

Ahmed Sartaj

Cybersecurity Analyst | SOC Operations | Incident Response | Detection Engineering | Cloud Security | Vulnerability Management

Mississauga, ON | (437) 605-6310 | itsme_ahmed@outlook.com | linkedin.com/in/ahmedsartaj | github.com/MalcomX21

PROFESSIONAL SUMMARY

Cybersecurity professional with a Master of Science in Computer Science and 3+ years of hands-on experience across SOC operations, incident response, detection engineering, threat intelligence, vulnerability management, cloud security, and identity and access management in a Managed Security Service Provider environment. Monitors, triages, and investigates 60+ daily security alerts across Microsoft Sentinel, IBM QRadar, Splunk, CrowdStrike Falcon, and Microsoft Defender for enterprise environments supporting 3,400+ users, maintaining 30 to 60 minute SLAs. Engineers 100+ MITRE ATT&CK; mapped detection rules, achieving 80% false positive reduction and 70% breach exposure reduction. Conducts forensic investigations, root cause analysis, and post-incident reviews. Supports vulnerability assessment, cloud security posture evaluation across AWS and Azure, SAST and DAST findings analysis, and compliance activities including NIST CSF, ISO 27001, PCI DSS, and SOC 2. Automates security operations using Python, PowerShell, and Bash, reducing manual overhead by 35%. Holds CHFI, IBM QRadar SIEM V7.4.3, CCNA, AWS Solutions Architect, and Enterprise Security Fundamentals certifications, with CompTIA Security+ and Network+ training. Currently pursuing CyberArk Sentry and PAM Defender, Microsoft SC-300, and AWS Security Specialty.

TECHNICAL SKILLS

Security Operations and Monitoring:	Security Operations Centre (SOC) Operations (Tier 1, Tier 2, Tier 3), Security Monitoring, Event Detection, Event Filtering, Event Investigation, Alert Triage, Validation, and Analysis, Incident Identification and Assessment, 24/7 SOC Environment, Shift-Based Operations, Incident Scope Establishment, Escalation Decision-Making, Service Desk Ticket Management, SLA Adherence
SIEM, EDR, and Security Tooling:	Microsoft Sentinel (KQL, Analytic Rules, Workbooks, Playbooks), IBM QRadar SIEM V7.4.3 (Certified, AQL, Offense Management, Rule Tuning), Splunk (SPL, Correlation Searches, Dashboards), ArcSight (familiar), CrowdStrike Falcon EDR, Microsoft Defender for Endpoint, Cortex XDR (familiar), Red Canary MDR (familiar), IDS/IPS (Snort, Suricata familiar, Cisco FirePower), CSPM (Wiz familiar, AWS Security Hub, Microsoft Defender for Cloud), WAF (AWS WAF, Cloudflare familiar), Cloud-Native Logging (CloudTrail, Azure Monitor)
Incident Response and Digital Forensics (DFIR):	Incident Response Lifecycle: Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Lessons Learned, Incident Response Playbook and Runbook Development and Maintenance, Root Cause Analysis, Attack Vector and Timeline Reconstruction, Post-Incident Review and Documentation, Digital Evidence Collection and Analysis, Chain of Custody Concepts, CHFI Certified (EC-Council), Computer Hacking Forensic Investigation
Threat Intelligence and Threat Hunting:	Cyber Threat Intelligence (CTI) Collection, Analysis, and Dissemination, Multi-Source Intelligence Analysis, Emerging Threat Identification, Threat Actor Profiling and TTP Analysis, Indicators of Compromise (IOC) Identification, Enrichment, and Sharing, Proactive Threat Hunting Across Enterprise Environments, MITRE ATT&CK; Framework (Technique Mapping, Coverage Analysis, Detection Gap Analysis), Open-Source and Commercial Threat Feeds, STIX/TAXII (familiar)
Detection Engineering:	Detection Use Case Development and Tuning, 100+ MITRE ATT&CK; Mapped Detection Rules Engineered, KQL, AQL, SPL, Sigma Rules (familiar), Behavioral Analytics, False Positive Reduction (80%), Detection-as-Code Methodologies, Alert Triage Automation, Signature Tuning and Alert Analysis
Vulnerability Management:	Vulnerability Assessment and Risk Prioritization, Technical Scan Data Synthesis, Exploitability Analysis, CVE and NVD Analysis, CVSS Scoring, Nessus (Tenable familiar), Qualys (familiar), Nuclei (familiar), Patch Management Coordination, Remediation Guidance Development, Vulnerability Lifecycle Management
Cloud Security:	AWS (Solutions Architect Certified, EC2, S3, IAM, CloudTrail, GuardDuty, Security Hub, VPC, WAF, KMS, Lambda), Microsoft Azure (Entra ID, Defender for Cloud, Conditional Access, PIM, Key Vault, Azure Monitor, Sentinel), Google Cloud Platform (GCP, familiar), Cloud Security Posture Management (CSPM), CIS Benchmark Evaluation, Cloud Access Security Broker (CASB) Concepts, SaaS and Cloud-Native Environment Security, Zero Trust Architecture

