REGAN GOMES

SOC Analyst | Cyber Security Professional

332-293-3618 | gomesregan37@gmail.com| New York, NY

CAREER SUMMARY

Cybersecurity professional offers over 10 years of experience in cybersecurity, including specialized roles as a SOC Analyst, IT Security Engineer, and Security Analyst. Industry expertise spans critical sectors such as global healthcare insurance, banking, and international IT managed services. Contributions include maintaining high SLA compliance for security alerts and reducing identity-related incidents by 11% through proactive monitoring and dashboard tuning. Proven track record in securing global cloud migrations and managing enterprise-wide vulnerability assessments to protect sensitive member and financial data. Technical proficiency encompasses real-time threat detection using Microsoft Sentinel and Splunk SIEM, alongside deep log analysis with KQL and SPL. Advanced skills in cloud security via Microsoft Defender and identity protection ensure robust defense against sophisticated credential-based attacks. Expertise in network traffic analysis using Wireshark and incident mapping to the MITRE ATT&CK framework allows for rapid root-cause identification. Exceptional documentation and communication skills facilitate clear executive reporting and seamless shift handovers within 24/7 security operations centers. Strong problem-solving abilities and a collaborative mindset enable effective coordination with cross-functional teams to contain and remediate emerging threats.

KEY SKILLSET

- **SIEM and Log Management:** Microsoft Sentinel, Splunk (SIEM), Azure Log Analytics, KQL (Kusto Query Language), SPL (basic), Log Analysis, Alert Investigation, Security Event Correlation, Dashboard Monitoring.
- **Cloud Security (Azure):** Microsoft Defender for Cloud, Azure Security Center, Azure AD Identity Protection, Conditional Access Monitoring, Cloud Security Monitoring.
- **Endpoint and Vulnerability Security:** Microsoft Defender for Endpoint, CrowdStrike Falcon (basic), Tenable.io, Nessus, Vulnerability Assessment, Endpoint Threat Detection.
- **Threat Intelligence and Incident Response:** VirusTotal, AlienVault OTX, IOC Analysis, Alert Triage, Incident Investigation, MITRE ATT&CK Mapping.
- **Network Security Monitoring:** Wireshark, TCPDump (basic), Network Traffic Analysis, Packet Inspection, DNS/HTTP Analysis, Suspicious Activity Detection.
- **Identity and Access Security:** Active Directory Monitoring, Authentication Logs Analysis, Privileged Access Monitoring, Account Compromise Detection.
- **Security Operations:** Security Monitoring, Incident Handling, Playbook Execution, Threat Hunting (basic), False Positive Analysis, SOC Processes.
- **Ticketing and Case Management:** ServiceNow, Jira (basic), Incident Documentation, Case Management, Escalation Tracking.
- **Systems and Platforms:** Windows Server, Linux Fundamentals, Microsoft Azure, VMware, Network Infrastructure Security.
- **Scripting and Automation:** PowerShell (basic), KQL Queries, Bash (basic), Security Automation Support.
- **Compliance and Frameworks:** MITRE ATT&CK, NIST Cybersecurity Framework (CSF), ISO 27001, PCI-DSS, HIPAA (awareness).
- **Reporting and Documentation:** Incident Reports, Investigation Notes, SOC Metrics, Executive Summaries, Security Documentation.

WORK EXPERIENCE

SOC Analyst

Aetna Inc. | Hartford, CT | Sep 2024 – Present

- Monitor daily security alerts in Splunk SIEM and Microsoft Sentinel, reviewing logs from Azure, on-prem Windows servers, and healthcare applications that process member and claims data at Aetna Inc.
- Validate triggered alerts by analyzing correlated events in Azure Log Analytics using KQL, checking for unusual authentication behavior, failed MFA attempts, and suspicious access to PHI-related systems.
- Examine identity-based risks in Azure AD Identity Protection, focusing on risky sign-ins, impossible travel events, and conditional access policy violations affecting internal users and remote staff.
- Investigate endpoint detections through Microsoft Defender for Endpoint and CrowdStrike Falcon (basic), reviewing process activity, registry changes, and file hashes to confirm malware or policy violations.

- Perform vulnerability review activities using Tenable.io and Nessus scan results, helping identify missing patches on Windows servers supporting provider portals and internal healthcare systems.
- Correlate firewall, DNS, and HTTP logs with endpoint alerts, and use Wireshark or TCPDump (basic) when necessary to validate suspicious outbound connections.
- Conduct IOC checks through VirusTotal and AlienVault OTX, comparing file hashes, domains, and IP addresses to determine whether alerts relate to known threat campaigns.
- Map confirmed attack behaviors to the MITRE ATT&CK framework, helping the team understand techniques such as credential access or privilege escalation within the healthcare environment.
- Follow SOC playbooks to contain validated incidents by disabling affected accounts, enforcing password resets, or isolating endpoints, while escalating complex cases to Tier 2 analysts.
- Document each investigation clearly in ServiceNow, capturing timelines, log evidence, and remediation steps, contributing to maintaining over 82% SLA compliance for medium and high-severity alerts.
- Support monitoring efforts aligned with HIPAA and NIST CSF requirements, ensuring that investigations involving member data are properly handled and documented.
- Assist in security monitoring during system changes tied to the CVS Health digital integration initiative, reviewing new Azure workloads and access controls for potential misconfigurations.
- Contribute to weekly SOC reporting by summarizing alert trends, risky user activity, and recurring phishing patterns, helping reduce repeat identity-related incidents by approximately 11% within one year.

