Cyber Incident Response Tabletop Exercises (TTX)

for Financial Services Institutions (FSIs)

FINOS

controlplane

Agenda

- Whoami
- What a Tabletop Exercise (TTX) is and why is it important?
  - Security Incident Response 101
- Recap of the 2024 FINOS TTX and key lessons learned
- How to plan, structure, and execute a TTX within your organization
- 2025 initiatives

Whoami

2011

Security Engineer

2015

inmarsat

Chief Security Engineer

Head of SecOps Engineering

Head of Security Engineering

2021

controlplane

Security Engineering Manager

Head of Technical Solutions

Whoami

- Cloud native and open source security consultancy and product company
- Established in 2017
    - 55 people across the UK, Europe, APAC and North America
- Security specialists in cloud, Kubernetes, containers, and Open Source (we train too!)
- Focused on deeply “Threat Model-ed”, Secure-by-Design and Secure-by-Default Cloud Native architectures
- Accustomed to work in highly-regulated environments
- Help customers bridging the gap between infra and SecOps

controlplane

Agenda

- ~~Whoami~~
- What a Tabletop Exercise (TTX) is and why is it important?
  - Security Incident Response 101
- Recap of the 2024 FINOS TTX and key lessons learned
- How to plan, structure, and execute a TTX within your organization
- 2025 initiatives

Security Incident Response 101

Incident:

“An event that could lead to the loss of, or disruption to, an organization's operations, data, services or functions”.

“A **security** incident is an event that may indicate that an organization's systems or data have been compromised, or that measures put in place to protect them have failed.”

Reponse:

A set of **People**, **Process**, **Technology** to identify, contain, eliminate and recover from such events.

Security Incident Response 101

PEOPLE

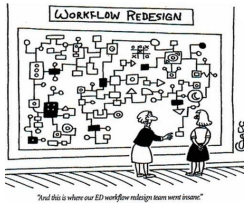
Security Analysts

Security Engineers

Forensics

Managers

PROCESS



Define playbooks/ runbooks

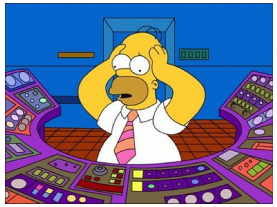
Threat Intel dissemination

Assets isolation

Evidence gathering

Stakeholders comms

TECHNOLOGY



Sensors (IPS, EDR, ...)

Sensors (Falco, CloudTrail, VPC Flowlogs...)

Log collection and processing (SIEM)

Automation tech

Security Incident Response 101

NIST Incident Response Steps

- Step #1: Preparation
- Step #2: Detection and Analysis
- Step #3: Containment, Eradication and Recovery
- Step #4: Post-Incident Activity

SP 800-61 Rev. 2

SANS Incident Response Steps

- Step #1: Preparation
- Step #2: Identification
- Step #3: Containment
- Step #4: Eradication
- Step #5: Recovery
- Step #6: Lessons Learned

