Joshua Lapitan

jawlapitan@gmail.com | LinkedIn | Website

CERTIFICATIONS

CompTIA Security+ (Plus)	*January 2024*
CompTIA CySA+ (Plus)	*January 2025*
ISC2 Certified in Cybersecurity (CC)	*November 2022*
Microsoft Certified: Azure Fundamentals (AZ-900)	*October 2025*
CISSP	*In Progress*

TECHNICAL SKILLS

Detection & Response: Varonis Data Security Platform · insider-threat detection · data-exfiltration prevention · incident triage & escalation · KRI / insight tuning · runbook & playbook development

SIEM & Query Languages: Microsoft Sentinel · Splunk · KQL · SPL

Identity & Infrastructure: Active Directory · Exchange Online · domain controllers · file servers · DNS

Cloud: Microsoft Azure · Microsoft 365

Scripting & Tooling: Python · PowerShell · AI-assisted development (builds custom security tooling)

RELEVANT EXPERIENCE

Varonis Systems, Inc. — **Raleigh, NC / Remote**

MDDR (Managed Data Detection & Response) Analyst II — *May 2024 – Present*

Promoted from Analyst I, July 2025

- Triage and investigate 70 - 80 security alerts and investigations daily across hundreds of enterprise client environments using the Varonis Data Security Platform, specializing in insider-risk detection, data-exfiltration prevention, and anomalous-activity analysis.
- Validate 5+ critical incidents per day, escalating confirmed threats including early-stage account compromises and cases warranting forensic investigation for containment and remediation alongside client-side security stakeholders.
- Configure and refine analyst-facing insights and Key Risk Indicators (KRIs), tuning login and location anomaly detections and correlation logic e.g., flagging combinations such as suspicious role names paired with VPN activity to surface likely threat-actor or penetration-test behavior.
- Identify and respond to real-world threats surfaced through the platform, including phishing-driven account compromises, email-based data-exfiltration attempts, and brute-force attacks.
- Build end-to-end user and system behavior timelines by correlating telemetry across Active Directory, Exchange Online, domain controllers, file servers, and DNS to drive accurate, evidence-based investigations.
- Surface detection-logic and data-fidelity gaps to the engineering team, including a password-reset alert that misattributed the acting account, driving fixes that improved alert accuracy and analyst trust in the platform.

Ernst & Young (EY) — **Philadelphia, PA / Remote**

Cybersecurity Consultant, Staff — *September 2022 – January 2024*

- Translated 30+ complex analytic rules from SPL to KQL during a SIEM platform migration from Splunk to Microsoft Sentinel, supporting integration of 10+ distinct log sources with seamless data ingestion and operational continuity.
- Authored foundational design and requirements documentation for a large-scale Identity & Access Management (IAM) and Identity Governance & Administration (IGA) solution, serving as the blueprint for development teams and end-users and aligning the solution with business and technical objectives.
- Authored a detailed implementation and configuration guide for deploying a Multi-Factor Authentication (MFA) solution using Okta FastPass and Windows Hello for Business, enabling a smooth rollout and strengthening identity security against unauthorized access.
- Authored technical responses for four major client proposals, contributing to EY's business development and helping secure new cybersecurity engagements.

- Created and disseminated internal documentation and architectural blueprints that standardized best practices and became go-to references for consultants across the Cyber practice.

Penn State IT University Park, PA
Service Desk Consultant / Lab Consultant *August 2019 – May 2022*

- Provided 24x7 phone, email, and remote technical support to students, faculty, and staff, troubleshooting account lockouts, password resets, network connectivity, software updates, and printing/PC issues.
- Created and updated ServiceNow incidents to ensure proper documentation and categorization, escalating unresolved issues to voice operations or Tier 2 support.
- Delivered on-site support across campus computer labs and remote assistance via LabChat.

EDUCATION

Pennsylvania State University University Park, PA
B.S. in Cybersecurity, Minor in Information Sciences & Technology *May 2022*
GPA: 3.45 / 4.00 | Major GPA: 3.67 | Dean's List: Fall 2019, Spring 2020, Summer 2020, Spring 2021

LEADERSHIP & VOLUNTEERING

Purposeful Unconditional Service To Others (PUSO) Foundation **Remote / Multiple Locations**
College Outreach Associate / Director of Fundraising *May 2021 – Present*
501(c)(3) non-profit supporting impoverished communities, schools, and relief efforts worldwide.

- Provide fundraising coaching and mentorship to 100+ school organizations across the East Coast and Midwest; collectively raised over $72,000 during the 2022–2023 school year.
- Manage Salesforce database operations, maintaining accurate records and running reports for the leadership team.
- Coordinate with college outreach interns and directors to promote the PUSO brand, elevate awareness, and collaborate on organizational website development.