IT Security Engineer

Wipro | Dhaka, BD | Nov 2017 – Jun 2023

- Evaluated system security requirements for the "Wipro Global Cloud Migration" project, ensuring that new Azure-based workloads adhered to the company's internal security baselines and NIST standards.
- Configured and deployed Nessus vulnerability scanners across distributed network segments to proactively identify unpatched systems and insecure configurations within the client environment.
- Monitored incoming security telemetry using Splunk and Azure Log Analytics, filtering through thousands of daily logs to detect anomalies such as brute-force attempts or unauthorized API calls.
- Triage security incidents within the ServiceNow ticketing system, ensuring that critical-priority events are categorized and escalated to the appropriate response team within strictly defined SLAs.
- Investigated suspicious login behavior and account lockouts by analyzing Active Directory authentication logs and verifying user access patterns against established group policies.
- Analyzed potential phishing threats and malicious attachments by extracting file hashes and performing domain reputation checks through VirusTotal and AlienVault OTX.
- Utilized Wireshark to capture and inspect network packets during connectivity troubleshooting, identifying suspicious DNS queries that indicated possible malware beaconing.
- Verified the status of endpoint protection agents in Microsoft Defender for Endpoint, confirming that all remote workstations had active real-time scanning and current signature updates.
- Developed basic PowerShell scripts to automate the collection of security logs from Windows servers, which increased data collection efficiency across legacy infrastructure.
- Mapped identified threat patterns to the MITRE ATT&CK Framework to assist senior engineers in creating more accurate detection rules for future attack scenarios.
- Drafted detailed technical documentation for resolved incidents, ensuring that the root cause and remediation steps were clearly recorded for future audit compliance and team training.

IT Security Analyst

Accenture | Dhaka, BD | May 2015 – Oct 2017

- Kept a close watch on live security event streams using Splunk and early Azure Log Analytics to spot any unauthorized access attempts across the global infrastructure.
- Managed the intake of security tickets within ServiceNow, making sure each incident was categorized correctly so that high-risk patient or financial data remained protected.
- Participated in "Project Identity-Secure," where you audited user permissions in Active Directory to clean up "permission creep" and ensure offshore teams had only the access they truly needed.
- Identified hidden weaknesses by running scheduled Nessus scans across corporate office subnets, flagging outdated Windows servers that missed critical security patches.

- Dug into the root cause of suspicious login failures by correlating VPN logs with authentication timestamps to distinguish between forgetful employees and potential brute-force attacks.
- Vetted suspicious attachments and URLs reported by users through the phishing mailbox, using VirusTotal and AlienVault OTX to confirm if they contained actual malicious payloads.
- Assisted during network troubleshooting by using Wireshark to capture packets, specifically looking for unusual DNS traffic that might suggest a malware infection was trying to "phone home."
- Teamed up with the infrastructure group to confirm that security patches were successfully deployed, checking the final status of endpoints to ensure no machine was left vulnerable.
- Took ownership of incident notes, writing up clear, step-by-step documentation of your findings so the next shift at Accenture could pick up exactly where you left off.
- Prepared daily status updates for the shift lead, summarizing the day's most interesting alerts and tracking how quickly the team was resolving incoming tickets.

IT Support Engineer

Standard Chartered | Dhaka, BD | Apr 2010 – Apr 2015

- Managed the end-to-end deployment and maintenance of banking workstations and peripherals across Dhaka branches, ensuring that Windows-based systems were correctly imaged with secure financial applications and that all retail hardware remained operational to prevent service disruptions for bank customers.
- Acted as the primary gatekeeper for identity and access by troubleshooting Active Directory account issues and folder permissions, while simultaneously leading the "Branch Hardening Initiative" to physically secure server racks and disable unauthorized USB ports on public-facing terminals to prevent data leakage.
- Resolved high-priority technical escalations involving Outlook, VPN connectivity, and network outages, often providing onsite support to ensure bank tellers and branch managers could access core banking systems without security-related delays.

IT Support Assistant

BJIT | Dhaka, BD | Jan 2007 – Mar 2010

- Assembled and prepared specialized developer workstations, which involved installing Windows XP/7 environments, configuring essential coding tools, and setting up local network printers to support the "Global Delivery Backbone" project, ensuring new engineers were ready to work from day one.
- Handled the daily cleanup and maintenance of office systems, manually running antivirus scans and applying security patches to protect the network from local worm infections, while also troubleshooting hardware issues to keep the software development lifecycle moving without interruption.
- Facilitated smooth internal operations by managing user account resets in Active Directory and helping staff with email configuration, while providing hands-on support for basic network cabling and switch port connectivity within the BJIT server room.

PROFESSIONAL TRAINING & CERTIFICATION

- **CompTIA Security+**
- **CEH – Certified Ethical Hacker**
- **CCNA – Cisco Certified Network Associate**
- **CompTIA A+**

ACADEMIC ACHIEVEMENTS

- **MSc in Computer Science & Engineering,** Stamford University Bangladesh (3.77 out of 4.00)
- **BSc in Computer Science & Engineering,** Stamford University Bangladesh (3.50 out of 4.00)