IOActive®

Research-fueled Security Services

Open-Source Intelligence (OSINT) Threat Simulation for High-Value Targets

Today's Reality

Publicly available data increasingly fuels credible social engineering campaigns against high-value targets. Adversaries use aggregated information from breach corpuses, social platforms, conference materials, developer ecosystems, and certificate transparency logs to construct detailed profiles of executives and key personnel. Advances in synthetic media and automated data collection make these attacks faster, more convincing, and harder to detect. The result is often financial fraud, account compromise, or the manipulation of internal processes using only information that is already public.

IOActive's OSINT Threat Simulation for High-Value Targets provides the visibility and intelligence needed to counter this threat. By replicating the techniques of genuine adversaries, this program reveals how individuals and organizations appear through an attacker's lens, then translates those insights into clear remediation and awareness actions. The service strengthens defensive posture by helping leaders understand and manage the real-world exposure of their people and brands.

AT A GLANCE

- Observational Assessment: No direct contact with targets and no live attack execution.
- Individual and Group Insights: Per-individual exposure profiles are combined with group-level trends and prioritized remediation.
- Actionable Scenarios: Clear, realistic threat scenarios and supporting artifacts that are understandable for leadership.
- Flexible, Remote Delivery: Fully remote execution, parallelizable across multiple targets, with weekly status updates and a final briefing.
- Optional Continuous Program: Ability to convert to an ongoing service with periodic refreshes and updates.

Who is a high-value target?

High-value targets extend well beyond the executive team, including anyone with elevated access, influence, or privileged insight.

These groups can include:

- Finance approvers, IT and service desk staff, HR and recruitment teams, legal and corporate communications personnel, product and engineering leaders, board liaisons, and executive assistants.
- Senior staff and trustees within significant charitable organizations, grant-making bodies, and non-profits where access to funds, beneficiary data, or reputational leverage can be exploited.
- Individuals and groups at higher-risk who hold significant assets, such as high-net-worth individuals, family offices, asset managers.
- Individuals with authority over treasury, investment, or payment workflows outside of traditional corporate structures.

Risk exposure often increases during periods of change or heightened scrutiny, including restructuring, mergers and acquisitions, leadership transitions, security incidents, funding rounds and major grant cycles, and high-profile product, regulatory, or public announcements.

Risk examples

Deepfakes use synthetic audio or video to imitate a trusted person, making familiar voices and faces unreliable as proof of identity and reinforcing the need for deepfake defense controls. Deepfake-assisted finance approvals, crafted from executive speech clips and recent travel details, can appear as highly convincing, time-sensitive requests. Helpdesk reset pretexts become effective when public HR data is combined with familiar ticketing language. Vendor impersonation succeeds where public RFPs, visible technology stacks, and service desk phrasing align. Account takeover is frequently enabled by reuse of personal email addresses or phone numbers that bridge consumer and corporate accounts.

Scope and guardrails

Responsibility. OSINT threat simulation is an observational exercise. We do not contact individuals or conduct live social engineering exercises. Any optional simulated content, such as voice or video media, is produced only with explicit advance consent. All activities are performed remotely and in full compliance with legal and ethical standards.

Business impact. Findings translate technical exposure to actionable business context, covering areas such as helpdesk verification, executive communications, financial authorization, identity proofing, and staff awareness. These findings can help reduce fraud risk, accelerate takedown actions, and strengthen control effectiveness without disrupting normal operations.

Forward-looking processes. The quality of synthetic and altered media is rapidly advancing, data broker ecosystems are expanding, and more enterprise processes rely on identity recovery mechanisms that are inherently weak. Organizations that strengthen these processes now will improve resilience, limit reputational exposure, and reduce the cost of future incident response.

Our services & methodology

IOActive's approach builds on established OSINT practices, enhanced by extensive real-world adversarial simulation experience. This methodology provides actionable insight into organizational and individual exposure while remaining fully ethical and observational.

Kickoff and success criteria. We begin the engagement by aligning on objectives, in-scope roles, consent posture for any simulated media, reporting audiences, and success metrics. Cadence for status updates, approvals, and deliverables is agreed upon up front to ensure transparency and clarity.

1) **Intelligence collection & exposure mapping.** Using only publicly available sources, we construct comprehensive digital footprints for each in-scope individual. Sources include:

   - Name variants, usernames, and professional and personal email addresses
   - Social media platforms (LinkedIn, Facebook, X, Instagram)
   - Public breach and credential exposure data
   - Domain registrations and online assets
   - Developer and cloud traces (e.g., GitHub, package registries)
   - Media appearances, conference content, and public presentations
   - Interactions with vendors, tools, or technologies

Findings are classified as personal or organizational exposure and correlated with roles and trust boundaries to highlight potential risk vectors.

