Nathan Hunstad

https://www.nathanhunstad.com

Experienced leader with 20 years in IT & Security. Led teams of between 2 and 10 FTEs/contractors for 10 years, with a demonstrated track record of delivering risk-appropriate and business-enabled security results at large or medium scale. Able to lead projects strategically over long time frames while having the technical knowledge to deep-dive when necessary. Experienced with media interviews, webinars, and conference presentations. Personal expertise in security both on-prem, hybrid, and cloud environments. Interested in a new challenge running a security program for either a medium or small company.

Security Programs	Compliance	Technologies
Product/Application Security	FedRamp	Cloud (AWS, Azure)
Insider Risk	SOC2	SIEM
Identity & Access Management	PCI-DSS	SOAR
Threat & Vulnerability Management	HIPAA	TVM/SAST/DAST
Governance, Risk, and Compliance	ISO27001	

Code42 Software, Inc.

Key leader who is integral to building security program to its current high maturity level. Built SOC, TVM, Red Team functionalities. Leads application security, Identity and Access Management, and Insider Risk teams. Provides business with data analytics and product feedback.

Deputy CISO (1/22-Present)

- Manage Platform Application Lifecycle Security (PALS), Insider Risk Managment (IRM), and Identity and Access Management (IAM) teams, consisting of 7 FTEs.
- Provide security consulting on projects such as customer data access, significant infrastructure and architectural changes, and new product features.
- Support the implementation of security tools into development pipelines to “Shift Left” for Application Security, including SAST, DAST, and container scanning tools.
- Oversee major IAM modernization project which replaced on-prem Active Directory servers with cloud-native SaaS solutions.
- Advocate for security in general, and Insider Risk Management in particular, though conference presentations, blogs, podcast interviews, and other media.
- Support divestiture of Crashplan Group via consulting on technical and operational separation projects.

Principal Security Researcher & Engineer (7/19-1/22)

- Principal owner of security tools including Security Orchestration, Automation, and Response (SOAR) tool, logging infrastructure, and intel tools.
- Support investigations into security events and alerts, including remediation activities.
- Research current trends in attacker Tactics, Techniques, and Procedures (TTPs) to ensure accurate security tool testing and response coverage.
- Implement internal Agile DevSecOps program to provide development services to security team.
- Create original security content for blogs, webinars, and other marketing channels.

Director, Security (3/18-7/19)

- Director of team of 7 FTEs including Security Operations, Security Engineering, Security Architecture, and Red Team.
- Manage portfolio of over a dozen security tools.

- Work with software developers on implementation of security tools and processes to improve maturity of DevSecOps program.
- Automate investigative, response, and reporting activities using a variety of languages.
- Provide security consulting to rest of organization in accordance with required security controls.

Security Operations Manager (7/16-3/18)

- Manage team of three FTEs plus one contractor.
- Manage security logging platform, including Elastic for logging visualization and search.
- Manage firewall platform, including management of upgrade of firewall technology.
- Implement Threat and Vulnerability Management program.
- Provide SME expertise on security operations for customer vendor assessments.

Best Buy Corporation

Identified and implemented key program objectives as part of new threat hunting and cyber intel team. Created custom tools and integrated with existing security tech stack to improve visibility to threats. Analyzed malware and worked with stakeholders leading to takedown of C2 infrastructure abroad.

Cyber Hunter – Cyber Threat and Intelligence Team (3/15-7/16)

- Conduct internal hunt activities to detect malware not seen by existing security controls.
- Write custom host data collector in C to collect actionable IOCs from endpoints.
- Write and deploy multiple Tanium actions for hunt activities and incident response.
- Create dashboards, data monitors, and rules in SIEM tools to monitor security events.
- Create and extend custom web scrapers in Python to gather data from multiple sources including Twitter, Pastebin, and sensitive deep web locations.
- Create malware analysis sandbox environments using VMWare, Windows XP, and Windows 7.
- Conduct malware analysis using using several disassemblers and debuggers.

Target Corporation

Conducted risk assessments and lead internal security consulting teams, identifying risks and tracking through GRC process.

Manager – Consulting, Information Protection (8/13-2/15)
Senior Analyst – Consulting, Information Protection (10/12-8/13)
Analyst – Risk Assessments, Information Protection (10/11-10/12)

Minnesota House of Representatives, Democratic-Farmer-Labor Caucus

IT Analyst (10/04-10/11)

Education & Certifications

University of Minnesota, Twin Cities Campus

M.S., Security Technologies (Awarded 12/11)
B.A., Political Science (Awarded 8/00)

- CISSP: 2012-2024, #437974
- AWS Certified Security – Specialty: 2018-2020
- AWS Certified Developer – Associate: 2016-2019
- AWS Certified SysOps Administrator – Associate: 2016-2019
- AWS Certified Solutions Architect – Associate: 2016-2019
- Certified Ethical Hacker (C|EH): 2014-2017