

Dominique Long

Email: hello@dominiquelong.tech | Website: Dominiquelong.tech

Work Experience

IT Support Intern — *Dassault Systèmes* | Waltham, MA | February 2026 – Present

- Provided Tier 1 IT support in an enterprise environment, troubleshooting hardware, software, account access, and endpoint issues while meeting service-level expectations.
- Managed user accounts, permissions, access requests, and login-related issues through Active Directory and other enterprise systems.
- Supported new-hire onboarding by configuring laptops, setting up applications, provisioning access, and guiding employees through initial device setup.
- Documented incidents, troubleshooting steps, resolutions, and escalation details to improve consistency and internal knowledge sharing.
- Collaborated with IT team members to resolve technical issues while following company policies, security requirements, and escalation procedures.
- Developed a custom HTML-based walk-up support portal to improve user intake, request tracking, and in-person support workflows.
- Created interactive onboarding tutorials that helped employees understand device setup, enterprise applications, and common IT processes.

Telemetry Technician ICU — **Hartford HealthCare** | Meriden, CT | November 2017 – January 2025

- Responded to real-time alerts and escalated critical findings to nursing and clinical staff according to established protocols.
- Documented observations, interventions, and escalations accurately in compliance-driven systems.
- Worked in fast-paced, high-pressure environments requiring attention to detail and timely decision-making.
- Collaborated with multidisciplinary teams while adhering to strict healthcare policies and procedures.

Patient Care Technician — Abbott Terrace | Waterbury, CT | December 2013- October 2017

- Monitored resident activity and reported unusual conditions or incidents to supervisors following established procedures.
- Maintained accurate documentation and communicated effectively with staff in a fast-paced, compliance-driven environment.

Projects

Microsoft Sentinel & Azure

- Built an end-to-end SOC monitoring environment in Azure using Microsoft Sentinel and Log Analytics to collect and analyze security events.
- Generated and investigated authentication and security activity on a Windows VM using KQL queries to identify suspicious behavior.
- Installed Sysmon for enhanced endpoint visibility and captured process, registry, and network telemetry.
- Troubleshoot and resolved log ingestion issues by creating custom Data Collection Rules (DCRs) to successfully ingest Sysmon operational logs into Sentinel.

Honeypot

- Developed a Python-based honeypot to simulate a login service and intentionally capture unauthorized authentication attempts.
- Logged failed login attempts with timestamps, usernames, passwords, and source context for analysis.
- Implemented basic lockout and rate-limiting logic to observe brute-force behavior patterns.
- Analyzed captured data to understand common attacker techniques and credential abuse attempts.

Education

Charter Oak State College — Bachelor of Science in Cybersecurity, GPA: 3.5/4.0 — Expected Graduation: 2027

CT State Community College — Associate of Science in Cybersecurity & Homeland Security — Completed: May 2025

Honors: Dean's List (2024 & 2025)

Relevant Coursework: Incident Response, Access Controls & PKI, Operating System & Asset Security, Network Essentials, Ethical Hacking & Penetration Testing, Practices in Security Management, Program Logic & Design with Python, Database Design, Project Management, Legal Issues in Information Security

Technical Skills

SOC & Security: SIEM Monitoring, Alert Triage, Log Analysis, Incident Documentation, Authentication Analysis, Endpoint Telemetry Review, Threat Hunting Basics, Escalation Procedures

Cloud & Monitoring: Azure, Azure Monitor, Log Analytics Workspace, Microsoft Sentinel, Data Collection Rules (DCR), Data Collection Endpoint (DCE), Azure Monitor Agent (AMA), Azure Resource Groups, Network Security Groups (NSGs), Splunk

OS & Logging: Windows Event Logs (Security, System, Application), Sysmon (Microsoft-Windows-Sysmon/Operational), Event Viewer

Querying & Scripting: KQL (Kusto Query Language), PowerShell (basic), SQL (basic)

Identity & Admin: Active Directory, Users and Groups, Group Policy (GPO)

Virtualization: VMware

Operating Systems: Windows, Linux