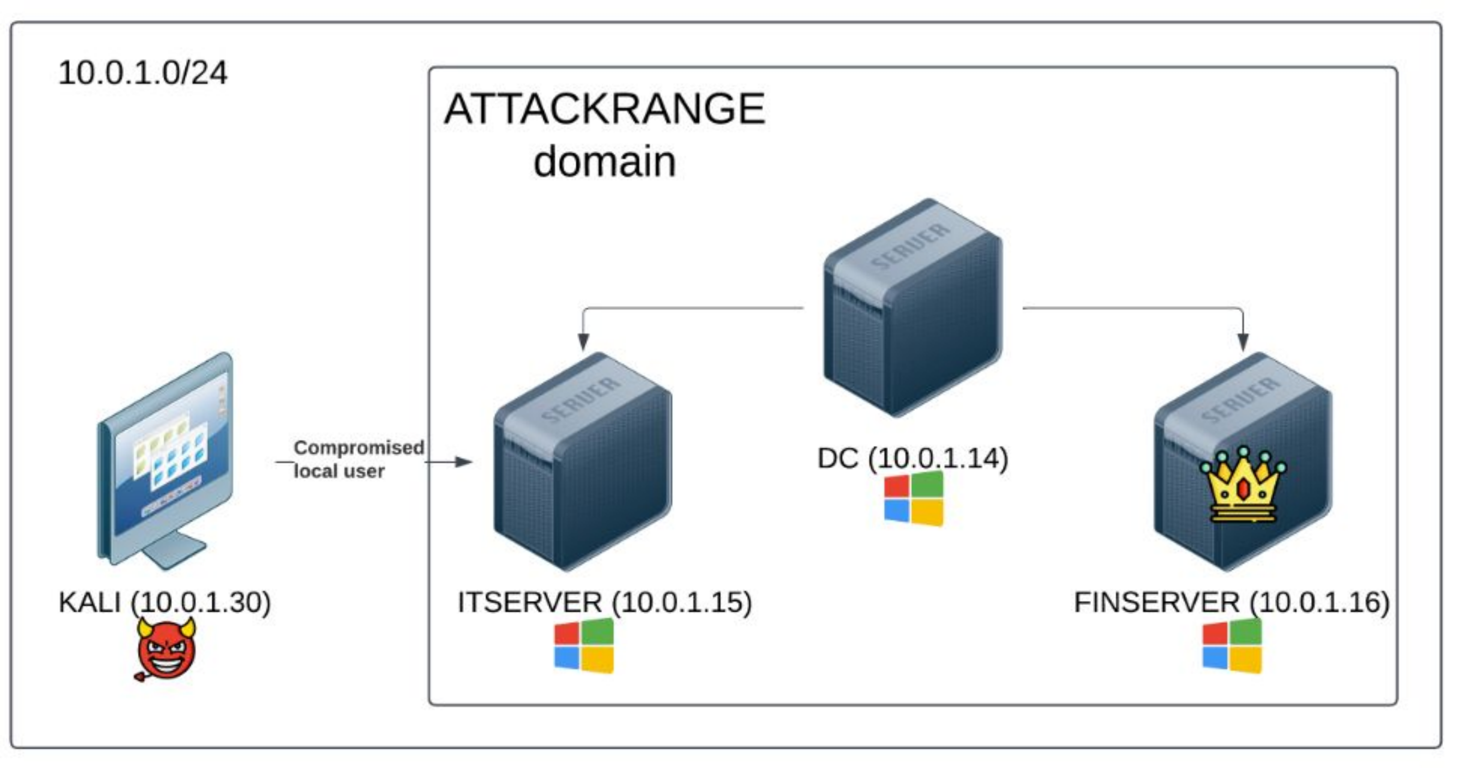
Threatening emails allegedly from NCSC in circulation
In recent days, fraudsters have been sending numerous e-mails on behalf of the NCSC, threatening that criminal proceedings have been initiated against the recipient. The fraudsters use the NCSC domain ('ncsc.admin.ch') as the sender's domain. Please ignore such threatening e-mails.

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.

