ENDI SPASSE

Cybersecurity Engineer | Cloud Security | Information Systems Security
Yonkers, NY | (929) 899-3235 | endi.spasse.ca@gmail.com | LinkedIn | Projects

PROFESSIONAL SUMMARY

Results-driven and solution-focused Cyber Security Engineer with progressive experience protecting complex enterprise environments through cloud security, information assurance, security engineering, threat detection, vulnerability management, incident response, and risk mitigation. Ability to secure multi-cloud infrastructure by executing identity and access management, authentication safeguards, conditional access policies, multifactor authentication, endpoint protection, and preventive security controls. Skilled in analyzing security events, audit logs, threat indicators, malicious activity, and system vulnerabilities.

CORE COMPETENCIES

Product Security | Threat Detection | Incident Response | Cloud Architecture | Vulnerability Management | Access Controls | Network Defense | Identity Governance | Endpoint Protection | Security Automation | Stakeholder Engagement | Multifactor Authentication | Risk Assessment & Mitigation | Cross-functional Collaboration | Process Improvement Initiatives | Firewall Administration | Network Security | Firewall Configuration | Policy Management | Infrastructure Security

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer, Network Doctor – Englewood, NJ **10/2025 – Present**

- **Investigate and resolve** approximately 35 security alerts and incidents daily across an MSP portfolio of 184 organizations and 12,000 endpoints, regarding phishing, endpoint detection, identity, malware, phishing, and account-compromise detections through containment, remediation, and escalation.
- **Secure identity and access** across approximately 80 Microsoft 365 tenants using Entra ID, Conditional Access, Defender, Intune, Exchange Online, and Purview, mitigating risky sign-ins, enforcing MFA, and resolving access-control conflicts.
- **Analyze and remediate EDR/MDR** threats across 100+ client environments using SentinelOne, Microsoft Defender, Huntress, and Blackpoint, distinguishing malicious activity from false positives and analyze and take additional action to high-priority threats within 5–10 minutes.
- **Support client SOC 2 readiness and audit preparation** through security-control remediation, documentation, evidence collection, and coordination across security, engineering, Helpdesk, and client stakeholders
- **Investigate and neutralize** approximately 10 phishing incidents daily using Mimecast and MX ToolBox, analyzing message headers, URLs, attachments, authentication results, message traces, and sandbox findings to identify credential theft and malicious payloads. Along with using Phin for monitoring and enrolling users for phin simulation campaigns.
- **Contained a phishing-driven account and endpoint compromise** involving malicious PowerShell-delivered RMM software by isolating the affected system, disabling the account, revoking sessions, resetting credentials, auditing MFA and mailbox activity, blocking malicious infrastructure, and coordinating secure device reimaging.
- **Accelerated ransomware recovery** for a 300-user environment by securing approximately 100 endpoints, reimaging compromised systems, restoring backups, reconnecting Active Directory devices, and implementing post-incident security hardening before production restoration.
- **Implement and improve security** procedures across client environments, including Conditional Access, travel-access controls, EDR exclusions, malicious hash and URL blocking, account containment, endpoint isolation, and post-incident remediation while coordinating with clients, engineers, Helpdesk, and MDR/SOC teams.

Solutions Architect Engineer Trainee | ESxTech – New York, NY **01/2023 – Present**

- **Supported 6+ AWS infrastructure deployments**, translating client and technical requirements into secure cloud configurations across IAM, compute, storage, networking, monitoring, and access controls.
- **Strengthened AWS security posture** using IAM, Security Hub, GuardDuty, CloudTrail, CloudWatch, and vulnerability-management controls to identify security risks, monitor suspicious activity, and support remediation.
- **Implemented and maintained infrastructure security controls** including IAM permissions, patch management, antivirus protection, firmware upgrades, backup and disaster-recovery procedures, improving system resilience and continuity.
- **Collaborated with technical stakeholders to assess infrastructure requirements**, troubleshoot security and operational issues, and implement cloud solutions aligned with business and security requirements.