Intelligence-driven Defense

Security Incident Response ~~101~~

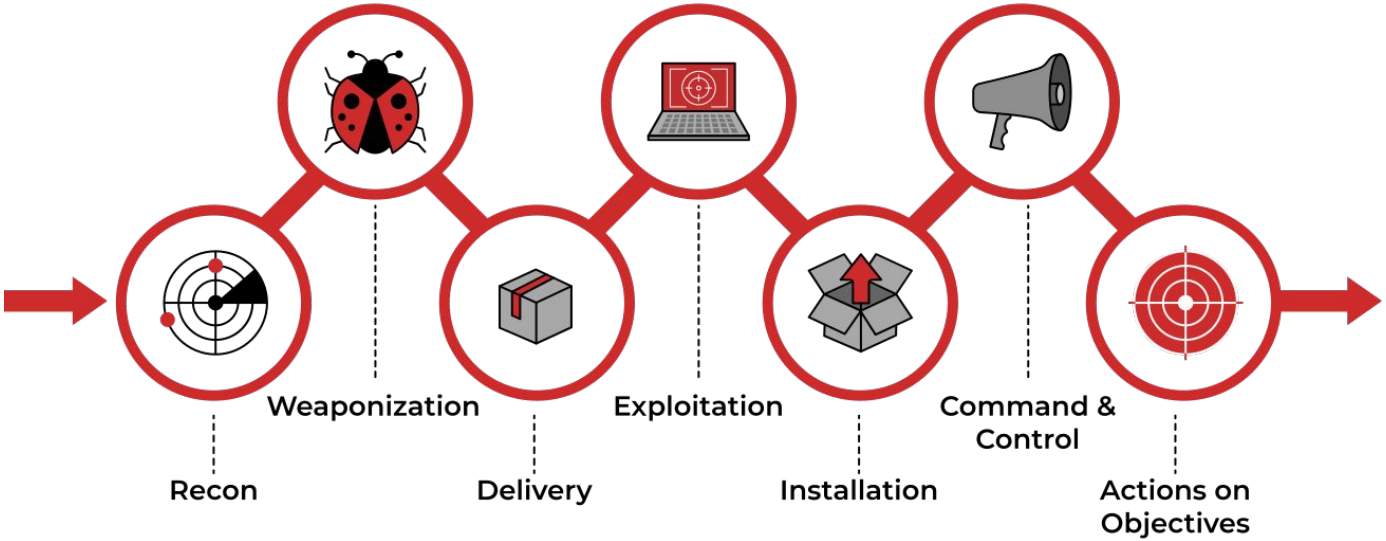
Reactive event-driven approach insufficient against **motivated** adversaries.

Incident Response must adopt a **Kill** (attack) **Chain** perspective:

- Step-by-step approach that identifies and stops enemy activity.
- **It no longer needs to be a purely reactive process**.
- Implements intent-based response, behavior-based detection to get a step ahead of adversaries.
- Critical to have the right **Intelligence** [**Indicators of Compromise** (IoC)].

