SERKET-TECH SECURITY x EXECUSOURCE

Prepare. Respond. Recover. Serket-Tech Security Tabletop Exercise Services

Cyber incident tabletop exercises for executive, technical, and operational readiness. Prepare teams for ransomware, AI-enabled impersonation, data extortion, cloud compromise, and public-facing disruption.

Cyber incidents rarely fail because only one technical control breaks. They escalate when decision ownership, authority validation, approval paths, communications, and recovery priorities are unclear. Serket-Tech Security designs and facilitates realistic tabletop exercises that let leadership, security, IT, legal, communications, finance, HR, and operations teams practice response decisions before a real event forces them to act under pressure.

Validate Decisions Before Pressure
Test who owns key decisions, when escalation occurs, and how competing priorities are resolved during a fast-moving incident.

Test Identity and Authority Controls
Exercise out-of-band verification, delegated authority, high-risk approvals, executive impersonation response, and suspicious request handling.

Turn Lessons into Action
Capture observed strengths, process gaps, control needs, training opportunities, and follow-up actions with owners and target dates.

Align Response, Legal, and Communications
Practice how technical updates become business decisions, customer messages, regulator notifications, board updates, and media statements.

Realism Matters

Strong tabletop exercises fail when they rely on fake workflows that don't align with the client. We tailor artifacts and discussion prompts to the tools and decision paths teams use every day.

- **Environment Alignment**
  Teams, Zoom, WebEx, Slack, email, calendar, ticketing, file-sharing, mobile, MFA, approval, and delegation workflows can be reflected in the scenario.
- **Synthetic Media Controls**
  Where voice or video simulation is used, Serket-Tech Security uses approved inputs, restricts access, discloses relevant tool flows, and limits retention.
- **Decision Realism**
  Exercises are written to test judgment in ambiguous situations, not to quiz participants on policy language or expose individuals.
- **No Production Impact**
  Exercises are discussion-based and do not execute containment, testing, tool changes, or operational actions against live systems.

SERKET-TECH SECURITY x EXECU SOURCE

Threat Scenarios We Can Simulate

Each exercise can be tailored to the client's business model, regulatory exposure, technology stack, threat profile, and maturity. AI can be part of the pressure, not the whole story.

AI Deepfake Executive Impersonation

Synthetic voice, video, text, or chat artifacts create a high-trust request from a senior leader, board member, customer, investor, or partner.

Ransomware and Data Extortion

Encryption, data theft, double extortion, business interruption, law enforcement coordination, cyber insurance, and restoration decisions.

Insider, Access, and Privilege Abuse

Suspicious privileged activity, unauthorized data movement, HR escalation, evidence handling, and containment decisions.

Third-Party and Supply Chain Disruption

Vendor outage, managed service provider compromise, software supplier breach, data processor incident, and customer assurance requests.

AI-Enabled BEC and Payment Fraud

Fraudulent invoice changes, urgent wire requests, gift card schemes, payroll redirection, vendor impersonation, and approval bypass attempts.

Cloud, SaaS, and Identity Compromise

Compromised accounts, MFA fatigue, OAuth abuse, mailbox rules, privileged access misuse, and suspicious file-sharing activity.

AI Governance and Shadow AI Risk

Sensitive data entered into unauthorized AI tools, model output misuse, policy gaps, vendor AI risk, and employee reporting workflows.

Data Breach and Privacy Crisis

Sensitive data exposure, evidence preservation, notification triage, legal privilege, regulator communication, and customer impact decisions.

Executive Teams

Board updates, strategic decisions, legal posture, public trust, and resource prioritization.

Security and IT

Triage, containment, identity review, logging, restoration, evidence, and tool coordination.

Business Operations

Customer impact, finance approvals, continuity decisions, workarounds, and recovery tradeoffs.

Legal and Communications

Privilege, notification duties, customer messaging, media handling, and single-source narrative control.

Serket-Tech Security Tabletop Methodology

Our process is designed to make the exercise technically accurate, operationally plausible, and relevant to how the client really works.

01
Discover and Align
Confirm objectives, sponsor, audience, operating constraints, risk themes, systems in scope, communications channels, and success criteria.

02
Design the Scenario
Build a plausible storyline with timed injects, decision points, branching options, and audience-specific pressure.

03
Create Realistic Artifacts
Develop facilitator materials, participant guides, inject matrices, sample messages, screenshots, voice clips, video clips, or live modules where approved.

04
Rehearse and Control
Run a readiness check, validate timing, test meeting logistics, confirm ground rules, and tune the flow before delivery.

05
Facilitate and Observe
Guide the exercise, deliver injects, capture decisions, record assumptions, identify friction, and keep the session focused on response outcomes.

06
Report and Improve
Deliver the after-action report, improvement plan, executive readout, prioritized actions, owners, target dates, and follow-up validation recommendations.

Engagement Paths

Clients can start with a focused tabletop or build a recurring resilience program across leadership, technical teams, business units, and board stakeholders.

1. Executive Crisis Tabletop

Built for executives, board-facing leaders, legal, communications, finance, HR, and business owners who must make fast decisions with incomplete information.

What It Can Include

- Two to three-hour facilitated session
- Scenario focused on escalation, authority, communications, continuity, and reputation
- Decision prompts for ransom, notification, customer impact, and board reporting
- Hotwash, after-action report, and improvement plan

2. Incident Response and Technical Coordination

Built for security, IT, cloud, identity, infrastructure, application, and operations teams that need to test handoffs and response choreography.

What It Can Include

- Technical injects tied to identity, endpoint, cloud, SaaS, logs, backups, and recovery
- Role mapping across the incident commander, scribe, legal, communications, and business owners
- Validation of escalation triggers, evidence capture, and containment decision paths
- Findings mapped to people, process, technology, and training actions

3. AI Deepfake and Fraud Simulation

Built for organizations exposed to executive impersonation, payment fraud, brand abuse, high-value approvals, and public-facing trust events.

What It Can Include

- Synthetic voice, video, text, or chat injects where approved and scoped
- Out-of-band validation, callback controls, dual approval, and delegated authority testing
- Fraud, finance, customer, vendor, and executive assistant workflow pressure
- Synthetic media handling controls and post-exercise deletion plan

Optional Modules

Communications war room, fraud workflow, ransomware negotiation discussion, board readout, policy and playbook workshop, or 60- to 90-day validation tabletop.

Typical Deliverables

Exercise charter, agenda, participant guide, facilitator runbook, inject matrix, evaluation notes, after-action report, improvement plan, and executive readout.

Who We Support

Legal, healthcare, finance, manufacturing, retail, higher education, logistics, government-adjacent, SaaS, and other regulated or high-trust businesses.

Build Readiness Before the Incident

Engage Serket-Tech Security for a tabletop readiness workshop, an executive crisis exercise, an AI deepfake simulation, or a recurring incident response exercise program.