Joshua Mitchum

730-221-8112 | Leorootsec@gmail.com | linkedin.com/in/joshuamitchum | California, USA

PROFESSIONAL SUMMARY

Security professional with three years of multi-tenant MSSP SOC experience and an active offensive security focus, backed by a hands-on IT foundation spanning hardware repair, systems administration, and end-user support. Background in adversary simulation, Active Directory attack chains, and detection engineering informed by an attacker's perspective. Holds PNPT, PJPT, and eJPT; OSCP currently in progress. Proficient in Microsoft Sentinel (KQL), Splunk, BloodHound CE, and the full Impacket/AD attack toolkit. Builds custom tooling to eliminate friction in offensive workflows. Active on HackTheBox and OffSec Proving Grounds.

CERTIFICATIONS

Practical Network Penetration Tester (PNPT) — TCM Security
Practical Junior Penetration Tester (PJPT) — TCM Security
Junior Penetration Tester (eJPT) — INE Security
Offensive Security Certified Professional (OSCP) — In Progress, OffSec

LABS & TRAINING

Dante Pro Lab — Hack The Box

EDUCATION

University of Maryland Global Campus (UMGC) — Bachelor of Science, Cybersecurity

EXPERIENCE

SOC Analyst
2023 – March 2026

Northern Technologies Group (NTG) — Managed Security Service Provider

- Authored and drove adoption of a BloodHound CE / AzureHound CE Quarterly Identity Attack Path Review program across 20+ client tenants — reduced the monthly privileged-account audit review from a full week to a single day.
- Built custom KQL detection rules in Microsoft Sentinel mapped to MITRE ATT&CK — covering credential stuffing, lateral movement, authentication bypasses, and ACL/permission abuse — informed directly by attacker-perspective lab work.
- Investigated Microsoft 365 and Entra ID abuse including privileged role misuse, delegated permission exploitation, and over-privileged account identification across 20+ client tenants.
- Proposed and designed a Kasm Workspaces malware detonation sandbox approved by SOC management, providing isolated dynamic analysis for suspicious files and URLs without risk to client infrastructure.
- Performed static and dynamic malware analysis using FLARE VM, Ghidra, and sandbox detonation to extract IOCs, map TTPs, and produce detection logic from real samples.
- Engineered Python automation for EDR compliance gap analysis across FortiEDR and Halcyon EDR, surfacing endpoint coverage blind spots across 20+ tenants that would otherwise require manual auditing.
- Triaged and investigated security alerts across a 24x7 multi-tenant SOC covering 20+ client tenants, consistently meeting a required minimum of 20 alerts triaged per tool, per shift, across Microsoft Sentinel, Splunk, FortiEDR, Halcyon EDR, and FortiMail.
- Ran vulnerability assessments using Greenbone/Nessus, scored by CVSS severity, and delivered remediation guidance to client stakeholders.
- Served as NOC backup for network monitoring (Zabbix), outage response, and infrastructure health checks across the client tenant base.

Junior Technician → Senior Windows Technician
2021 – 2023

Carbondale Computer Repair

- Progressed from Junior Technician to Senior Windows Technician over two years, taking on increasing ownership of infrastructure, training, and escalated technical work.
- Administered and maintained a custom-built, in-house ticketing platform, managing workflow, uptime, and issue tracking for all incoming service requests.
- Configured and maintained network firewall infrastructure, managing rule sets and access policies to secure client and internal networks.
- Performed on-site network and server troubleshooting across client environments, resolving connectivity, performance, and infrastructure issues.
- Diagnosed and remediated malware/virus infections across client Windows systems, restoring functionality and hardening against reinfection.
- Performed component-level hardware repair including soldering and board-level diagnostics/repair on laptops, desktops, and peripherals.
- Trained and mentored incoming Windows technicians on repair workflows, ticketing procedures, and troubleshooting methodology.

Junior Technician **2019 – 2021**

Fyxit

- Managed inventory tracking and parts procurement to support ongoing repair operations.
- Performed small electronics and mobile device repairs, including phone screen/component replacement.
- Diagnosed and resolved Windows OS issues across customer devices, including troubleshooting boot failures, driver conflicts, and performance degradation.
- Conducted virus and malware cleanup on customer systems, restoring device functionality and performance.
- Performed data recovery on damaged or corrupted drives to retrieve customer files and critical data.

TECHNICAL SKILLS

Offensive / AD	BloodHound CE, AzureHound CE, Mimikatz, Impacket, Rubeus, CrackMapExec, PowerView, Evil-WinRM, Responder, Metasploit, Burp Suite
AD Attack Chains	Kerberoasting, AS-REP Roasting, ACL/DACL abuse, Pass-the-Hash, Pass-the-Ticket, lateral movement, forest trust exploitation, PSRemoting backdoors
Web Security	OWASP Top 10, Burp Suite, SQLMap, Nikto — application enumeration, injection, authentication bypass
Malware Analysis	FLARE VM, Ghidra, IDA Pro — static and dynamic analysis, IOC extraction, TTP mapping
SIEM & Detection	Microsoft Sentinel (KQL — advanced), Splunk (SPL), FortiEDR, Halcyon EDR — detection engineering, rule tuning, telemetry gap analysis
Monitoring / NOC	Zabbix — infrastructure and uptime monitoring, alerting, NOC backup support
Cloud / Identity	Microsoft Entra ID (Azure AD), OfficeActivity log analysis, conditional access review, privileged role abuse investigation
Scripting	Python, PowerShell, Bash — custom tooling, API integration, automation, log enrichment
Infrastructure	Docker, Docker Compose, Vagrant, VirtualBox, pfSense, Debian Linux — lab build and hardening
Hardware / Field IT	Component-level soldering and board-level repair, PC/laptop/mobile diagnostics and rebuild, firewall configuration, ticketing system administration, data recovery
Platforms	HackTheBox, OffSec Proving Grounds, TryHackMe

KEY PROJECTS

Active Directory Attack Lab | Personal Lab
Full AD attack chain practice environment — Kerberoasting, AS-REP Roasting, ACL/DACL abuse, Pass-the-Hash, Pass-the-Ticket, lateral movement, and forest trust exploitation. Used directly to build MITRE ATT&CK-mapped detection logic and understand attacker dwell patterns.

Zentrix — Penetration Testing Productivity Tool | Personal Project (In Progress)
Python/Qt desktop application with embedded terminal, tabbed session navigation, and a lightweight AI model that auto-generates structured notes from terminal sessions — built to reduce engagement documentation overhead and support clean lab reporting.