Jonathan Lunger

Bloomsburg, PA | (570) 317-7624 | jonathanlungerpro@gmail.com
linkedin.com/in/jonathan-lunger-91820527a | github.com/jonathanlunger

EDUCATION & CERTIFICATIONS

B.S. Cybersecurity and Digital Forensics | Commonwealth University of Pennsylvania - Bloomsburg | May 2026
Minor: Arabic Studies | National Security Agency-designated Center of Academic Excellence curriculum
CompTIA Security+ (SY0-701) | Earned June 2026 | Splunk SOC Essentials and Search Processing Language fundamentals

PROFESSIONAL EXPERIENCE

IT Technician | WellSpan Health | Nov 2024 - Nov 2025

- Completed foundational Splunk training and collaborated with the Security Operations Center for approximately 12 months, applying index selection, time filtering, graphing, and timelines while triaging 5-6 alerts per shift.
- Scoped phishing incidents, retrieved endpoint logs, mapped IPs to workstations, and analyzed headers and threat intelligence with VirusTotal and AbuseIPDB; escalated suspicious domains for blocking and contacted users to validate failed logins and coordinate password resets.
- Used Microsoft Endpoint Configuration Manager (MECM) and manual Group Policy updates to deploy and verify security patches across 300+ Windows endpoints, bringing outdated systems current and supporting HIPAA-aligned configurations.
- Completed 75-100 endpoint deployments per week against a target of 50, exceeding the planned pace by 50%-100% while achieving 100% BitLocker validation, asset tracking, and permanent metal labeling across 1,000+ computers at three hospital campuses.
- Responded to a missed BIOS configuration affecting all 130 computers in an emergency-room deployment; prepared and swapped in approximately 100 replacement workstations while correctly imaging the remaining systems, bringing the ER online within hours that same day.
- Installed and tested approximately 100 badge-scanner setups, enabling secure badge-based access to shared healthcare workstations and reducing delays associated with manual sign-ins.

Technology Lead | Bloomsburg University | Jun 2018 - Dec 2022

- Updated and tested web-filtering rules to block 100+ unauthorized streaming and potentially malicious domains, verifying policy enforcement and reducing workstation exposure to unsafe web content.
- Personally applied Group Policy updates across 500+ workstations and laptops, using command-line verification to confirm current Windows builds and applied security configurations.
- Resolved approximately 10-20 Active Directory password resets and account lockouts per week, verifying each request directly with the student or employee before restoring access and reducing full-time IT staff's weekly account-support workload by an estimated 30%-40%.
- Documented and escalated approximately five complex ServiceNow incidents per week involving account access, network outages, and unavailable network drives, recording symptoms, troubleshooting actions, and setup details to give full-time administrators a complete investigation and handoff history.
- Reset storage and ghosted approved Linux or preconfigured system images onto approximately 650 university computers, removing prior user data and preparing devices for redeployment or resale, including 300+ systems for Trash to Treasure.
- Maintained technology availability during a major building outage by deploying approximately 10 mobile workstation carts with isolated wireless connections, backup hotspots, and uninterruptible power supplies, keeping scheduled events operational.

CYBERSECURITY PROJECTS

Wazuh SOC Home Lab | Personal Project | 2026

- Developed custom rule 100100 by chaining to Wazuh rule 4101, producing six level-7 alerts from a controlled Nmap scan and mapping the detection to MITRE ATT&CK T1046 Network Service Discovery.
- Enabled Windows Defender Firewall dropped-packet logging, configured the Wazuh agent to ingest pfirewall.log, and used wazuh-logtest and wazuh-analysisd to diagnose parsing and rule errors.
- Built an isolated three-VM VMware lab with Wazuh, Windows 11/Sysmon, and Kali Linux, establishing an end-to-end telemetry path from controlled attacker activity to indexed dashboard alerts.

Phishing and Harassment Email Investigation | University Project | 2025

- Correlated a Gmail session and harassment POST less than two minutes apart using matching IP, MAC address, and user-agent data, producing a formal forensic timeline that attributed the activity while documenting evidentiary limitations.
- Filtered a packet capture in Wireshark to isolate 618 mail-related frames, then followed HTTP streams and analyzed form submissions, email headers, session cookies, and internal IP/MAC mappings to identify the source device.
- Matched identical user-agent strings across the Gmail session and harassment POST and analyzed the anonymous-email service's rewritten From header, explaining how sender manipulation affected SPF, DKIM, and DMARC analysis.

TECHNICAL SKILLS

SIEM & Detection: Splunk (SPL), Wazuh, alert triage, log correlation, dashboards, Sysmon, TheHive, Cortex, VirusTotal, AbuseIPDB
Systems & Networking: Windows, Linux, Active Directory, Group Policy, MECM, VMware, ServiceNow, BitLocker, TCP/IP, DNS, Wireshark, Nmap
Forensics & Security: FTK, Volatility, memory and file-system analysis, timeline reconstruction, chain of custody, IAM, RBAC, MITRE ATT&CK, NIST incident response, Python, PowerShell, Bash