William "Alec" Akin

Pullman, Washington, United States

✉ w.alec.akin@gmail.com   📞 5095925043

in linkedin.com/in/wakin   🔗 https://alecakin.com/about

Summary

Alec has been a Senior Engineer, Cybersecurity at T-Mobile since November of 2020. He has roughly 15 years in IT and 11 in cybersecurity with employers including Boeing, Schweitzer Engineering Laboratories, NCC Group, Micron, and Delta Dental of Idaho. His background spans incident response, malware analysis, reverse engineering, cyber intelligence, security research, and cybersecurity leadership. In his free time, he continues to contribute his cybersecurity and technical skills. He was the Vice President on the board of Directors for FBI InfraGard's Idaho State Chapter, and is the Treasurer on the Board of Directors, former Director of Security for the Police Data Accessibility Project, and Auxiliarist for the Marine Corps Cyber Auxiliary (civilian), in addition to contributing where he can in security research, bug bounties, and providing pro-bono guidance to friends in many industries. Alec is also a staunch supporter of neurodivergence and neurodiverse inclusion and accommodation, especially as a neurodivergent person himself.

External Links/Contact:
https://www.linkedin.com/in/wakin
https://github.com/rainmana
https://alecakin.com/about/
w.alec.akin@gmail.com

Experience

Auxiliarist

Marine Corps Cyber Auxiliary

Feb 2023 - Present (4 months)

In April 2019, the Marine Corps announced the newly-established Marine Corps Cyber Auxiliary (Cyber Aux), a volunteer organization aimed at increasing Marine Corps cyberspace readiness. The Cyber Aux is comprised of a small cadre of highly-talented cyber experts who train, educate, assist, and mentor Marines to keep pace with constantly-evolving cyber challenges.

The Cyber Aux will assist in simulated environments and during periods of instruction, but are not authorized to execute hands-on cyber activities.

Primary Skills:
- Mentoring marines on evolving cybersecurity landscape leveraging personal skills and expertise
- Teaching classes and courses when asked/appropriate including travel to military installations to provide this support or via remote webinar
- Providing instruction through the use of internal forums and publishing platforms of USMC
- Participate as a civilian without "hands-on-keyboard" mentoring, guidance, teaching, etc.

Senior Cybersecurity Engineer

T-Mobile

Nov 2020 - Present (2 years 7 months)

- Provide key strategic cybersecurity insights, updates, and advisement to senior leadership on ongoing enterprise cybersecurity risks, their impact, and remediation strategies
- Perform team-lead functions to support engineers new to the field, assist in developing their skills, and provide a meaningful mentoring relationship that aligns with career and organizational goals and objectives
- Plan remediation strategies and options for complex, enterprise-impacting risks and support partner teams and organizations as a Subject Matter Expert both in a consultant role as well as lead functions - whichever necessary
- Provide meaningful cybersecurity insights, industry developments, and best practices to management and senior leadership to drive critical cybersecurity strategy development
- Consult as a Subject Matter Expert for other teams, organizations, groups, and business functions as needed and upon request where skills and experience align to drive joint, enterprise risk posture improvements (e.g., designing/developing automation solutions to address massive OSINT gathering, automation, Python programming, penetration testing, incident response, legal team support, mobile application and mobile device project consulting, etc.)

Shifted to CTP CSODS/Detection Engineering Team in Summer 2022:
- Primary DevSecOps Engineer (automation, data science, development, code, etc.) to our SIEM teams in support of their mission - especially in a SOAR context and expanding our capabilities
- Cybersecurity presenter and public speaker for internal groups as well as whole company (typically focused on security awareness but have also covered emerging technologies and where they could be leveraged to further strategic objectives and goals)

Started Six Month Rotation on CTP CIRT Team January, 2023
- Quickly come up to speed to assist CIRT as a temporary member by performing all expected responsibilities and actions of regular CIRT member

/* **Treasure Board of Directors**
Police Data Accessibility Project, Inc.
Dec 2020 - Present (2 years 6 months)
- Active Treasurer and Board of Directors board member for the Police Data Accessibility Project. This role also includes utilizing my experience as a cybersecurity career professional to provide critical strategic insights on the evolving security threats that face a non-profit, open-source project

- More information can be found at the following URLs (including media/articles and other information):

Website: https://pdap.io
GuideStar: https://www.guidestar.org/profile/85-4207132
WIRED article: https://www.wired.com/story/police-accountability-data-project-open-source-reddit/
Vice Motherboard: https://www.vice.com/en/article/5dpxvq/this-transparency-project-is-creating-a-massive-collection-of-police-data

Cybersecurity Program Manager
Advanced Health Services (A Subsidiary of Delta Dental of Idaho)
Aug 2019 - Nov 2020 (1 year 4 months)
- Manage, mature, develop, and expand the cybersecurity program for Idaho's leading dental insurance providers with more Delta Dental member companies and others to be added over time

