Yoni Binstock

Cybersecurity Leader & Hands-On Practitioner with 15+ years securing enterprise systems, leading cross-functional security teams, and aligning programs with NIST CSF, ISO 27001, and GDPR. Proven track record in threat detection, incident response, GRC compliance, and security awareness programs that reduced phishing click rates by 73%. Adept at bridging executive strategy with technical execution to strengthen security posture and resilience.

Email: ybinstock@gmail.com
LinkedIn: https://www.linkedin.com/in/yonibinstock/
GitHub: https://github.com/ybinstock
Location: Los Angeles, California

Skills

- **Cybersecurity**: Threat detection, incident response, vulnerability assessment, secure network architecture, network security, identity & access management (IAM), encryption & cryptography, digital forensics, SIEM, NIST CSF, NIST RMF, GRC compliance, risk management, DevSecOps, penetration testing oversight, TTP analysis aligned with MITRE ATT&CK, log analysis, OSINT tooling, RCSA/control testing cycles, vendor security due diligence, security KPIs, corporate BCP/DR plans, Zero Trust Architecture, EDR/XDR, SOAR, SAST/DAST, STRIDE, CVSS based remediation
- **Tools & Platforms**: Wireshark, Splunk, Nessus, Git
- **Team Management:** Hiring, 1:1s, performance reviews, conflict resolution, creation of a high-performance culture, cross-functional collaboration
- **Software Development**: Python, Linux, SQL, Typescript, JavaScript, CLI

Cybersecurity Certifications

- Google Cybersecurity Professional Certificate
- CompTIA Security+
- CISSP / Associate of ISC2
- Blue Team Level 1 (BTL1)
- CISM - *in progress*

Experience

CTO | Atomic Digital Design | 2022–2025
Led enterprise cybersecurity, IT governance, and compliance programs for a global creative technology company, overseeing a 12-person development/IT team and a $10K/year security tooling budget.

- Reduced phishing click rate by **73%** by launching 12 monthly security workshops, phishing simulations, and employee reward programs for rapid threat reporting; delivered regular security posture updates to executives.

- Implemented **32 AI-enabled IP cameras** with motion analytics and RFID/mobile badge authentication; integrated camera/badge logs into **Splunk SIEM** for real-time alerts, meeting **PCI-DSS physical security** requirements, and improving incident investigations.

- Enforced **multi-factor authentication (MFA)**, strict **role-based access controls (RBAC)**, and least-privilege principles across all internal systems to strengthen identity and access management.

- Adopted **NIST CSF** and **NIST RMF** frameworks; conducted risk assessments, compliance audits, and integrated **ISO 27001** controls and **GDPR** measures to ensure regulatory alignment and data privacy.

- Established IT security policies covering firewall configuration, endpoint protection, automated vulnerability scanning, and **disaster recovery/business continuity planning**.

- Authored a **160-page cybersecurity playbook** with 24 **MITRE ATT&CK-aligned** incident-response runbooks, reducing threat resolution time and standardizing escalation protocols.

- Coordinated delivery of secure digital projects for high-profile clients, including Renault, Balenciaga, Hermès, Dior, and Steve Madden, ensuring compliance with enterprise client security requirements.

- Built and led a high-performance culture through daily standups, team-building initiatives, and a leadership approach that fostered trust, accountability, and cross-functional collaboration.

Education
- Boston University (Master of Arts), 2011
- Rollins College (Bachelor of Arts), 2010