William “Alec” Akin

Sr. Engineer, Cybersecurity | T-Mobile

Basic Information

- **Location:** Pullman, WA 99163, USA
- **Phone:** +1 (509) 592-5043
- **Email:** w.alec.akin@gmail.com
- **Homepage:** https://alecakin.com/about
- **LinkedIn:** https://www.linkedin.com/in/wakin

Languages

- Python, BASH, GoLang

Skills

- Incident Response, Forensics, and OSINT
- Insider Threat Management
- Detection Engineering
- Technical Leadership and Collaboration
- Cybersecurity Program Management
- Penetration Testing and Reverse Engineering
- Automation, Integration, Enrichment of Cyber Systems
- Cybersecurity Strategy
- Threat Modeling
- Customer Relations and Collaboration

Professional Summary

Alec is an established cybersecurity expert who is currently a Senior Engineer, Cybersecurity at T-Mobile. He has 15 years of IT experience, specializing in cybersecurity for over 12 years, though, his neurodivergent special interest has been cybersecurity since early childhood - before he even knew what to call it. His diverse background includes specialties in incident response, insider threat, reverse engineering, penetration testing, cyber intelligence, and cybersecurity strategy which includes program design, implementation and advancement. Alec has made significant contributions to renowned organizations like Boeing, Schweitzer Engineering Laboratories, NCC Group, Micron, and T-Mobile, as well as smaller organizations such as the Police Data Accessibility Project, Delta Dental of Idaho, FBI Infragard, and more.

Work History

T-Mobile - Pullman, WA

Senior Engineer, Cybersecurity | November 2020 - Current

Roles/Teams: Cybersecurity Risk Management, Detection Engineering, Cloud CIRT, Threat Hunting (Detection Validation)

- Rotated across Cybersecurity Risk Management, Detection Engineering, Cloud CIRT, and Threat Hunting teams during a nearly three-year tenure at T-Mobile. Details are team-specific unless otherwise noted.
- Advised senior leadership on cybersecurity risks and strategic initiatives.
- Served a six-month rotation on the Cloud CIRT team, focusing on incident response and automating detection/investigation strategies.
- One of two senior engineers on the Detection Engineering team, led DevSecOps, security response automation, and innovative detection solutions.
- Acted as Technical SME in corporate policy review and contributed to policy authoring
- Mentored new engineers, focusing on elevating technical skills on Risk Management and Detection Engineering teams.
- Led cross-functional projects in intelligence gathering, containment, and integration across multiple teams.
- Developed enterprise-level risk remediation strategies in collaboration with stakeholders.
- Utilized Splunk and Python to research OpenAI's applicability in cybersecurity detection and response.
- Presented on the risks and opportunities of OpenAI and ML technologies to internal teams and leadership
- Launched "Cross-Functional Friday Chat" to foster team collaboration as a self-driven initiative.
- Served as SME on high-stakes projects including incident response, threat hunting, reverse engineer, penetration testing, and advanced forensics.
- Consulted with the internal insider threat team on incident response and automated intelligence integration.
- Authored malicious code for security stack testing using the Mandiant Security Validation suite.
- Partnered with other senior and principal engineers to lead a case study on the transition to a Zero Trust architecture for all of T-Mobile.

Delta Dental of Idaho (Advanced Health Services) - Boise, ID

Cybersecurity Program Manager & Information Security Analyst | February 2019 - November 2020

- Overhauled and matured Delta Dental's cybersecurity program, exceeding leadership goals and strategic objectives.
- Launched an integrated security training program, resulting in a 70% decrease in security incidents and 100% training completion.
- Aligned the cybersecurity program with enterprise objectives, including NIST CSF, HIPAA, SOC1/2, and DDPA compliance.
- Developed a comprehensive vulnerability management program and deployed next-gen antivirus/EDR, enhancing risk mitigation and operational awareness.
- Crafted integrated plans for disaster recovery, business continuity, and incident response, enabling organizational resilience.
- Led the enterprise-scale migration from LogRhythm to Splunk as the primary SIEM, ensuring compliance and timeline objectives.
- Directed incident response for a major Emotet vector, documented in collaboration with the FBI and featured in Silent Sector Blog.

