Alexander Wiegman

San Francisco, California | alex@madicetea.me | (209)-353-5377 |
https://github.com/madicetea | https://www.linkedin.com/in/mrlogicalalex

Key Skills and Competencies

- Identity & Access Management (IAM) Administration
- Team Collaboration Lead
- Data Visualisation (JIRA, Redash)
- Security Policy Technical Implementation
- Curious to emerging threats and technologies
- Data Reports' Script Writing (Python, SQL)
- Detailed, Customer-Focused Problem Solving
- Prometheus and Grafana alerting
- Incident Detection and Pattern Recognition
- Incident Post-Mortem Documentation
- Incident Trend and Root Cause Analysis
- Identity Provider (IdP) authentication (SSO, SAML, OIDC)
- Automated Endpoint Compliance Monitoring
- Security Policy and Procedure Development
- Security Tooling for architecting integrations
- Threat Signature Writing

Certifications:

Azure System Administrator AZ-104	| 2021-2024
AWS Cloud Practitioner CLF-C01	| 2021-2024
CompTIA Network+ (ce / N10-008)	| 2022-2025
CompTIA Security+ (ce / SY0-601)	| 2021-2025
CompTIA A+ (ce / 220-1101 and 220-1102)	| 2017-2025
CompTIA Mobility+ MB0-001	| 2017-2024
CompTIA CDIA+ CD0-001	| 2017-2024

Work Experience

Cloud Security Solutions Engineer **Amazon Web Services, Inc.** **06/2023 - (ongoing)**
Remote

- Coordinated 100 investigatory and compliance solutions requests across 12 AWS Security service domains for high-value corporate and Japanese government AWS clients, within a 2-3 day average turnaround time.

- Achieved a 98% customer satisfaction rating by delivering exceptional customer experiences.

- Innovated a process, reducing Japanese language correspondence review time by at least one (1) day.

- Proactively identified and escalated five (5) technical and two (2) localization edits, enhancing AWS documentation page accuracy and improving the customer image of AWS worldwide.

- Orchestrated cross-functional team collaboration for three (3) feature request initiatives, substantiating the need for implementation with data from up to 300 customers.

GRC Security Administrator **Blameless, Inc.** **05/2022 – 01/2023**
Remote

- Spearheaded the technical implementation of vendor risk management using OneTrust VRM and introduced two self-service "Security Profile" platforms - OneTrust and Whistic.

    - Integrated Whistic with Salesforce, granting Sales and Legal quicker access to share our standard customer trust questionnaires, reducing the pre-sales cycle by up to one week, and contributing to over $25 million in Annual Recurring Revenue (ARR).

- Designed and managed corporate endpoint device management for compliance with AICPA SOC2 Type 1 and ISO 27001:2013 standards, selecting and configuring Endpoint Detection and Response (SentinelOne EDR), Data Loss Prevention (Google Workspace DLP), Automated Technical Compliance (Drata), and Mobile Device Management (JAMF & Intune MDM). Also administered Identity and Access Management for over 80 employees across multiple platforms, including Azure and Google Workspace.

- Managed the Security team's response during two (2) security incidents, ensuring proper change management and compliance with regulatory standards such as GDPR and CCPA.

- Founded our annual Security & Privacy awareness program, delivering training through KnowBe4 and conducting semi-annual phishing tests. Increased organizational phishing awareness from 50% to 70%.

- Directed a monthly internal audit program, collaborating across all teams and management levels to proactively reduce organizational risk. Audits focused on access control, policy adherence, and audit trail alerts, ensuring comprehensive center-out model of governance throughout the company.

Governance Risk & Compliance (GRC) Analyst **Kong, Inc.** **09/2021 – 05/2022**
Remote

- Led an AICPA SOC 2 Type 2 audit (over 5 weeks) and co-presented an ISO 27001:2013 pre-assessment (over 1 week) to ensure customer trust and guide compliance policy development.

- Managed corporate security and technical control software deployments, including Proofpoint DLP, CrowdStrike EDR, Splunk SIEM data logging, and Drata (an automated endpoint compliance recorder).

- Led sales prospect document sharing and security questionnaire policy, streamlining processes with SIG-LITE questionnaires and OKTA SSO integration to OneTrust QRA.

- Authored a streamlined change management workflow in JIRA, ensuring compliant changes without impacting engineering teams.

- Consulted with Legal and Management to advise on the Personal Information Privacy Law (PIPL) of China during the planning stages for opening a new office location in China.

- Created JIRA visualization dashboards and filtered lists for valuable reporting insights for corporate leadership.