Exercise only

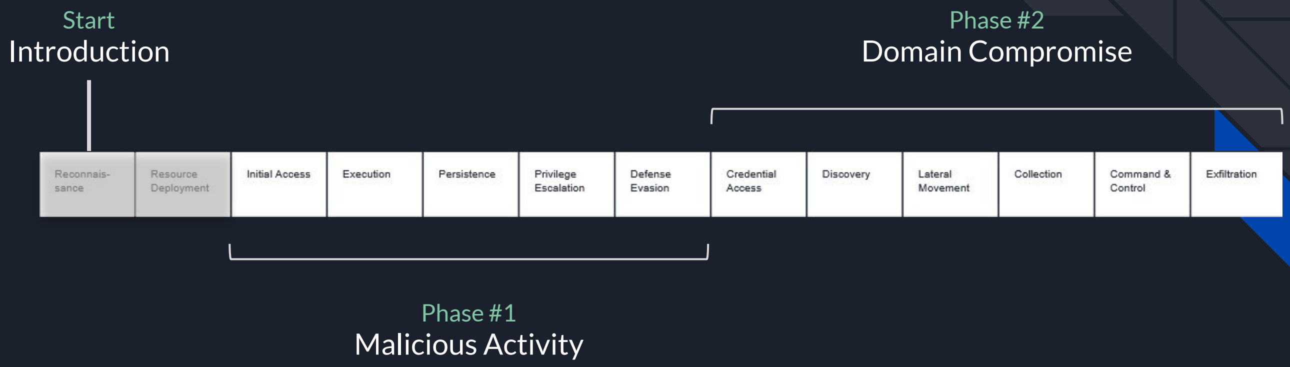
Cyber Threat Intelligence Introduction

Attack Range Overview



Cyber Threat Intelligence Deep-Dive

Phase 1:
Malicious Activity



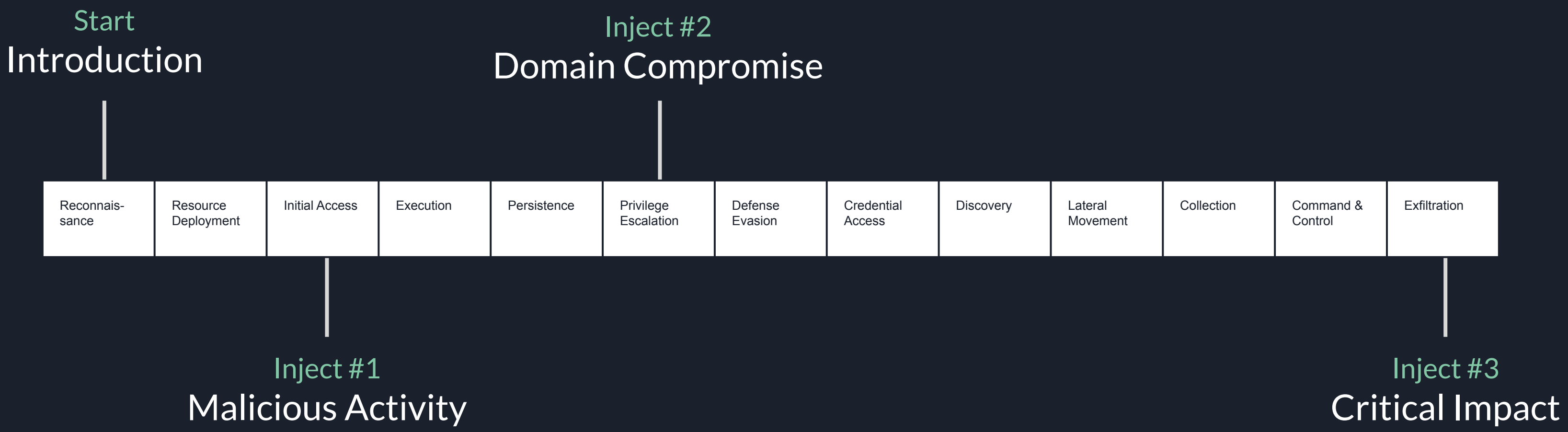
Start
Introduction

Phase #2
Domain Compromise

Reconnais-sance | Resource Deployment | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command & Control | Exfiltration

Phase #1
Malicious Activity

Tabletop Exercise - Overview



Start
Introduction

Inject #2
Domain Compromise

Reconnais-sance	Resource Deployment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration

