Mohammad B. Anwar

US Citizen - Greater Detroit Area, Michigan | Ba2512005@gmail.com

Cyber Security Architect – HITRUST

Highly experienced IT & Security Leader, Product Manager, and Software Development Lead with over 13 years of experience. Unique blend of hands-on technical expertise and robust leadership abilities. Proven track record of successfully navigating complex domains, including hardware and infrastructure, software, and web services. He can quickly adapt to new ideas and execute them with minimal supervision, consistently delivering outstanding results.

Skilled at fostering team collaboration, driving business growth, and optimizing processes across diverse environments. He is passionate about leading cutting-edge projects that leave a lasting impact on the organizations he serves.

- Excels at leading the strategic direction of large-scale security programs (short + long term)
- Defining and executing security roadmaps and projects, including budgets
- Defining and managing priorities and risks, achieving company goals, and exceeding customer expectations while delivering results on time and within budget.
- Working knowledge of regulatory standards and compliance frameworks (e.g. HITRUST, NIST Cybersecurity Framework, ISO27001, SOC2, HIPAA, GDPR).
- Experience with security risk management techniques and tactics. (MITRE)
- Experience working in a regulated environment: Healthcare HIPAA & HITRUST
- Collaborative leader and team member with a strong work ethic and unwavering job focus.

A strong communicator with excellent interpersonal, written, and verbal skills. He can engage and solicit input from all stakeholders to deliver clear solution proposals with efficient execution. He has profound knowledge of security best practices, automation, IT infrastructure, architecture, application development and support, networks, and computer operations to lead effectively.

Security Skills

- **Compliance:** HITRUST, HIPAA, SOC2, NIST SP800-53, ISO 27001, CSF, GDPR, Zero-Trust, Insider Threat
- **Automation:** Security Orchestration and Automated Response (SOAR certified), XSOAR, Swimlane SOAR, Splunk SOAR, IBM Resilient, FireEye SOAR, SIEM, Splunk, Securonix
- **EDR/XDR:** SentinelOne, Bitdefender, Microsoft Defender, Cososys, Darktrace
- **Data Protection**: CyberArk Vault, PIMSU, Encryption, Digital Guardian (DLP), Google workspace, SSO, proxies
- **DAST/SAST:** Halo Security (TrustedSite), SonarQube, Qualys, Fairwinds (container security),
- **Email & SaaS:** Darktrace, created custom NLP spam filter, Logicworks, KnowBe4
- **Vulnerability Scanning:** AlertLogic, SecurityHub, nmap Guard duty, SecurityHub, SSM
- **Cloud & DevOps**: AWS, Azure, Kubernetes hardening, Cloudformation, Ansible, Git, Iaas, Caas, Paas, Saas
- **Programming**: Java, JavaScript (ReactJS and NodeJS), Python, C/C++, .NET C#, Go
- **Web Technologies:** HTML, CSS, JavaScript (React, Node.js, Angular)
- **Virtualization:** VMware, VirtualBox, HyperVisor
- **Containerization:** Docker, Kubernetes, EKS

Mohammad B. Anwar

US Citizen - Greater Detroit Area, Michigan | Ba2512005@gmail.com

Accomplishments

- **Grand prize winner** for designing and leading a team of 7 for the best solution in Security Triage Automation (GE NextTech 2017)
- **Certified in SOAR** Security Orchestration and Automated Response (Swimlane 2021)
- **Created AI** to automatically detect spam in emails
- **Created official instructional videos** for SOAR tooling (FireEye)

Certifications

- SOAR Administrator (Swimlane 2021)
- CISM (in progress)

Work Experience

Cyber Security Leadership (8/18 – 6/23) ~6+ Years

Security Architect - Akasa (Healthcare AI automation)

- Lead a team of technical staff for company-wide security initiatives, championing best practices to Influence the development and improvement of corporate policies supporting program objectives.
- Engage regularly with CTO and executives to report on security health of company
- Direct compliance and infrastructure team to adhere to and apply security best practices
- Conduct audits and risk assessments through environment scans and remediate vulnerabilities through configuration changes and creating standards for secure application development
- Lead Implementation of container (Kubernetes) hardening within HIPAA, NIST, SOC2, and ISO security policies through collaborating with engineering leadership and CTO.
- Manage business relations with vendors for security reviews and remediation coordination.
- Create and manage security budget, engage vendors for cost savings, and optimizing financial efficacy
- Defined evaluation process and policies for security vendors to align with compliance requirements; evaluating security companies and vendors to fit within budget and scope.
- Design and implement secure software processes to mitigate risk using encryption, IAM, policies using principal of least privilege and zero trust.
- Develop incident response plans and facilitate tabletop exercises for training response teams.
- Reduce vulnerabilities through implementation of patch and update management strategy
- Automated tedious tasks (updates, key rotations, onboarding/offboarding, vendor reviews, infrastructure optimization & notifications) streamlining automatic remediation of issues, allowing for employees to focus on more impactful initiatives.
- Partner with compliance team to promote security awareness and educate employees
- Instrumental in leading company for obtaining and maintaining HITRUST certification.
- Implemented upgrade of EDR and asset management tools to better secure infrastructure

Impact: Secure the company's infrastructure, establish trust with leadership and enable company to be secure, allowing better focus on business objectives, maintaining compliance to establish and maintain trust with customers.