Senior Security Operations Analyst **PerimeterX, Inc.** **11/2019 – 08/2021**
San Mateo, CA / Remote

- Achieved a 99% satisfaction rating throughout a few thousand customer correspondences, specializing in customer solutions for technical integrations, data logging, high-value AIO software research, JavaScript supply-chain risk analysis, and asset identification questionnaires (e.g., cookies and scripts).

- Designed and deployed 30 automated alerting patterns and data query systems, utilizing Prometheus with Grafana visualisation, and YAML, SQL, JavaScript, and Python for Slack alerting, to significantly enhance data analysis and threat detection capabilities.

- Automated and optimized 20 SQL queries with parameters, resulting in a 40%-75% efficiency improvement and a 250% boost in usability across customer-facing teams. Generated and delivered pivotal reports contributing to securing up-sell agreements up to 550%.

- Contributed suggestions for three (3) novel solutions at Architecture and Product discussions that quickened customer onboarding by up to 10%.

- Collaborated cross-functionally with R&D, Product, Solutions Integration, Success, and Sales teams to develop hundreds (100s) of innovative AI detection patterns, matching billions of requests, for Indicators of Compromise (IoC).

- Served as a Subject Matter Expert (SME) lead and mentored a team of ten (10) including three (3) Security Operation Center (SOC) individuals on a range of topics, including solutions architecture, integrations infrastructure (e.g., Fastly, Amazon CloudFront, Cloudflare, NodeJS, NGINX, Apache), YARA/SQL/Lucene signature creation, client-side JavaScript analysis, SQL and Python programming, red/blue team threat research, mobile app QA testing, version control, issue tracking, data export, portability solutions, and CCPA/GDPR compliance.

Security Research Analyst **Pipeline Security, K.K.** **02/2019 – 07/2019**
Tokyo, Japan

- Proactively researched and addressed risk vulnerabilities, enhancing knowledge of regional security threats in APAC for Spamhaus. This involved configuring secure policies and installing updates on cloud-hosted virtual machines to bolster security measures.

- Designed and implemented a BIND DNS server with Response-Policy Zones to facilitate SIEM data ingestion and visualization through Elastic, Logstash, and Kibana (ELK). This implementation significantly improved threat detection capabilities.

- Demonstrated technical expertise and commitment by authoring and publishing four (4) informative how-to articles, while also leading the redesign of the knowledgebase and homepage. These efforts resulted in an enriched user experience with a more intuitive interface.

- Provided essential production support to three customer companies, directly contributing to an up-sell of over 200% for one (1) of the clients.

- Investigated and resolved a false-positive spam listing issue, attributed to a shared hosting provider's nameservers (NS), with a recovery time objective (RTO) of one (1) day. Diligent analysis and corrective actions ensured high availability for our email communication.

- Actively spearheaded cost-saving initiatives by overseeing secure data destruction and modernizing operating systems and software on company computers. These measures not only enhanced security but also led to savings of over 750,000 Japanese yen in operating costs.

Security Engineer & Website Developer **Junction Ltd.** **10/2016 – 05/2017**
Tokyo, Japan

- Identified and responsibly disclosed a security vulnerability in the Hackathon's signup form, ensuring the protection of personal information.

- Co-authored and published the Junction Tokyo 2017 hackathon website, which is currently archived in the Internet Archive Wayback Machine.

- Developed expertise in WordPress backend administration, including security plugins, implementation of Let's Encrypt HTTPS certificates, and knowledge of European and Finnish digital security laws.

- Collaborated with the social networking team to create and share Twitter updates (now X) for website and event promotion.

- Assumed responsibility for managing network security, conducting data forensics, and overseeing physical security measures in sponsors' demo areas during the Hackathon event.

Other Roles Held

Faculty Development Curriculum Researcher – University of Tokyo | 09/2018 - 02/2020

Remote Sensing Engineering Researcher – Institute of Industrial Science, University of Tokyo | 09/2018 - 08/2019

Student Council Governance, and Technology Logistics Officer – University of Tokyo | 05/2016 - 08/2019

Dorm Resident Assistant – University of Tokyo | 09/2017 - 08/2019

English Conversation Tutor – University of Tokyo | 09/2017 - 07/2019

Professional Ethics Lecturer – University of Tokyo | 09/2018 - 12/2018

Biology Lab Teaching Assistant – University of Tokyo | 01/2018 - 02/2018

Education

San Jose State University **06/2023 – (ongoing)**
Master's degree in Library and Information Science (MLIS) [*ongoing*]

GPA: 3.94

Selected Relevant Coursework: Information Security – Info (Risk) Assurance, Open Education Librarianship

San Jose City College / Modesto Junior College **01/2020 – 05/2020**
Coursework in *Certificate* for CIS Unix Networks, Level 1 (*paused)*