2) **Threat modeling & risk categorization.** Exposure is analyzed through an attacker's lens to model organizational impact. Where relevant, we reference MITRE ATT&CK tactics to contextualize risk. Findings are prioritized based on credibility, exploitability, and potential impact on business processes.

3) **Scenario development.** We develop narrative attacker playbooks that show how public information could be used for phishing, vishing, impersonation, or helpdesk manipulation. Supporting artifacts may include:

   - Spoofed email examples
   - Calendar invites
   - Cloned profile previews

With explicit prior consent, we can produce short simulated voice or video snippets for training purposes.

4) **Remediation & training.** We provide targeted recommendations for individuals and the organization, including:

   - Social privacy and digital footprint hardening
   - Data broker opt-outs and identity separation
   - Multi-factor authentication (MFA) and password hygiene
   - Account compartmentalization and helpdesk verification improvements
   - Enhancements to detection and response for social engineering.

We can brief each participant individually or run a group session focused on recognizing AI-enabled impersonation and practical defensive measures.

5) **Reporting & communications.** Regular status updates and a final Threat Simulation Report are provided for both technical and leadership audiences. Reporting emphasizes exposure, threat paths, and remediation pathways, with appendices documenting evidence and methodology.

6) **Continuous program option.** You can extend the engagement to a recurring service with onboarding flows for new executives and sensitive roles, iterative refresh after organizational changes, remediation follow-ups, and quarterly trend reporting.

Deliverables

- **Per-individual Exposure & Threat Profile.** A comprehensive view of each high-value target, including digital footprint, attacker objectives, and realistic threat scenarios.
- **Threat Simulation Report.** Executive summary, group-level trends, prioritized remediation recommendations, and appendices documenting evidence and methodology.
- **Optional Simulated Media.** Short voice or video simulations produced only with explicit prior consent, used for awareness and training purposes.
- **Ongoing Communication.** Weekly status updates during execution, with a closeout briefing or live walkthrough to present findings and recommendations to stakeholders.

Outcomes and KPIs

We focus on a small set of measurable outcomes rather than vanity metrics. Exposure decreases over time as data-broker records are removed and sensitive public posts are addressed. Time-to-takedown for impersonation domains and social profiles shortens as organizational processes mature. Scenario closure rates improve as policies and controls neutralize the attack playbooks we document. Multi-factor authentication and verification coverage are strengthened across helpdesk and finance workflows, effectively turning social-engineering pathways into dead ends.

Readiness & client responsibilities

To ensure an efficient exercise and maximize value from its results, you should:

- Designate a project liaison and provide emergency security contacts.
- Review deliverables in accordance with agreed schedules.
- Coordinate internal stakeholders to ensure timely provision of information and approvals.
- Confirm consent posture for any optional simulated media.

For more information about IOActive's Cybersecurity Services, email info@ioactive.com or visit ioactive.com.

Prepare for the Future Now

Companies trust IOActive because:

1. **Pioneering Research:** Renowned for ground-breaking cybersecurity research, uncovering vulnerabilities that shape industry standards.
2. **Expert Cybersecurity Assessments:** Drawing on extensive expertise, we uncover risks often overlooked by others, ensuring robust protection for your infrastructure.
3. **Customized Advice:** We deliver personalized cybersecurity strategies that address our client's specific business needs and threats.
4. **Global Industry Recognition:** Acknowledged by both peers and clients, our contributions to the cybersecurity community have earned a prestigious reputation.
5. **Innovative Cybersecurity Tools:** Leveraging state-of-the-art tools and techniques, we are at the forefront of cybersecurity technology.
6. **Dedicated Client Partnership:** We prioritize long-term client relationships, offering continuous support and strategic guidance to navigate the evolving security threatscape.

ABOUT IOACTIVE

IOActive, a trusted partner for Global 1000 enterprises, provides research-fueled security services across all industries. Our cutting-edge cybersecurity teams provide highly specialized technical and programmatic services including full-stack penetration testing, program efficacy assessments, and hardware hacking. IOActive brings a unique attacker's perspective to every engagement to maximize cybersecurity investments and improve the security posture and operational resiliency of our clients. Founded in 1998, IOActive is headquartered in Seattle with global operations, including state of the art hardware hacking labs in Seattle, WA, Madrid, Spain and Cheltenham, UK. For more information, visit ioactive.com.