

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



Chief Security Engineer

Head of SecOps Engineering

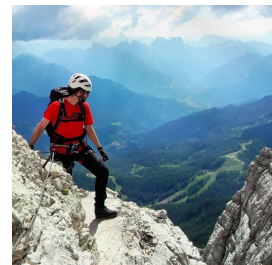
Head of Security Engineering

2021



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

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.

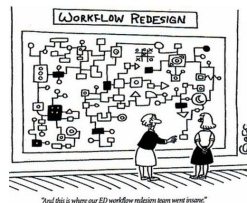
Security Incident Response 101

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~~

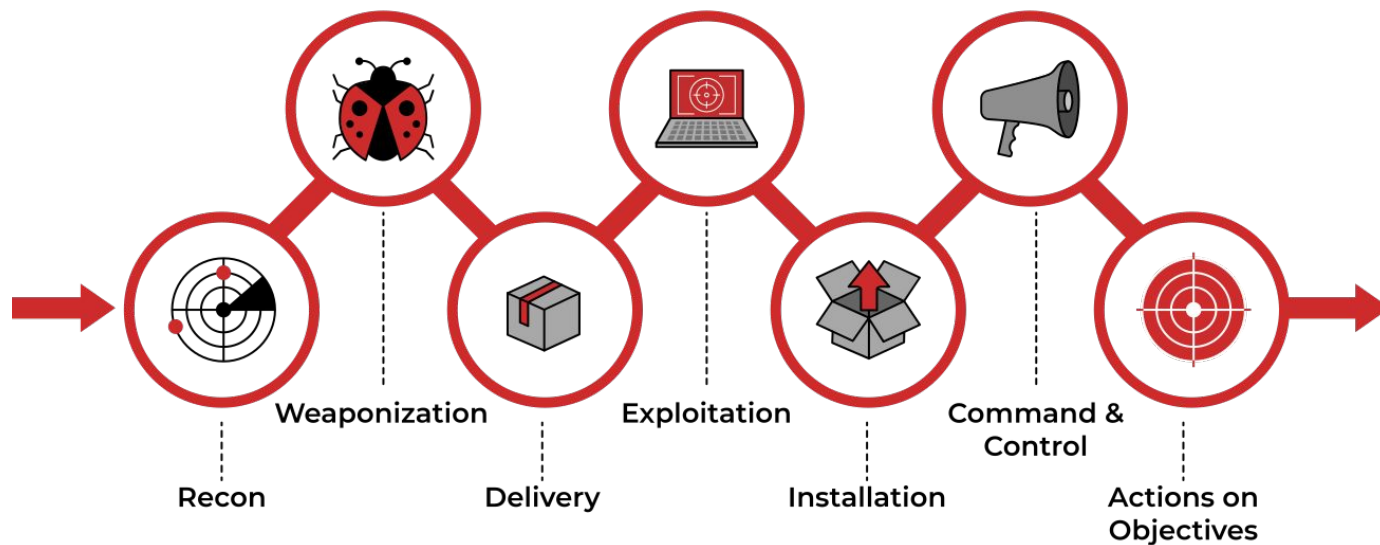
Reactive event-driven approach insufficient against **motivated** adversaries.

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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques

Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collection Data (3)
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Collection
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Forced Authentication	Cloud Service Dashboard	Cloud Service Discovery	Browser Session Hijacking (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Create or Modify System Process (4)	Forge Web (4)	Cloud Storage Object Discovery		
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Forge Web (4)			
Search Open Technical Databases (5)	Trusted Relationship	Serverless Execution	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (14)	Event Triggered Execution (14)	Modify Authentication Process (7)	Debugger Evasion		
Search Open Websites/Domains (3)	Software Deployment Tools	System Services (2)	System Services (2)	Event Triggered Execution (14)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Multi-Factor Authentication Interception	Domain Trust Discovery		
Search Victim-Owned Websites	User Execution (3)	Hijack Execution Flow (12)	Windows Management Instrumentation	External Remote Services	Hide Artifacts (10)	Hide Artifacts (10)	Multi-Factor Authentication Request Generation	File and Directory Discovery		
		Implant Internal Image		Process Injection (12)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Network Sniffing	Group Policy Discovery		
		Modify Authentication Process (7)		Indicator Removal (9)	Process Injection (12)	Process Injection (12)	OS Credential Dumping (8)	Network Service Discovery		
		Office Application Startup (6)		Masquerading (7)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	OS Credential Dumping (8)	Network Share Discovery		
		Pre-OS Boot (5)		Modify Authentication Process (7)	Valid Accounts (4)	Valid Accounts (4)	Steal or Forge Authentication Certificates	Network Sniffing		
				Modify Cloud			Steal or Forge Authentication Certificates	Peripheral Device Discovery		
							Steal or Forge Authentication Certificates	Permission Groups Discovery (3)		

Techniques

TECHNIQUES		Mitigations	
Privilege Escalation	Abuse Elevation Control Mechanism	M1048	Application Isolation and Sandboxing
Access Token Manipulation	Boot or Logon Autostart Execution	M1038	Execution Prevention
Boot or Logon Initialization Scripts	Create or Modify System Process	M1026	Privileged Account Management
Domain Policy Modification	Debugger Evasion		
Escape to Host	Event Triggered Execution		
Event Triggered Execution	Exploitation for Privilege Escalation		
Exploitation for Privilege Escalation	Hijack Execution Flow	DS0032	Container
Hijack Execution Flow	Process Injection	DS0008	Kernel
Scheduled Task/Job	Valid Accounts	DS0009	Process
Defense Evasion	Credential Access		
Discovery	Lateral Movement	DS0034	Volume
Collection			

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]