Selected Relevant Coursework: Introduction to Unix/Linux, Linux System Administration via Red Hat Academy, C/C++ Programming, Internet Principles and Protocols

(The) University of Tokyo [UTokyo] **09/2015 – 09/2019**
Bachelor's degree in Environmental Science & *Minors* in Informatics & Science and Technology Studies

Selected Relevant Coursework: Neural Networks in Remote Sensing, Android Application Development, Operating Systems, Computer Architecture, Compilers, Database Management Systems with SQL, Human Impacts on Artificial Intelligence, Artificial Intelligence and Statistical Machine Learning for Engineering Students, Mathematical Modelling and Simulations with MATLAB, OpenCV with C++, Deep Learning with Python

Relevant List of Skills

Operating Systems:

Windows, Mac, Linux (RHEL, Fedora, ChromeOS, Debian, CentOS, Android, Ubuntu)

Software and Platforms:

[Technical Software and Platforms]

UNIX bash, SQL, VCL, JavaScript, Python, HTML, YAML, JSON, Java, Ruby, AWS CloudFormation, AWS CloudTrail, Amazon CloudWatch, AWS IAM, AWS Organizations, AWS IAM Identity Center (SSO), AWS GuardDuty, AWS SecurityHub, AWS Elastic Cloud Compute (EC2), AWS Elastic Load Balancer (ELB), AWS Security Groups, AWS Config, AWS QuickSight, AWS Billing, AWS CostExplorer, Google Earth Engine, Google Maps API, Google Compute Engine, BigQuery, VMWare, Fastly, Prometheus, Elastic Logstash Kibana (ELK), CircleCI, git, SSH, whois, Jenkins, homebrew, Insomnia, DMARC, Android Studio, JAMF, Intune, Mobile Device Management (MDM), Splunk, Security Incident and Event Management (SIEM), Proofpoint, Google Workspace, Data Loss Prevention (DLP), SentinelOne, CrowdStrike, Endpoint Detection and Response (EDR), Drata, Azure Active Directory, Identity and Access Management (IAM), Google Groups, Google SAML, OKTA SAML, Docker, Kubernetes, MongoDB Atlas, Qualys, web browser "navigation" JavaScript API, Grafana, Slack Bot API, Discord Bot API, Indicators of Compromise (IoC), Security and Artificial Intelligence, Domain Name System (DNS), Response-Policy Zones, Content Delivery Network (CDN), Managed Security Service Provider (MSSP), Managed Detection and Response (MDR), Extended Detection and Response (XDR), Security Orchestration, Automation and Response (SOAR), Data Delivery, Datadog, Sentry, Sumo Logic, HTTP Endpoint Data Streaming, SendGrid, HubSpot, Autonomous System [Number]s (AS[N]), Internet Topology, JIRA, Atlassian Confluence, Whistic, Data Classification, Threat Modeling, Qualitative Risk Analysis, Quantitative Risk Analysis, Security Incident Response Plan (SIRP), Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), Privacy Impact Assessment (PIA), Continuous Monitoring, Secure Development Lifecycle (SDLC), Security Operations Center (SOC), Security Governance, Security Compliance, Security Policy and Procedures, Security Metrics, Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), Risk Mitigation, Risk Assessment Methodologies, Data Encryption, Data Masking, Data Anonymization, Data Retention Policy, NIST Cybersecurity Framework, MITRE AT&CK Cybsercurity Framework, Two-Factor Authentication (2FA), Multi-Factor Authentication (MFA), Cloud Security, Container Security, Zero Trust Architecture, Internal Audit, Business Continuity and Disaster Recovery (BCDR), Data Encryption and Key Management Solutions, Threat Intelligence Platforms and Feeds, Security Ratings and Scoring Services, Security Analytics and Behavioral Analysis Tools, Security Awareness Training Platforms, Phishing Simulation Platforms, Spamhaus, KnowBe4

[Security Controls and Regulatory Standards]

Center for Internet Security (CIS) Controls, Payment Card Industry Data Security Standard (PCI DSS), HIPAA, SIG-LITE Questionaries (ver. 2020-2022), NIST 800-53, NIST 800-88, Code of Federal Regulations (CFR) Sections 10, 21, and 42, AICPA SOC 2 Type 1, AICPA SOC 2 Type 2, ISO 27001:2013, ISO 27001:2022, Security Regulatory Standards, General Data Protection Regulation (GDPR), EU-US Privacy Shield, California Consumer Protection Act (CCPA), California Privacy Rights Act (CPRA), Personal Information Protection Law of China (PIPL), Act on the Protection of Personal Information of Japan (APPI)