Nick Stach

090-1700-4453
nick.stach.it@gmail.com
https://github.com/tristach/tristach
https://www.linkedin.com/in/nick-stach

SUMMARY

Cybersecurity-focused professional with hands-on experience building and securing cloud environments in Microsoft Azure. Designed and deployed a honeynet-based SOC environment, developing monitoring pipelines using Microsoft Sentinel, Sysmon, and Logic Apps to analyze real-world malicious traffic in a controlled setting. Skilled in log analysis, threat detection, and automation using KQL, Python, and PowerShell. Background in IT support and cloud systems, with a strong focus on practical security implementation.

CLOUD SECRITY & SOC EXPERIENCE (Azure)

- Built a cloud-based SOC environment in Microsoft Azure using Windows and Linux virtual machines.
- Designed and deployed a honeynet to capture and analyze real-world malicious traffic.
- Ingested endpoint telemetry using Sysmon and Azure Monitor Agent (AMA) with Data Collection Rules (DCR) into Log Analytics Workspace.
- Developed and deployed KQL queries to detect brute-force activity, malware, suspicious process behavior, and anomalous network and authentication activity across Azure environments.
- Created Microsoft Sentinel analytics rules and automated alerting workflows using Logic Apps.
- Simulated and analyzed attacks including RDP brute force and malware (EICAR).
- Conducted vulnerability scans using Tenable Nessus (credentialed and non-credentialed).
- Applied NSG rules and access restrictions to reduce exposed attack surface.
- Measured and reduced malicious activity by 98 – 100 percent in a controlled environment after implementing security controls.

EXPERIENCE

Company: Rainbow EIKAWA 2019 November – Present

Title: Co-Owner & IT / Security Lead

- Managed IT systems and web infrastructure for a small education business.
- Used Microsoft Azure and EntraID to configure role assignments and security group management.
- Implemented basic security controls including NSGs, firewall rules, and access restrictions.
- Used Microsoft Sentinel to monitor logs and explore threat detection concepts.
- Developed and maintained web tools using JavaScript and GitHub Pages.
- Implemented secure Azure configurations using NSGs, Private Link, and Microsoft Defender for Cloud aligned with NIST frameworks.
- Developed KQL queries to support Log Analytics workspace and Microsoft Sentinel resulting in four SIEM dashboards and workbooks.

Company: Log(N) Pacific 2023 June – Present
Title: IT/Cybersecurity Support Engineer

- Troubleshot and support Microsoft Azure services including Microsoft Sentinel (SIEM), Virtual Machines, Azure Monitor and Azure Active Directory.
- Provisioned/troubleshot Azure Virtual machines (VMs), VNets and NSGs (firewalls).
- Provided support for the setup, configuration/troubleshooting of osTicket ticketing system/platform.
- Created and managed file-share permissions on Windows Server to maintain data/security integrity.
- Diagnosed and resolved basic network issues minimizing downtime and improving network reliability.
- Demonstrated understanding of DNS fundamentals, effectively troubleshooting related issues while optimizing configurations.

Company: Berlitz Japan 2014 February – 2019 November
Title: Manager/IT Support.

- Provided IT support, onboarding, and training across cloud-based systems.
- Managed user permissions and supported internal systems in Azure environments.
- Assisted with security practices including MFA and access control.

Company: Symbology Inc. 1997 January – 2000 June
Title: Label and EDI Data Specialist

- Guided end-users on fraud prevention and compliance enforcement in Electronic Data Interchange.
- Oversaw EDI standards and compliance monitoring saving clients thousands in errors/fines.
- Monitored and implemented UCC (Uniform Code Council) standards and implementation rules.
- Used electronic verification systems to help EDI users avoid fraud and maintain security compliance.
- Implemented and uphold best practices for data security infrastructure to help major retailers such as Pepsi, WD-40 and Bacardi maintain InfoSec/EDI security.

CYBERSECURITY PORTFOLIO

Azure SOC & Honeynet Environment.
GitHub: github.com/tristach/Azure-Cloud-SOC.

- Built and validated a cloud-based SOC environment using Azure and Microsoft Sentinel.
- Simulated real-world attacks (RDP brute force, malware, SQL login attempts) to test detection workflows.

Cloud-Cover (Python Automation Tool).
GitHub: github.com/tristach/rakuten-ML-cloud-cover.

- Developed Python-based tool to analyze logs and identify suspicious IP activity.
- Automated detection workflows supporting SOC-style analysis.

CERTIFICATIONS

CompTIA Security+ (expected December 2026).
Google Cybersecurity Certification (2024).
Cybersecurity Masterclass, Leveld Careers (2023).
FEMA ICS-100 (2023).

SKILLS AND TECHNOLOGIES

Microsoft Office Suite, Microsoft Teams, Ticketing Systems, Microsoft Azure, Network Security Groups (NSGs), Firewalls, ACLs (Access Control Lists), Virtual Machines (Windows/Linux), Virtual Networks, Active Directory (Azure AD / Entra ID), File Permissions, Windows 10/11, SIEM (Microsoft Sentinel), Log Analytics Workspace, Azure Monitor, Azure Monitor Agent (AMA), Data Collection Rules (DCR), **Sysmon (endpoint telemetry)**, SQL, KQL, Python, PowerShell, Logic Apps, TCP/IP Networking, Cloud Security Posture Management (CSPM), Threat Detection, Incident Response, Vulnerability Assessment and Management, **Nessus**, Security Operations (SOC) Practices, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Wireshark, Git, GitHub, VS Code, Linux Command Line.