

Sujan Guditi

gsujan1@vt.edu

| [linkedin.com/in/sujan-guditi](https://www.linkedin.com/in/sujan-guditi)

| 5uj4n.com (personal website)

Professional Summary

Cybersecurity professional with experience owning enterprise vulnerability management programs and hands-on Tenable Nessus and Rapid7 InsightVM experience in regulated, multi-system environments. OSCP-certified with an attacker-informed perspective that sharpens exploitability assessment beyond raw CVSS scores. Skilled in applying STIG and CIS baselines, running credentialed scans across Windows and Linux, and translating prioritized findings for both engineering teams and executives. MITRE ATT&CK-aligned incident response background with SOC leadership across HITRUST and NIST SP 800-53 contexts.

Certifications & Achievements

- **OSCP+/OSCP** - Offensive Security - December 2024
- **Foundational Cybersecurity Technologies (GFACT)** - GIAC - January 2022
- **Security+** - CompTIA - Expired January 2024
- **Top 2% of users on TryHackMe**
- **Eagle Scout** - Boy Scouts of America, Troop 007 - May 2016

Education

B.S. Business Information Technology (Concentration in Cybersecurity)

2016 - 2021

Virginia Tech

Technical Skills

- **Vulnerability Assessment:** Tenable Nessus SC, Rapid7 InsightVM, credentialed scanning (Windows/Linux/network), scan template & policy configuration, STIG & CIS baseline application, FISMA-aligned continuous monitoring
- **Threat Detection & Response:** CrowdStrike Falcon XDR, Carbon Black, Google SecOps SIEM, F5 WAF, Zscaler ZIA, MITRE ATT&CK, Cyber Kill Chain, log correlation, TTP analysis, SOP/runbook authoring
- **Offensive Security:** OSCP-certified internal/external pentesting, Active Directory attack path analysis, BloodHound, Impacket, NetExec, Mimikatz, Kerberos exploitation, privilege escalation
- **Compliance & GRC:** HITRUST, NIST SP 800-53, CIS STIGs, control gap identification, evidence collection, remediation tracking
- **Scripting & Automation:** Python, PowerShell, Bash - data parsing, tool integration, reporting automation
- **Platforms & Protocols:** Windows Server, Linux (RHEL/CentOS/Kali), Azure, TCP/IP networking

Work Experience

Security Operations Center Lead

2022 - Present

UST Healthproof (now HealthEdge, a Bain Capital company), Aliso Viejo, CA

- Own enterprise vulnerability management program across multiple acquisitions, including full migration from Tenable Nessus to Rapid7 InsightVM; manage credentialed scans of Windows, Linux, and network devices for continuous monitoring across regulated systems.
- Configure and maintain scan templates and policies by asset type, repository, and credential profile, sustaining optimized coverage and repository accuracy across FISMA-analogous compliance environments.

- Apply CIS and STIG baselines to surface configuration gaps across Windows, RHEL, and CentOS; deliver risk-prioritized remediation reports that separate exploitable risk from theoretical exposure using threat intelligence and asset context.
- Coordinate with engineering teams, system owners, and ISSOs to explain findings, recommend mitigations, and drive remediation to closure; author and maintain SOPs and runbooks for scanning and emergency-response procedures.
- Investigate incidents using CrowdStrike Falcon, Carbon Black, Google SecOps, Zscaler ZIA, and F5 WAF; perform TTP analysis aligned to MITRE ATT&CK and the Cyber Kill Chain, producing root-cause documentation and executive summaries.
- Support HITRUST assessments under NIST SP 800-53 through control documentation, evidence collection, and remediation tracking; integrated ZPA, InsightConnect, and Wiz to maintain control coverage.

Cybersecurity Intern

May 2021 - December 2021

Emergent Holdings, Detroit, MI

- Automated collection of vulnerability scan data, XDR telemetry, and Azure Security Center metrics into Power BI dashboards, improving enterprise-wide visibility into control effectiveness.
- Deployed backend infrastructure to Azure; developed working familiarity with Azure security architecture and cloud-based monitoring.