Inject #1
Malicious Activity

Inject #3
Critical Impact

Phase 1: Red Emulation

Lunch Break

Timetable

Time	Activity
09:00 - 09:30	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	Table-top Phase 1
15:00 - 15:15	Coffee Break
15:15 - 15:45	Emulation Phase 2: Domain Compromise & Critical Impact
15:45 - 16:30	Table-top Phase 2 + Detection Engineering Deep-Dive
16:30 - 16:45	Closing Remarks

Phase 1: Blue Team Deep-Dive

Phase 1: Table-top Exercise

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 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

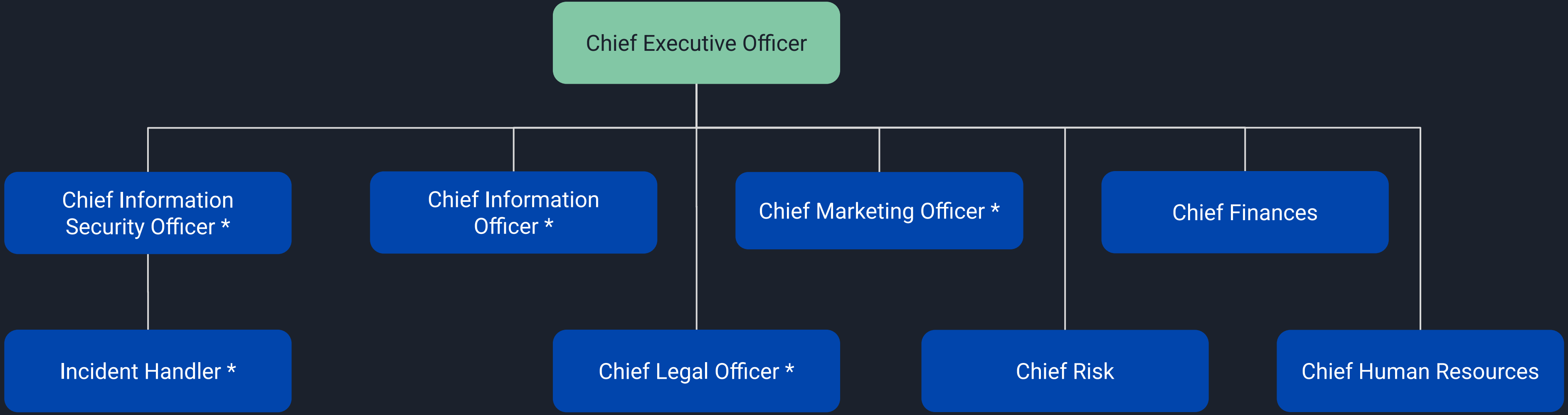
100m+
Yearly revenue

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*

Now it’s your turn!

These are your TTX functions for today…

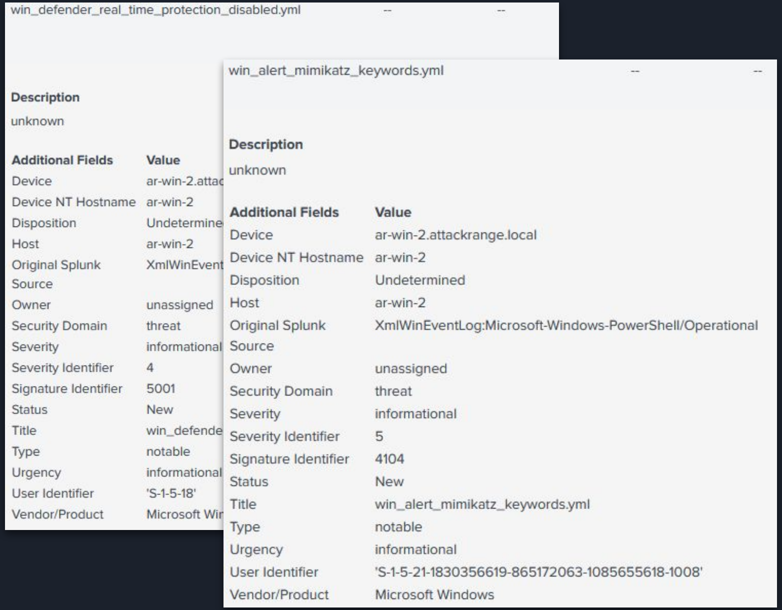
- Chief Information Security Officer
  - Is on top of the investigation. Gathers latest analysis information and informs the management / crisis team in an understandable way
- Chief Information / Technology Officer
  - Advises on technical implications and takes decision to shutdown services on CISO’s 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.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 Wir