Intelligence-driven Defense

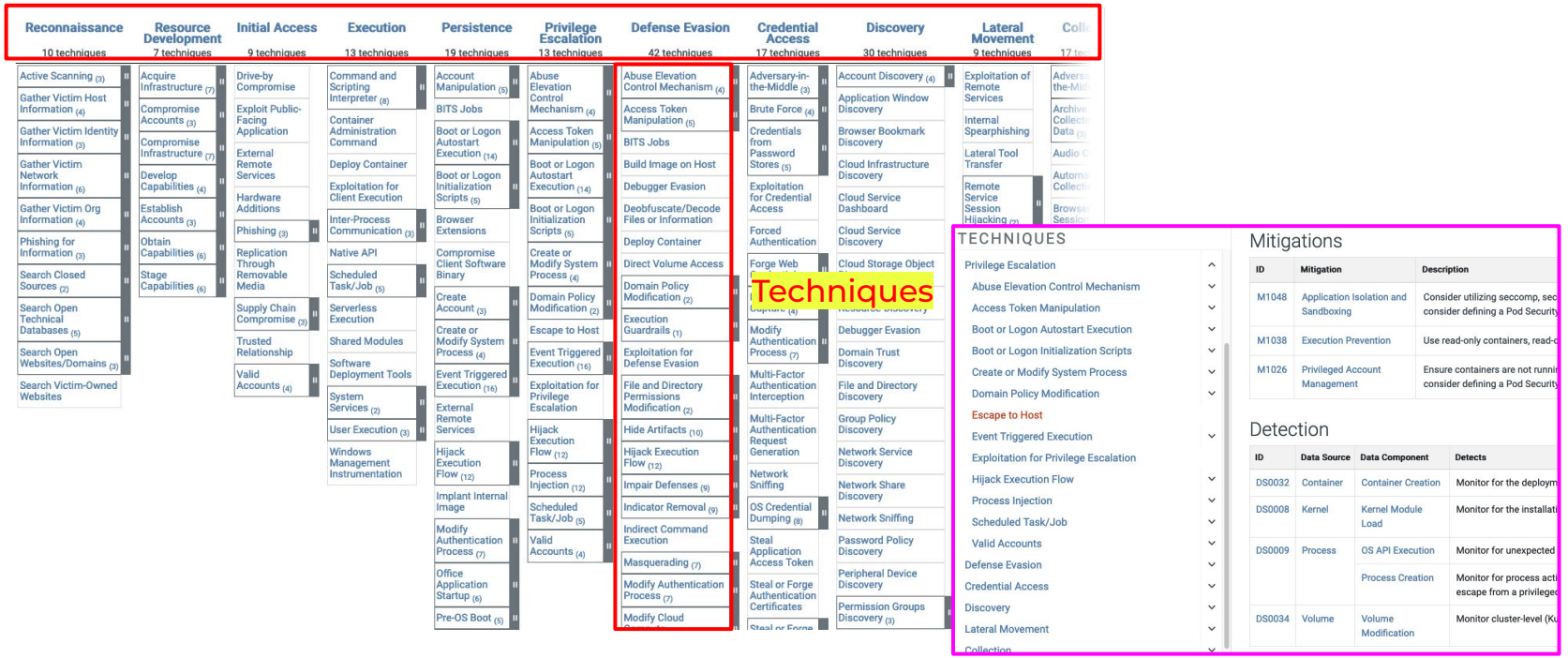
Cyber Kill Chain



Intelligence-driven Defense

MITRE | ATT&CK®

Tactics



Intelligence-driven Response

Playbooks: High-level guide for responding to specific incidents

Key Elements:

- Incident Types
- Decision Trees & Escalation Paths
- Roles & Responsibilities
- Communication & Reporting

Why Use Playbooks?

- Ensures consistent, quick, and effective responses
- Reduces errors and improves coordination across teams
- Supports compliance with standards (e.g., DORA, NIST)

Testing Playbooks: Tabletop Exercises (**TTX**)

Intelligence-driven Response

Tabletop Exercise: Response testing

- Structured security incident simulation
- Simulated scenarios to evaluate response readiness
- Discussion-based, focusing on decision-making, collaboration, and communication
- Brings teams across the entire business at the same table

Intelligence-driven Response

Tabletop Exercise: Why is it important?

- FSIs are prime targets for cyber threats due to high-value data
- Cloud native security introduces new challenges and risks
- DORA & NIS2 mandate financial institutions to test incident response capabilities
- TTXs help reveal security gaps response strategies **before** an attack occurs, and improve response to cyber threats
- Enhances cross-team coordination between security, risk, compliance, and executive teams

Agenda

- ~~Whoami~~
- ~~What a Tabletop Exercise (TTX) is and why is it important?~~
  - ~~Security Incident Response 101~~
- Recap of the 2024 FINOS TTX and key lessons learned
- How to plan, structure, and execute a TTX within your organization
- 2025 initiatives

2024 FINOS TTX

Open Source in Finance Forum London

- **Purpose**: FINOS and ControlPlane organized the first cloud native incident response tabletop exercise (TTX) to assess FSIs' preparedness for modern cyber threats.
- **Event**: 90-minute interactive simulation, behind closed doors, Chatham house rules
- **Participants**: Core team of senior security representatives from global FSIs
    - Citi, JPMC, NatWest Boxed, Morgan Stanley RBC, Quadrature, IG Group
- **Format**: A gamified live incident simulation, conducted under Chatham House rules, allowing open discussions.
- **Focus Areas**: Cloud native threat detection and response strategies, and aligning security operations with evolving regulatory and business needs.

2024 FINOS TTX

Open Source in Finance Forum London: outcomes

- FSIs are still adapting to cloud native threats
    - New tech, risks and shared responsibility models
- Context matters – data classification and blast radius analysis are critical
- Strong teams are essential – balancing technical & soft skills under pressure
- Playbooks must be tested – real-world rehearsals matter more than documentation
- Regulatory Alignment is Essential: TTXs must align with DORA and NIS2 to ensure compliance.

Agenda

- ~~Whoami~~
- ~~What a Tabletop Exercise (TTX) is and why is it important?~~
  - ~~Security Incident Response 101~~
- ~~Recap of the 2024 FINOS TTX and key lessons learned~~
- How to plan, structure, and execute a TTX within your organization
- 2025 initiatives

Building a TTX

Selling the TTX Internally – Why It Matters

- Cyber incidents are a business risk, not just a security issue
- Regulations mandate it → DORA, NIS2, and other frameworks require cyber resilience testing
- TTXs expose gaps before an actual crisis does
- It's not just about technology → Financial, reputational, and legal risks are at stake
- FSIs need cross-functional coordination to survive a crisis
- Highlight the ROI: better preparedness, reduced risk exposure, and enhanced recovery capabilities

Building a TTX

The buy-in

- Speak in Business Terms → "How would we handle a breach that exposes customer data?"
- Leverage Regulatory Pressure → "DORA requires us to test our response capability."
- Use Real-World Examples → "Look at how [competitor/bank X] struggled with their last breach."
- Demonstrate Financial Impact → "A cyberattack can cost millions in downtime and fines."
- Involve Key Decision-Makers Early → Make them feel ownership of the exercise.

