Seth Feldman

North Charleston, SC
funtime@iamfuntime.com

Professional Summary

Accomplished and innovative cybersecurity professional with over 20 years of extensive experience in the Information Security sector, specializing in custom threat detection, security engineering, endpoint, and network security. Proven expertise in understanding penetration testing procedures to identify vulnerabilities and recommend robust security solutions. Solid track record of developing and implementing comprehensive security protocols, with a strong ability to identify, evaluate, and mitigate potential risks and threats. Adept at leading cross-functional teams and managing multiple projects concurrently. A dynamic leader that consistently stays at the forefront of emerging trends, technologies, and advancements in cybersecurity. Passionately committed to ensuring the integrity, confidentiality, and availability of corporate data and information systems.

Core Competencies

- **Security Architecture & Design**: Cloud Security (AWS, M365), Network Segmentation, SIEM Engineering, Endpoint Hardening
- **Threat Detection & Response**: Detection-as-Code, Threat Hunting, Incident Response, MITRE ATT&CK Alignment
- **Technical Expertise**: Detection Engineering, Adversary Simulation, Log & Telemetry Analysis, Security Tooling Automation
- **Leadership & Strategy**: MSSP/XDR Development, Team Enablement, Customer Advisory, Executive-Level Briefings
- **Operational Excellence**: Playbook Development, Root Cause Analysis, Cross-Team Collaboration, Continuous Improvement

Professional Experience

Head, Cyber Threat Engineering & Response

Ostra Security | *July 2025 - Present*

- Streamline alert ingestion pipelines to reduce noise and enable analysts to focus on high-priority incidents.
- Design and implement automation within SOC triage and incident handling workflows to accelerate response times.
- Direct detection engineering initiatives across network, endpoint, and cloud environments to strengthen coverage of adversary TTPs.
- Develop and operationalize threat hunting and threat intelligence playbooks to proactively identify and mitigate emerging threats.
- Lead and expand SOC, detection engineering, and threat hunting teams while improving onboarding through structured training and standardized workflows.
- Provide strategic alignment of security operations with business objectives to enhance event correlation accuracy and overall organizational resilience.

Principal, Threat & Security Response

Blackwell Security | *October 2023 - July 2025*

- Engineered tailored threat detections for healthcare-specific threats across network and endpoint environments.
- Guided incident response operations including triage, escalation, and post-incident reviews.
- Provided strategic insight into tooling gaps, visibility challenges, and control weaknesses.
- Led incident response investigations during breach events to support recovery and containment.
- Created and maintained security playbooks, knowledge bases, and training materials for client and internal use.

Key Achievements:

- Standardized incident response workflows across multi-tenant healthcare clients.
- Significantly improved threat detection coverage by introducing adversary simulation into detection tuning.
- Delivered C-level advisory briefings resulting in increased security investment.

Senior Cloud Security Engineer

BigID | *November 2021 - October 2023*

- Built and maintained security tools across AWS, GCP, and Azure environments.
- Developed automation scripts and pipelines for cloud detection and response.
- Managed incident response for cloud-based workloads, collecting forensic data and mitigating threats.

- Deployed continuous monitoring solutions to track misconfigurations and vulnerabilities.
- Authored cloud security policies and enforced them via CI/CD automation.

Key Achievements:

- Decreased cloud misconfiguration incident rate by 40% through policy enforcement automation.
- Created a scalable detection framework adopted across all cloud projects.
- Reduced response time for cloud incidents by 60% using automated playbooks.
- Spearheaded onboarding of new security tooling integrated into GitLab pipelines.

Cyber Hunt Analyst / Purple Team / Signatures & E-Policy Lead

Adapt Forward Cyber Security | *July 2017 - October 2021*

- Developed custom IDS signatures and deployed them to 100+ sensors globally.
- Created playbooks and tools to support network security monitoring (NSM) operations.
- Led Purple Team exercises with Red Team collaboration for defensive validation.
- Maintained and updated WAF and IDS/IPS policies using automation and team coordination.
- Conducted threat hunts and IOC development to detect advanced threats.

Key Achievements:

- Improved detection of advanced threats across multiple military networks.
- Automated signature deployment, reducing manual errors and rollout time.
- Facilitated collaborative Red vs Blue exercises that led to significant detection rule enhancements.
- Recognized for strengthening sensor coverage and tuning policies for operational units.

Cyber Hunt Analyst

Dependable Global Solutions | *July 2014 - July 2017*

- Performed network and host-based intrusion detection for CSSP subscriber sites.
- Conducted real-time correlation and IOC analysis for active threats.
- Provided on-call support during high-severity incidents, including full 24x7 surge coverage.
- Participated in threat hunting operations and wrote initial event detection logic.
- Coordinated with external teams to resolve and document security incidents.

Key Achievements:

- Played a key role in reducing incident response time during 24x7 surges.
- Identified and responded to multiple real-world adversary campaigns.
- Created knowledge base articles and IR documentation still in use by the team.
- Contributed to CSSP’s compliance and operational audit success.

Education

Bachelor of Science in Information Systems Security

Westwood College | *2006*

Certifications

- **GCIA** - GIAC Certified Intrusion Analyst (Expired) *#3643*
- **CompTIA Security+ +**
- **CCSP** - Certified Cloud Security Professional (Expired) *(#828477)*

Professional Memberships

- **SANS** - SysAdmin, Audit, Network, and Security Institute
- **CompTIA** - Computing Technology Industry Association

References available upon request