Micron - Boise, ID

Incident Response Analyst | January 2018 - January 2019

- Directed insider threat investigations, focusing on tracking threat groups and identifying APT-driven data exfiltration.
- Partnered with legal and engineering to assess insider threat-related IP violations.
- Produced risk-rated reports on key targets using deep analysis.
- Conducted memory forensics to pinpoint nation-state actors and emerging malware.
- Specialized in advanced log analysis across diverse operational settings using tools like RSA Archer, Demisto, Splunk, Microsoft eDiscovery tooling, etc.
- Spearheaded incident response planning and led investigations.

NCC Group - Austin, TX

Security Consultant | July 2017 - December 2017

- Specialized in insider threats and APTs as part of NCC Group's customer-facing IR team, also handling unique malware and advanced threat actor methodologies.
- Utilized tools like Volatility and Rekall for advanced memory forensics and threat identification including in the creation of bespoke IOCs via Splunk, Yara, and Snort.
- Conducted malware reverse engineering to dissect advanced malware behaviors with open source tools and technologies.

- Managed advanced log collection and analysis in diverse operational settings using Elastic, Splunk, and grep and other open source tooling.
- Spearheaded customer-involved incident response planning and resolution, including high-profile cases.
- Employed OSINT and custom tools including industry-known tools like Maltego for intelligence gathering on key assignments.
- Assisted in external engagements targeting advanced insider threats, leveraging detection engineering, SIEM usage, and OSINT skills.

Schweitzer Engineering Laboratories - Pullman, WA

Information Security Analyst / Associate Information Security Analyst | September 2014 - July 2017

- Established insider threat detection using advanced analytics via Splunk, proxies, and diverse log sources, enhancing organizational security.
- Managed global corporate proxy systems across 110+ locations, optimizing infrastructure for secure, reliable connectivity.
- Spearheaded vulnerability management with Rapid7 Nexpose and Acunetix, focusing on system administration and automation integration.
- Managed and utilized forensics tools like Encase and Proofpoint, supporting insider threat analysis and incident investigations.
- Advised internal departments on specialized security needs, enhancing the organization's overall security posture.
- Led incident response efforts, coordinating with cross-functional teams for effective resolution.
- Promoted within a year for exceptional performance and contributions.
- Led the SIEM platform build-up, wrote custom rules and created dashboards, elevating threat detection capabilities.
- Architected honeypots, Snort, and IDS systems, strengthening defenses against evolving and insider threats.
- Designed a custom malware analysis environment for proactive threat mitigation and incident response.

Boeing - Bellevue, WA

Information Security Intern | May 2011 - September 2014

- Contributed significantly to Boeing's cybersecurity initiatives as an Information Security Intern.
- Hired as one of Boeing's youngest interns due to self-taught cybersecurity expertise and exceptional dedication.
- Co-designed global corporate network security, enhancing cybersecurity measures and protocols.
- Participated in large-scale cybersecurity projects both independently and as a team member.

- Authored network security hardware configs, demonstrating robust security implementation skills.
- Evaluated and advised on secure data flows for aerospace/defense subsidiary networks.
- Benchmarked and identified improvement areas in network and security infrastructure.
- Enhanced infrastructure security through implementing redundancies and addressing vulnerabilities.
- Engineered complex bi-directional firewall rules, independently managing the review and off-hour implementation process.
- Contributed to threat modeling practices and provided key feedback to leadership.
- Entrusted with implementing high-security firewall rules in DoD hybrid-classified datacenter areas, supervised by a DoD-approved escort for compliance.

Additional Experience

- Police Data Accessibility Project - Board Treasurer | December 2020 - Current
- US Marine Corps Cyber Auxiliary - Cyber Auxiliarist | February 2023 - Current
- University Of Idaho - Technology Support Services IT Technician | September 2010 - August 2018
- Genesee School District #282 - Aide to the Technology Director | June 2008 - October 2008
- Texas State Guard - E4 Specialist | October 2017 - January 2018

Media And Articles

Authored Media

- 5 Cybersecurity Policies to Get You Started
- Compliance is Critical - and Potentially Indicative

External Media

Develop.Idaho 2019 via SilentSector Blog

- DEVELOP.IDAHO CONFERENCE - INCIDENT RESPONSE PANEL (presenter)

Education

Purdue University Global | Indianapolis, IN

- *Bachelor of Science Cybersecurity | January 2021 - Current - 4.0 GPA*