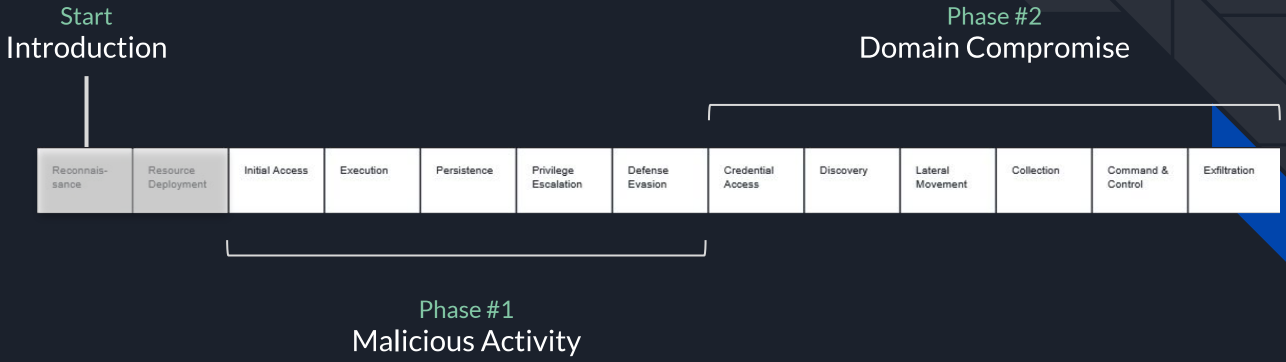
win_alert_mimikatz_keywords.yml -- --

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



Start
Introduction

Phase #2
Domain Compromise

Reconnais-sance	Resource Deployment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration

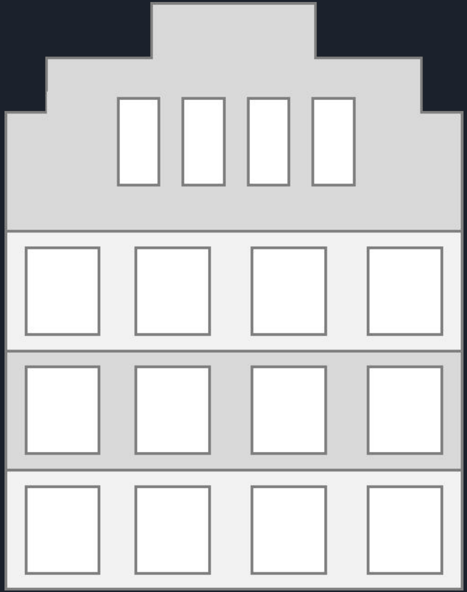
Phase #1
Malicious Activity

Phase 2 :Red Emulation

Phase 2 :Blue Team

Phase 2 : Table-top Deep-Dive

Recap: Global Crisis Response



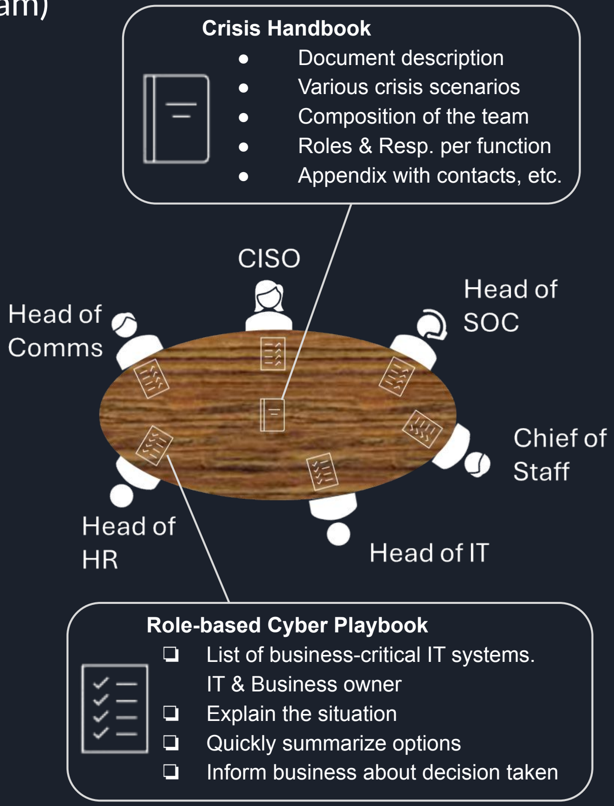
Team	Responsibility	Members		Rhythm
Board of Directors (BoD)	- Ultimate decision power and responsibility - Protects shareholder			Kept informed
Group Crisis Management Team	- Speaks in front of media during global crisis - Decides on global impact	- CRO - CTO - CFO - CISO (sec. incident)	Inform	Once a day when decision is required
Emergency Management Team	- Ensures timely reporting to regulators globally - Guides and coordinates local teams - Takes more strategic decision	- Chief of Staff - CISO - Legal & Compliance - Data Protection	Inform	Mornings and evenings
Local Incident Management Team	- Immediate response: People safety first - Handles incidents locally - Floods, terror attack - Reporting locally in local language	- Local IT - Compliance Officer - Physical Security	Inform	Hourly