Identity and Access Management (IAM):	Active Directory (Users, Groups, GPOs, NTFS Security, Domain Infrastructure), Entra ID / Azure AD (MFA, Conditional Access, PIM, Access Reviews, SSO), LDAP, SAML, OAuth, OpenID Connect, User Lifecycle Management (Onboarding, Offboarding, Access Provisioning), Privileged Access Management (PAM) Concepts, CyberArk Training (In Progress), Just-In-Time (JIT) and Just-Enough-Access (JEA) Concepts, Okta (familiar), SailPoint (familiar)
Network Security:	Firewall Administration (Fortinet FortiGate, Cisco ASA/FTD, Palo Alto familiar), Intrusion Detection and Prevention Systems (IDS/IPS), VPN Communication Protocols (IPsec, SSL/TLS, WireGuard), Network Segmentation, VLANs, Network Access Control (NAC concepts), TCP/IP, DNS, DHCP, LAN/WAN, Wireless Networking, Routing Protocols (BGP, OSPF concepts), CCNA Certified, Network Traffic Analysis, Packet Capture (Wireshark, tcpdump)
Application Security:	SAST (Static Application Security Testing) Findings Analysis, DAST (Dynamic Application Security Testing) Findings Analysis, SCA (Software Composition Analysis), OWASP Top 10, CWE, Secure Code Review Concepts, Snyk (familiar), SonarQube (familiar), Burp Suite (familiar), API Security, REST API Security, API Authentication and Authorization, SDLC Security Integration, DevSecOps Concepts
Operating Systems:	Windows Server 2016/2019/2022, Windows 10/11 Pro, Linux (Ubuntu, CentOS, RHEL): Command-Line Administration, Log Analysis, System Hardening, Shell Scripting, Unix (familiar), macOS (familiar), AIX and Solaris (familiar), Event Log Analysis, Sysinternals, Process Monitoring
Scripting and Automation:	Python (Security Automation, IOC Enrichment, Detection Tooling, Log Parsing, REST API Integration, Malware Analysis Scripts), PowerShell (AD Administration, M365 Security, Bulk Operations, Audit Scripting), Bash (Linux Administration, Shell Scripting, Automation), SOAR Workflow Automation, AI-Augmented Security Operations, REST API, JSON, YAML, KQL, SPL, AQL, SQL, Git/GitHub, VS Code
Compliance, GRC, and Frameworks:	NIST Cybersecurity Framework (CSF), NIST SP 800-53, NIST SP 800-171, ISO 27001, ISO 27002, SOC 2 Type II, PCI DSS, GDPR, HIPAA (familiar), ITIL Incident, Problem, and Change Management, CIS Benchmarks and CIS Controls, Risk Assessment and Risk Management, Security Policy Development and Documentation, Third-Party and Vendor Risk Management, Audit Evidence Collection
Containerization and DevSecOps (Familiar):	Docker (Container Build, Configuration, Management), Kubernetes (Cluster Concepts, Pod Security Policies, familiar), CI/CD Pipeline Security Concepts, Infrastructure as Code (Terraform familiar, ARM Templates familiar), Container Security Scanning
Certifications:	CHFI (Computer Hacking Forensic Investigator, EC-Council), IBM QRadar SIEM V7.4.3 Certified, AWS Certified Solutions Architect, CCNA (Cisco Certified Network Associate), Enterprise Security Fundamentals (BlueCape Security), CompTIA Security+ (trained), CompTIA Network+ (trained)
Certifications In Progress:	CyberArk Sentry, CyberArk PAM Defender, Microsoft SC-300 (Identity and Access Administrator), AWS Certified Security Specialty, Microsoft SCCM

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst / Security Engineer

Ebryx LLC, Managed Security Service Provider | Remote | June 2022 to September 2024