- Developed and matured the program to meet enterprise goals and objectives as well as align with strategic plans
- Subject matter expert on all cybersecurity-related parts of the enterprise both internally as well as external
- Plan, implement and improve upon existing infrastructure to bring innovative, effective, and efficient use of resources to better protect the business
- Build, maintain, and grow meaningful professional relationships with managers, senior managers, executives, individual contributors, and other owners of primary enterprise functions to further cybersecurity program's objectives, including support of compliance and regulatory objectives (NIST CSF, HIPAA, SOC1/2, DDPA, etc.)
- Manage vulnerability remediation program making sure all risks are understood from "50,000 foot" down to proof-of-concept exploitation and demonstration if necessary and remediation planning, timelines, and resource-planning analysis and recommendations
- Threat model complex risks affecting disparate parts of the business with significant enterprise impact whether financial, regulatory, or compliance, incident planning, or disaster recovery and business continuity
- Developed comprehensive incident response, disaster recovery, and business continuity plan with corporate stakeholders
- Lobbied for, chose, planned, integrated, and migrated from LogRhythm SIEM to Splunk at enterprise scale both from a management perspective, as well as primary "hands-on-keyboard" technical lead perspective. Worked with both onsite/internal customers as well as professional services coordinating and performing most aspects of migration and integration. These activities were performed in a way which met compliance and regulatory objectives as well as strategic and timeline objectives.

Volunteer Staff
Sweet William Foundation
Oct 2018 - Jan 2020 (1 year 4 months)
- Leverage and lead technological solutions to progress mission objectives

- Engage technology teams across different projects to produce results in technology, media development, information security, and application development

Information Security Analyst
Delta Dental of Idaho
Feb 2019 - Jul 2019 (6 months)
- Reviewed, restructured, and revitalized cybersecurity program to meet and exceed leadership expectations and strategic objectives
- Designed and implemented a security awareness training program and integrated it with H.R. performance tracking
- Implemented M.F.A. product addressing current and previously unknown risks to the enterprise by limited attack surface area
- Created Disaster Recovery and Business Continuity as well as Incident Response Plan in conjunction with corporate stakeholders
- Managed third-party security consultancy as a "force-multiplier" utilizing expertise to augment and improve current projects and deliverables
- Lobbied for and led the implementation of next-generation antivirus/E.D.R. product significantly increasing operational awareness, incident response capability, and decreasing attack surface area

- Led incident response team during an incident which later was developed into a presentation done in concert with the F.B.I. and Idaho business leaders. Spoke explicitly on incident response methodology and process for forensic analysis of potential Emotet infection vector

Media:
A security company's blog/write-up on the incident response activities listed above - https://www.silentsector.com/blog/develop-idaho-boise-conference-incident-response

Incident Response Analyst
Micron Technology

Jan 2018 - Jan 2019 (1 year 1 month)
- Track and identify targets of interest to produce reports of activities and provide executive team and legal counsel ratings of risk and other factors for short term investigations as well as long term including applied OSINT gathering techniques and tradecraft to additionally enrich reports
- Memory forensics image gathering and analysis to identify potential nation-state sponsored threat actors and new malware strains, including manual malware analysis and reverse engineering
- Advanced log collection and analysis of samples from a variety of environments, including standard enterprise networking environments to ICS/SCADA and manufacturing environments
- Incident response planning as well as execution as a primary team member with internal customers and as a lead for investigations

E4 Specialist (Honorable Discharge)
Texas State Guard

Oct 2017 - Jan 2018 (4 months)
- Assisted in the development of TXSG's first Cyber Security Team at the request of Governor
- Assisted in re-architecture of Texas Military Department bases of operation to improve the security of defense systems
- Provided advanced consultation to senior officers utilizing skills used in the corporate industry focusing primarily on security architecture design, deployment, and advancement as well as incident response and intelligence
- Assisted in the protection and enhancement of critical public service infrastructure including, but not limited to, essential systems of evacuation, communications, and emergency planning in the event of both manmade as well as natural disasters
- Modified service contract in the event of relocation as well as enlistment as E4 Specialist with fast-track plan to Chief Warrant Officer
- NCO and Senior Officer references are also available upon request, as well as discharge letters

Security Consultant
NCC Group

Jul 2017 - Dec 2017 (6 months)
- Advanced memory forensics image gathering and analysis using a variety of tools, but specifically focused on Volatility and Rekall for manual memory capture analysis
- Advanced malware analysis and reverse engineering utilizing tools such as strings, xxd, binwalk, etc.
- Advanced log collection and analysis of samples from a variety of environments from small companies to very large, utilizing custom capture and analysis tooling, Elastic, Splunk, and Linux tools such as grep
- Participated in incident response planning as well as execution as a primary team member with external customers

- Advanced use of OSINT and other intelligence gathering techniques and tools to further currently assigned projects utilizing custom searches, Maltego, and other tools

Information Security Analyst

Schweitzer Engineering Laboratories (SEL)

Oct 2015 - Jul 2017 (1 year 10 months)

- Primary product manager, Engineer, and SME of global corporate proxy systems supporting field offices in over 60 locations in the US and 50 internationally in 24 countries and expanding
- Primary product manager, engineering, and SME of forensics tools and systems in support of insider threat analysis and corporate investigations
- Support other internal organizations in the applied use of specialized security experience, especially to critical infrastructure
- Key incident response planning as well as execution as a primary team member