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.



Crisis Handbook

- Document description
- Various crisis scenarios
- Composition of the team
- Roles & Resp. per function
- Appendix with contacts, etc.

Role-based Cyber Playbook

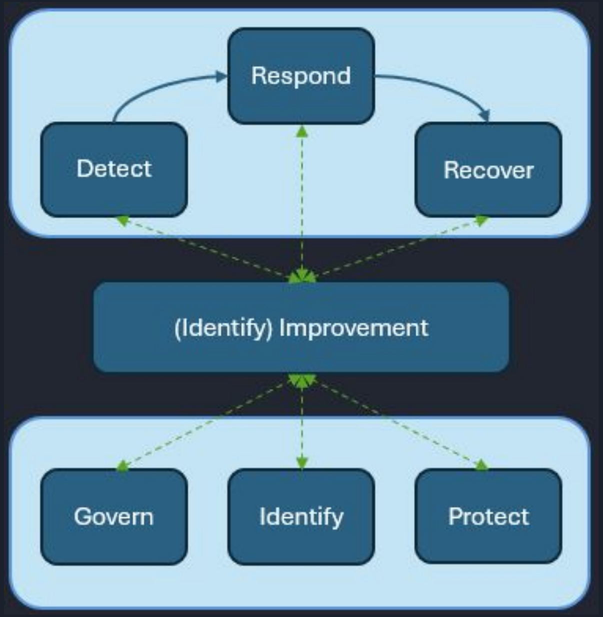
□ List of business-critical IT systems. IT & Business owner
□ Explain the situation
□ Quickly summarize options
□ Inform business about decision taken

Incident Response: NIST SP 800-61r3

Incident Response

Lessons Learned

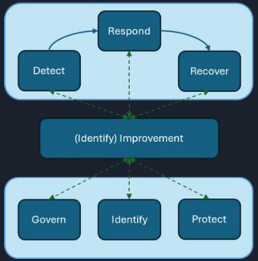
Preparation

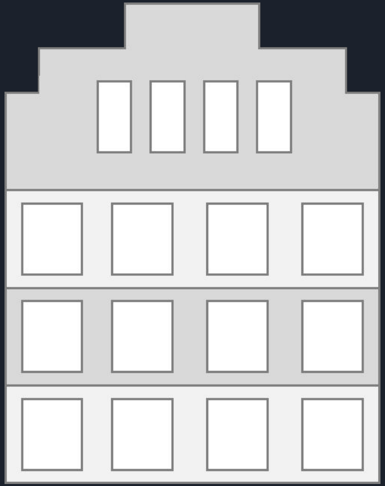


Help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications.