Experience Manager | LIVunLtd – New York, NY 10/2022 – 10/2025

- **Collaborated with department heads** to address technology and staffing requirements, develop executive presentations, and resolve escalations, improving cross-functional coordination.
- **Directed daily facility operations**, spanning payroll, human resources, OSHA compliance, inventory control, and audits, strengthening organizational efficiency and regulatory adherence.
- **Oversaw operations across six luxury amenity** facilities throughout Manhattan, resolving violations and enforcing stringent safety protocols to strengthen compliance, mitigate operational risks, and maintain premium service standards.

Graduate Director | Baruch ISACA Cybersecurity Club – New York, NY **01/2023 – 12/2024**

- **Steered Agile security practices across teams**, elevating secure development processes and collaborative environments.
- **Led monthly cybersecurity workshops** on vulnerability management, access control, best practices, and risk mitigation plans.
- **Increased student engagement by 60%** through targeted training and networking events focused on penetration testing, vulnerability assessment, and defensive countermeasures.

MAJOR PROJECTS

Centralized CloudTrail Monitoring and Analysis via Splunk [AWS, Splunk, Let's Encrypt, Certbot]

- **Engineered centralized AWS security monitoring** using CloudTrail, S3, SQS, and Splunk, accelerating real-time threat detection, strengthening IAM and TLS controls, and enhancing visibility into access changes, storage events, and anomalies.

Security Incident Response [AWS: GuardDuty, EventBridge, Lambda, SNS, CloudWatch, IAM Roles]

- **Developed event-driven AWS incident response**, integrating GuardDuty, EventBridge, Python Lambda, SNS, and CloudWatch to detect threats, isolate compromised EC2 instances, automate notifications, and reduce false-positive remediation through cross-account IAM controls.

Splunk-Driven Threat Feed Correlation Engine [AWS, Splunk, AlienVault OTX]

- **Engineered a Splunk threat-intelligence engine**, integrating Python, AlienVault OTX, HEC, and AWS VPC Flow Logs, automating indicator normalization, malicious IP detection, actionable alerts, and security dashboards.

Automated Monitoring & Remediation Framework [Azure, Datadog, Terraform, VSCode]

- **Architected automated Azure monitoring and self-healing** using Datadog, Functions, Python, and Log Analytics to detect CPU breaches, restart impacted Linux/Windows VMs, capture remediation events, and enable secure end-to-end recovery through service-principal authentication, protected webhooks, and RBAC controls.

WAF Enabled Multi-Layer Web App Firewall [AWS, Terraform, curl and bash]

- **Orchestrated and validated layered AWS security** using WAF, CloudFront, ALB, S3, and Terraform, mitigating SQLi, XSS, malicious IPs, geo-threats, and rate abuse through attack simulations, strengthened controls, audit trails, and threat visibility.

EDUCATIONAL BACKGROUND & PROFESSIONAL DEVELOPMENT

MS in Information Systems Cybersecurity | Baruch College, Zicklin School of Business – New York, NY
BS in Information Systems and Business Management | American University in Bulgaria – Blagoevgrad, Bulgaria
Certifications:

AWS Security, (In Progress) | AZ 104 Azure Administrator, (In Progress) | CompTIA Sec+ (Pending), 10/2026

ISCC, 07/2026 | AWS Solutions Architect, 04/2025 | AWS Certified Cloud Practitioner, 02/2024 | Qualys Vulnerability Management, 10/ 2023

APPRENTICE WORK HISTORY

Help Desk (Internship) | Permanent Mission of Albania to United Nations – New York, NY **01/ 2022 – 06/2022**

- **Reduced ticket resolution time by 40%** through standardized troubleshooting, log analysis, and remote support procedures.

Desktop Security Intern | Albanian Embassy in Hungary – Budapest, HU **06/2016 – 05/2017**

- **Deployed and configured operating systems**, applications, and network equipment, improving infrastructure reliability.