Tools Used: Python, Kubernetes, AWS (guard duty, securityhub, SSM, cloudtrail, cloudwatch, cloudformation), HITRUST, Darktrace, AlertLogic, Halo, SentinelOne, bitdefender, knowBe4, Darktrace

Mohammad B. Anwar

US Citizen - Greater Detroit Area, Michigan | Ba2512005@gmail.com

Senior Security Architect – Optiv 7/20-3/21

- **Head of Architecture team** to Design and implement automation software solutions for clients, ensuring high-quality service and innovative problem-solving.
- Develop new methods to deploy ECE cloud at scale using Ansible and AWS
- Advisor to the Automation Solutions Development Team for auditing playbooks and optimizations
- Mentor and guide other consultants to foster ideation and innovation.

Impact: Secure client's infrastructure while providing them with first class services.
Tools Used: IBM Resilient, XSOAR, Swimlane, ECE, AWS, Phantom SOAR (Splunk)

Senior Security Automation Architect – Longbow 12/19 - 3/20

- Design and implement security software automation solutions for customers and support business development in product creation, service line expansion, recruiting, and training.
- Advise on architect and design of security automation playbooks.
- Define use cases to drive the security engineering team to develop detection methods and behavioral models, supporting the discovery of accidental or malicious activities undertaken or soon to be undertaken by insiders that would violate policies or cause harm

Impact: Provide cyber automation solutions, consulting, and managed services to improve cyber effectiveness, efficiency, and security insights, reducing the threat of damaging breaches
Tools used: XSOAR, Microsoft Project

Security Architect – FireEye 1/19 – 12/19

- **Lead a team of Security Engineers** to Develop and refine security automation content such as workflows, playbooks, plugins, and processes to improve customer detection, response, and investigation.
- **Produced instructional videos** within a professional studio environment, guiding users on product utilization.
- **Collaborate with high-profile customers** to review SOC and IR processes, recommend automation techniques, and define plugin development requirements.

Tools Used: Objective Python, PyCharm, FireEye SOAR, Helix*Tools used: Objective Python, PyCharm, FireEye SOAR, Helix*

People Leadership (01/23-06/24)

Vice President – Al Maghrib (Michigan)

- Lead multiple teams of 20+
- Facilitate communication with leadership and stakeholders to define roadmap and strategy
- Delegate tasks to members for accomplishing strategic outcomes of running successful events with over 2500+ people, coordinating with stakeholders, staff, and team to ensure smooth operations
- Oversee member involvement and drive engagement, heading advertising and marketing division
- Mentor, guide, and train youth and facilitate accomplishing learning objectives
- Build relations with partners and vendors, expanding network and enabling opportunities
- Organize speaker events and workshops with over 2500+ participants
- VIP hospitality management and coordination

Lead Instructor – BetaCoders

- Teaching and mentoring high schoolers for learning python programming and cyber security
- Designing projects to apply learning to real world problems

Mohammad B. Anwar

US Citizen - Greater Detroit Area, Michigan | Ba2512005@gmail.com

General Electric (01/14 – 08/18) ~ 5 years
Senior Technical Product Manager - GE 8/17-8/18

Leading 20- member DevOps team for the Managing of roadmap, resources, infrastructure, and lifecycle and outcomes for ***BrilliantYOU*** which provides intuitive training and learning courses for 300,000+ employees at GE.

- Oversee project for intelligent recommendations for courses to employees based on historical data and user analytics.
- Managing release of features and improvements to improve overall user experience and engagement.
- Manage and support AWS infrastructure operations to get system stability handle up to 400 concurrent user loads.

Digital Technology Leadership Program - GE 07/15- 08/17
NexTech security triage automation (Grand prize-winning solution)

Won Grand prize (1st place) for a company-wide challenge sponsored the CEO of GE to automate the triage process for handling security threats in GE.
Lead a team to design, architect and implement on an automation platform called Phantom and paring it with machine learning, classifying all incoming emails to GE networks as phish, ham, or spam and categorize based on certainty levels. We are also leveraging a feedback loop where we can have user confirmation for emails that our algorithm is uncertain about.
Tools used: Python Falcon API framework, AWS, Phantom automation platform.