Associate Information Security Analyst

Schweitzer Engineering Laboratories (SEL)

Sep 2014 - Sep 2015 (1 year 1 month)

- Primary product manager and engineer for global SIEM implementation and deployment. This responsibility included writing custom SIEM rules, Snort signatures, performing advanced searches and dashboard creation, etc. to meet customer requirements
- Primary architect/designer, product manager, SME, and engineer for advanced detection and intelligence systems, including honeypots, snort, and IDS systems
- Primary architect, product manager, user, and engineer of custom malware analysis environment

Information Security Intern

Boeing

May 2011 - Sep 2014 (3 years 5 months)

Aiding in the re-design of global corporate network security systems

- Working on large-scale projects in a team setting as well as a single person
- Writing configuration files for network security hardware
- Assisted in evaluation of subsidiary companies' aerospace/defense-centric networks and produced recommended architecture for secure data flows between new subsidiaries and established corporate network infrastructure
- Evaluating networks and security infrastructure compared to established standards
- Improving upon established infrastructure to create redundancies and patch holes in security flaws and vulnerabilities
- Firewall engineering includes writing custom rules to meet customer needs for advanced, complex, bi-directional dataflow in advanced applications. Scheduled the review process and implemented rules independently in off-hours
- Assisted in the implementation of threat modeling practices as well as performed threat modeling analysis independently and provided feedback and guidance to leadership
- One of three primary firewall engineers tasked with implementing high security/high trust firewall rules for critical, sensitive applications in controlled areas to meet specific customer needs

Intern

St. Augustine's Catholic Center

Jan 2013 - May 2014 (1 year 5 months)
- Assist in daily tasks asked of by the Campus Minister, Secretary, and Parish Priest as well as other members of the staff
- Update web content to reflect current and upcoming events as well as archive content for future use
- Focus on the broad use of social media as well as other diverse technologies to further campus ministry objectives

Volunteer Intern
City of Moscow
Feb 2012 - Apr 2012 (3 months)
- Take questions from civilians and provide information in a timely fashion. Call officers when civilians needed assistance from an officer stationed on campus

Associated Students University of Idaho - ASUI Director of Technology
University of Idaho
Aug 2011 - Apr 2012 (9 months)
- Primary contact for anything related to information technology/technology development for the student body at the University of Idaho
- Main web developer for www.asui.uidaho.edu
- Provide consultation to ASUI senators as well as executive staff in technology-related topics

High Beta - Vice President (Interim)
Lambda Chi Alpha - Epsilon Gamma Chapter
Nov 2011 - Jan 2012 (3 months)
- Handled internal conflict resolution and organized events to bring members closer together
- Assumed presidential role when the president is unable to and assumed those responsibilities when needed

High Delta - Recruitment Chair
Lambda Chi Alpha - Epsilon Gamma Chapter
May 2011 - Nov 2011 (7 months)
- Directly in charge of all activities regarding recruitment for the fraternity
- Assisting others in the activities regarding the general recruitment processes as well as during the Rush time frame
- Position was mainly based on a keen sense of organizational abilities and the ability to work in a team setting as well as on your abilities and to identify potential candidates that fit a strict set of moral guidelines, core values, and demonstrated those in contextualized situations

Technology Support Services IT Technician
University of Idaho
Sep 2010 - Aug 2011 (1 year)
- Worked with Staff and Administrators
- All types of support problem-solving networking issues, re-imaging and backing up critical systems
- Rebuilt physical hardware components and all types of desktop support
- Heavy emphasis and experience working in customer relations

My primary goal was providing advanced technical support to staff and administrators, which went beyond the general support provided by the help desk. The job was customer support based on an on-the-hour charging system in a fast-paced and competitive work environment. I supported everything from network connectivity issues to operating system rebuilds, data recovery, and endpoint security forensics.

Aide to the Technology Director

Genesee Joint School District 282

Jun 2008 - Sep 2008 (4 months)

Installing, maintaining, and updating windows based systems
- Assistance in the migration from a Novell based network environment to a Microsoft Enterprise network environment
- Installation and maintenance of new network hardware
- Adding systems to Active Directory
- Help in the creation of User Policies as well as User Groups for students

Education

Purdue Global

Bachelor's of Science, Cybersecurity

2021 - 2024

I am pursuing my bachelor's degree in Cybersecurity at Purdue's online school, Purdue University Global. I have maintained a 4.0 GPA during my education at Purdue thus far.

University of Idaho

No Degree Earned, Political Science

2010 - 2014

Licenses & Certifications

CPR and AED - American Red Cross
Issued Jun 2015 - Expires Jun 2017

First Aid - American Red Cross
Issued Jun 2015 - Expires Jun 2017

Skills

Security Incident Response • Python (Programming Language) • Risk Management • Reverse Engineering • Malware Analysis • Leadership • Cross-functional Collaborations • Penetration Testing • Cybersecurity Strategy • AI Prompt Engineering