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





Team

Board of Directors (BoD)

Group Crisis Management Team

Emergency Management Team

Local Incident Management Team

- Validates, orchestrates and executes global cyber incident reporting (e.g., FINMA or MAS)
- Decides on system shutdown
- Internal and external communication with holding statements

- Issues new device to impacted user
- Informs local employees in local language
- Reports incident to local police

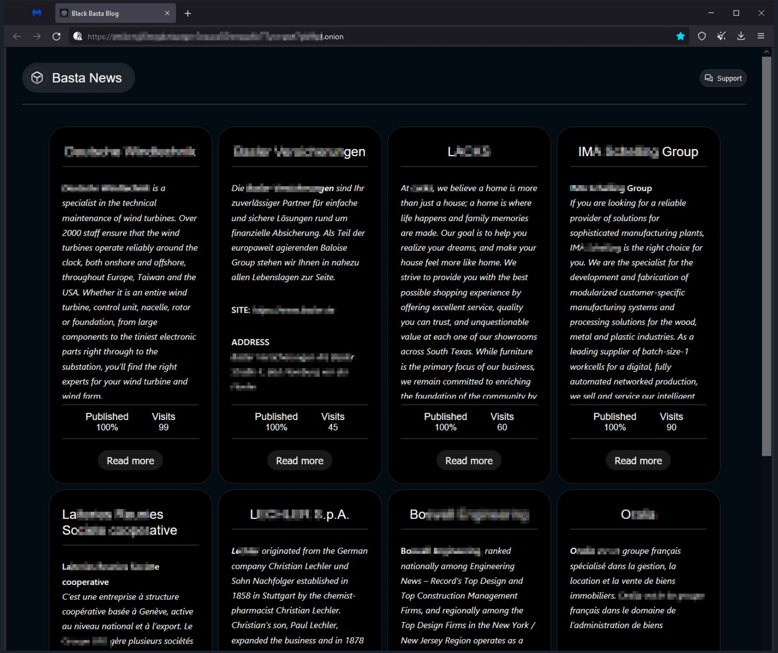
Clearly **define what a material cyber incident is**. Then, use your cross-functional crisis team in solving the cyber incident. As a CISO / Security function, you can **focus on what you do best**: Incident investigation and improving your protection capabilities. Let external communication, regulatory 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, Basel 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



Basta News

[redacted]

[redacted] is a specialist in the technical maintenance of wind turbines. Over 2000 staff ensure that the wind turbines operate reliably around the clock, both onshore and offshore, throughout Europe, Taiwan and the USA. Whether it is an entire wind turbine, control unit, nacelle, rotor or foundation, from large components to the tiniest electronic parts right through to the substation, you'll find the right experts for your wind turbine and wind farm.

Published 100% Visits 99

Read more

[redacted]gen

*Die [redacted]**gen** sind Ihr zuverlässiger Partner für einfache und sichere Lösungen rund um finanzielle Absicherung. Als Teil der europaweit agierenden Baloise Group stehen wir Ihnen in nahezu allen Lebenslagen zur Seite.*

SITE: [redacted]

ADDRESS

[redacted]

Published 100% Visits 45

Read more

L[redacted]

At [redacted], we believe a home is more than just a house; a home is where life happens and family memories are made. Our goal is to help you realize your dreams, and make your house feel more like home. We strive to provide you with the best possible shopping experience by offering excellent service, quality you can trust, and unquestionable value at each one of our showrooms across South Texas. While furniture is the primary focus of our business, we remain committed to enriching the foundation of the community by

Published 100% Visits 60

Read more

IMA [redacted] Group

[redacted] Group
If you are looking for a reliable provider of solutions for sophisticated manufacturing plants, IMA[redacted] is the right choice for you. We are the specialist for the development and fabrication of modularized customer-specific manufacturing systems and processing solutions for the wood, metal and plastic industries. As a leading supplier of batch-size-1 workcells for a digital, fully automated networked production, we sell and service our intelligent

Published 100% Visits 90

Read more

La[redacted]es So[redacted]ative

La[redacted]e cooperative
C'est une entreprise à structure coopérative basée à Genève, active au niveau national et à l'export. Le [redacted] gère plusieurs sociétés

L[redacted].p.A.

***Le[redacted]** originated from the German company Christian Lechler und Sohn Nachfolger established in 1858 in Stuttgart by the chemist-pharmacist Christian Lechler. Christian's son, Paul Lechler, expanded the business and in 1878*

Bo[redacted]

***Bo[redacted]** ranked nationally among Engineering News – Record's Top Design and Top Construction Management Firms, and regionally among the Top Design Firms in the New York / New Jersey Region operates as a*

O[redacted]

***O[redacted]** groupe français spécialisé dans la gestion, la location et la vente de biens immobiliers. [redacted] français dans le domaine de l'administration de biens*

Table-top 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 table-tops

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 & Feedback

Thank You!