- Monitored, triaged, validated, and investigated 60+ daily security alerts across Microsoft Sentinel, IBM QRadar, Splunk, CrowdStrike Falcon, and Microsoft Defender for enterprise environments supporting 3,400+ users, maintaining 30 to 60 minute SLAs in a 24/7 SOC environment.
- Engineered 100+ MITRE ATT&CK; mapped detection rules across KQL, AQL, and SPL, reducing false positive escalations by 80% and breach exposure by 70%, and continuously tuned signatures based on threat intelligence and operational feedback.
- Led and contributed to incident response engagements across the full lifecycle including preparation, detection, analysis, containment, eradication, recovery, and post-incident review, resolving critical incidents within SLA.
- Performed digital forensics investigations including digital evidence analysis, attack vector reconstruction, timeline analysis, and root cause identification (CHFI certified), producing detailed post-incident reports for internal and client stakeholders.
- Collected and analyzed cyber threat intelligence from open-source and commercial feeds, enriched indicators of compromise, performed proactive threat hunting, and shared actionable threat assessments with internal teams and clients.
- Conducted vulnerability assessments across enterprise environments, prioritized critical vulnerabilities by risk and exploitability, coordinated remediation with engineering teams, and produced mitigation guidance for client reporting.
- Implemented cloud security controls across AWS and Azure including IAM policy configuration, GuardDuty, Security Hub, Defender for Cloud, Conditional Access, and encryption key management, conducting CIS Benchmark assessments.

- Analyzed SAST and DAST findings from application security tooling, prioritized by exploitability, and provided engineering teams with actionable remediation context including fix guidance and secure coding references.
- Managed identity and access across Active Directory, Entra ID, MFA, and Conditional Access for 3,400+ users, enforced least privilege access, and supported access reviews and privileged access management workflows.
- Developed and maintained incident response playbooks covering phishing, malware, lateral movement, credential compromise, cloud misconfiguration, and data exfiltration scenarios, aligned with NIST CSF.
- Automated security operations workflows using Python, PowerShell, and Bash for IOC enrichment, alert triage, detection rule generation, log parsing, and SOAR integration, reducing manual investigation overhead by 35%.
- Supported compliance activities including NIST CSF, ISO 27001, PCI DSS, and SOC 2 audit evidence collection, policy documentation, and control gap remediation.

Associate Cybersecurity Analyst / Junior Security Engineer

Ebryx LLC, Managed Security Service Provider | Remote | November 2021 to June 2022

- Monitored SIEM platforms, triaged Tier 1 security alerts, and escalated complex incidents to senior analysts with complete investigation context and IOC findings.
- Supported vulnerability scan analysis, IOC enrichment, and detection rule tuning under senior analyst guidance.
- Administered Active Directory, Microsoft 365, and endpoint protection for enterprise clients across onboarding and offboarding lifecycle workflows.
- Contributed to playbook development, knowledge base articles, and standard operating procedures for recurring alert categories.
- Developed Python and PowerShell scripts for log parsing, account auditing, and configuration comparison across managed environments.

Service Advisor

Canadian Tire | Mississauga, ON | October 2024 to Present

- Delivered front-line IT support and customer experience assistance across 40+ weekly cases, performing ticket handling, troubleshooting, hardware and software diagnostics, and escalation coordination.
- Managed tickets through resolution lifecycle with clear documentation, improving resolution rate by 25% and reducing average resolution time by 20%.
- Communicated technical findings and recommendations clearly to non-technical stakeholders, demonstrating stakeholder communication skills required for cross-functional security engagement.

KEY PROJECTS

MITRE ATT&CK; Detection Engineering Program: Developed and tuned 100+ detection rules across Microsoft Sentinel (KQL), IBM QRadar (AQL), and Splunk (SPL) mapped to MITRE ATT&CK; techniques, reducing false positive escalations by 80% and improving coverage of initial access, lateral movement, privilege escalation, and exfiltration techniques.

Incident Response and Digital Forensics Operations: Led and contributed to incident response engagements across the full lifecycle, performed digital evidence analysis and attack vector reconstruction, and reduced breach exposure by 70% through structured containment and eradication workflows.

Cloud Security Posture and Vulnerability Management: Assessed cloud environments across AWS and Azure against CIS Benchmarks, prioritized critical vulnerabilities by risk and exploitability, and coordinated remediation with engineering teams across SaaS and cloud-native workloads.

Threat Intelligence and Proactive Threat Hunting: Collected and analyzed cyber threat intelligence from multiple sources, enriched indicators of compromise, performed proactive threat hunting, and produced actionable threat assessments shared with internal and external stakeholders.

Security Operations Automation Toolkit: Built Python, PowerShell, and Bash automation for IOC enrichment, alert triage, detection rule generation, log parsing, and SOAR workflow integration, reducing manual security operations overhead by 35%.

Compliance and Audit Support Program: Supported NIST CSF, ISO 27001, PCI DSS, and SOC 2 audit activities including evidence collection, policy documentation, control gap identification, and remediation coordination across enterprise client engagements.

EDUCATION

Master of Science, Computer Science, Algoma University

Bachelor of Engineering, Computer Systems, NED University of Engineering and Technology