Building a TTX

The Who

A successful TTX involves key stakeholders across the business:

- Executive Leadership → Decision-making, regulatory accountability
- Cybersecurity & IT → Threat detection, response execution
- Legal & Compliance → Regulatory obligations, liability risks
- PR & Communications → Internal and external messaging
- Operations & Business Units → Business continuity planning
- Risk Management → Evaluating financial & reputational risks
- Don’t forget external partners: service providers, regulators, and third-party vendors.

Building a TTX

The What - Opening the pandora's box

- Regulatory Breach (DORA/NIS2 violation leading to penalties)
- Ransomware Attack (Customer data is encrypted, business operations halted)
- Cloud Misconfiguration Incident (Exposed sensitive financial data)
- Insider Threat / Data Exfiltration (Unauthorized access, financial fraud)
- Third-Party Supplier Compromise (Attack via a key vendor)
- Nation-State Attack / Advanced Persistent Threat (APT)

Building a TTX

The What - Structuring it, step by step

- **Set Objectives** → Are we testing compliance, technical response, or crisis management?
- **Select the Scenario** → Choose a threat that is realistic and impactful
    - Keep scenarios complex, spanning multiple departments and involving external entities
- **Define Roles & Responsibilities** → Who makes key decisions?
- **Create an Incident Timeline** → Progressively escalate the situation
- **Simulate External Pressures** → Customers, regulators, media inquiries
- **Run the TTX** → Observe decision-making and coordination
- **Post-Exercise Review** → Identify weaknesses, update policies, and document findings

Building a TTX

The How - some guidelines

- Choose a facilitator to guide the exercise and keep discussions focused
- Establish a clear timeline and objectives for the exercise
- Ensure that each group has the opportunity to respond to the scenario, make decisions, and communicate their actions
- Use **injects** (additional information or crisis events) to simulate real-time pressure
    - Simulate real-world constraints (time pressure, media leaks, regulator inquiries)
- Encourage discussion, don't dictate answers
- Encourage honest assessments—where did we fail?

Building a TTX

Measuring Success – What Does a "Good" TTX Look Like?

- Teams communicate and collaborate effectively
- Decisions are made quickly, with clear accountability
- Gaps in security, communications, and compliance are identified
- Lessons learned lead to concrete improvements (updated playbooks, new training)
- Regulatory obligations (DORA, NIS2) are met with proper documentation

Building a TTX

The Post

- Document Findings → Identify security and procedural gaps
- Update Playbooks & Runbooks → Refine response strategies
- Executive & Board Briefing → Ensure leadership understands risks
- Regulatory Reporting → Provide DORA/NIS2 compliance documentation
- Plan the Next TTX → Make it a regular practice

Agenda

- ~~Whoami~~
- ~~What a Tabletop Exercise (TTX) is and why is it important?~~
  - ~~Security Incident Response 101~~
- ~~Recap of the 2024 FINOS TTX and key lessons learned~~
- ~~How to plan, structure, and execute a TTX within your organization~~
- 2025 initiatives

2025 Initiatives

Call to action

- **Next FINOS Tabletop Exercises**:
  - London – June 2025 at Open Source in Finance Forum
  - New York – Sept. 30 & Oct. 1, 2025 at Open Source in Finance Forum
- **Why Attend**?
  - Improve your cloud native security readiness
  - Get experience with real-world financial sector threats, in a safe environment
  - Learn best practices from security leaders across the industry
- **How to Register**:
  - Send your security, risk, and compliance teams to participate.

Wrap-up

Summary

- Tabletop Exercise is just one part of a broader digital operational resilience strategy
- Regular exercises, informed by lessons learned, create a stronger, more adaptable institution
- DORA compliance isn’t just about ticking boxes—it’s about ensuring you are truly resilient in the face of disruption
- The financial sector faces increasing cyber threats—proactive preparation is key
- Take action: Run your own TTX, and keep doing so for continuous improvement

[Title] - Divider Slide

[Subtitle]