Solution Architect - GETruck (Uber for the factory floor)
Designed and built a solution to optimize the factory floor move operations in partnership with Operation Management Leadership Program. This project addresses the problem of legacy move operations being completed via paper tracking by orchestrating the entire shop floor forklift operations with an uber-like service that tracks move requests through an intuitive application.
Impact: Improve move operations efficiency by 50%. Enable data analytics to be performed on the shop floor move process to further optimize efficiency.
Tools used: LAMP stack (Linux, apache, mysql, php), Javascript, html)

IT Risk – Insider Threat Architect– Glen Allen, VA
Managed the ingestion of audit data from critical business applications into Splunk to allow correlation of data egress by insider threats. Rolled out policy to alert users of exfil they were performing on company assets. Worked with insider threat team to take over security services for divested company.

Mohammad B. Anwar

US Citizen - Greater Detroit Area, Michigan | Ba2512005@gmail.com

- Created a policy in DG to alert users on network uploads to non-ge managed sites, informing users of their actions and reducing the number of users offloading data.
- Led a POC for ThetaRay Anomaly detection in Predix to evaluate if it can be a viable replacement for our Securonix environment to save 300k/ yr

ERP Platform Architect – Cincinnati, OH

Designed and implemented a system which provides visibility into ERP integrations that were failing and slowing down business processes. This project allows us to automate the fixes for integrations that go out of sync and error out. This has greatly reduced the amount of time spent by ops on troubleshooting and diagnosing, as well as the potential to reduce their workload for repairing these issues as well. Ultimately this will speed up root cause analysis on the issues in this entire ecosystem leading to lesser downtime, lesser cost impact, and happier customers.

- Created an ETL tool to dynamically transfer data & DDL from ERP systems to AWS data lake & correlation system to track integration faults between ERP, MES, and Kronos
- Enabled Automation of Integration fixes using correlation tool to automatically fix integration errors in ERP ecosystem.

Tools used: AWS, Java, mysql, mssql, oracle db

Kronos Cloud Architect – Schenectady, NY

Led a POC for next generation of Kronos to integrate with current environment and reduce java dependencies for a more stable platform. The impact of this project will be a reduced cycle time and cost when upgrading the current environment to v8.

- Proposed and implemented a load balancer solution to improve Kronos clock infrastructure to reduce downtime and increase reliability, greatly reducing impact on employee paychecks.
- Led a POC for Kronos in AWS to analyze cloud readiness of Kronos in order to reduce costs and improve performance.

IT Team Lead – General Electric 1/14 – 5/15

Brilliant Factory IT - Standards Specialist

Defined standards for machine communication and barcoding that will be used across GE's new brilliant factories. This ensures that all the factories at GE will be using the same method for transferring data and identifying parts.

Privileged Identity Management – Penetration Testing

Ensured OPM/SUPM product from CyberArk is properly configured and meets company security policy. Performed a case-by-case analysis of different configurations for this product in our current environment and reported what changes need to be made in order to meet company requirements. Exploit/penetration tested this product to ensure it is not able to be bypassed or used as an attack point for malicious users. The vulnerabilities I have found have been reported to CyberArk for remediation.

Tools Used: CyberArk Pimsu, Vault, Linux

Privileged Identity Management – Solutions Development

Mohammad B. Anwar

US Citizen - Greater Detroit Area, Michigan | Ba2512005@gmail.com

Designed an improved process to provide access to shared accounts and administrative tools used to provision and remediate highly privileged accounts through the use of a web service. Worked closely with another intern to deliver an enterprise class full stack web API and user interface backed with a queuing solution to remediate the single threaded nature of the underlying application.
Tools Used: C# .NET 4.5, RabbitMQ, CGI, CyberArk

Corporate Global Operations IT – Infrastructure Upgrade
Managed project to upgrade server infrastructure containing 22 servers around the world from Windows Server 2003 to Windows Server 2012 ensuring application compatibility, security compliance, and 100% application up-time throughout the transition. Improved server efficiency through implementing new technologies to reduce network load.
Tools Used: Windows Server 2003, Windows Server 2012, ITIL, ServiceNow

IT Support Manager - Wayne State University 2/12-1/14
Manage IT operation team that supports 150 users throughout the center by providing a broad range of IT support services such as equipment installation and configuration, technical support, problem resolution, and training related to desktop computers, related devices and applications used within the center under Windows and Mac environments.
Maintain server infrastructure while managing users, printers, computer, and file server through active directory.

- Install, Maintain, and Manage Windows and Mac OS under standalone and domain servers.
- Diagnosis, repair, setup and maintenance of desktop, laptops, tablets, printers, copiers, scanners, projectors, and other office technologies. Repair/Maintain/Setup of networked LaserJet Printers and scanners.
- Devised new method of asset tracking through object-oriented design.

Skills developed:

- Database and server administration using active directory and MMC.
- Knowledge of command line diagnostics and advanced windows XP/vista/7 administrative tools
- Office technology experience including setup, diagnosis, repair, and maintenance.