CELTY STURLUSON

SOC ANALYST

San Francisco Bay Area, CA | celty@opulant.dev | opulant.dev | github.com/opulant

PROFESSIONAL SUMMARY

SOC analyst in security operations and identity support since October 2025, now triaging 100+ alerts per day across 200+ defense-industrial-base clients subject to CMMC and NIST SP 800-53. Monitor and investigate alerts in Microsoft Sentinel, Microsoft Defender XDR, and Google SecOps, contain compromised accounts in Microsoft Entra ID, and write phishing campaign findings reports for clients. Hold an ABET-accredited B.S. in Cybersecurity and Information Assurance and 14 industry certifications, including CompTIA Security+, CySA+, and PenTest+. U.S. citizen, eligible for Public Trust.

TECHNICAL SKILLS

SIEM: Microsoft Sentinel, Microsoft Defender XDR, Google SecOps (Chronicle), KQL, UEBA, alert triage, alert tuning, log analysis

Incident Response: phishing analysis, IOC enrichment (VirusTotal, AbuseIPDB), MITRE ATT&CK, Cyber Kill Chain

Identity and Cloud: Microsoft Entra ID (Azure AD), Conditional Access, Azure, Active Directory, Group Policy, IAM, MFA, MDM

Compliance and Documentation: NIST SP 800-53 Rev. 5, NIST SP 800-37 RMF, CMMC, FISMA, risk assessment, BC/DR planning, findings reports, technical writing

Security Testing (labs and coursework): Burp Suite, Metasploit, Nmap, John the Ripper, hashcat, Hack The Box

Systems and Scripting: Windows Server, Linux, TCP/IP, VPN (Palo Alto GlobalProtect, Ivanti/Pulse Secure), Python, SQL, REST APIs

Ticketing and Remote Support: ConnectWise, ServiceNow, LogMeIn Rescue, ITIL 4

PROFESSIONAL EXPERIENCE

SOC I Analyst, managed security provider for the defense industrial base (remote) Jun 2026 - Present

- Triage 100+ security alerts per day in Microsoft Sentinel, Microsoft Defender XDR, and Google SecOps across 200+ defense-industrial-base clients under CMMC and NIST SP 800-53; escalate about 10 per day with evidence and remediation steps
- Contain compromised accounts by revoking user sessions and resetting credentials in Microsoft Entra ID; support MDM device-compliance checks and remote actions
- Investigate phishing campaigns by analyzing headers, sender infrastructure, URLs, and attachments with VirusTotal and AbuseIPDB; write campaign findings reports for clients
- Write KQL queries for investigations and threat hunting; draft queries and log summaries with AI tools and verify each result before use
- Traced about 15 false new-IP alerts per day in a UEBA policy for Microsoft Entra ID Conditional Access to an IPv6 parsing failure that stored each IPv6 sign-in as an empty IP value; escalated to security engineering, whose fix stopped the alerts
- Map observed activity to MITRE ATT&CK and the Cyber Kill Chain to prioritize escalations and recommend controls
- Coordinate incident remediation with MSP partners and security engineering; document cases in ConnectWise

Infrastructure Analyst, global IT services firm (remote) Oct 2025 - Jun 2026

- Provided identity and access management (IAM) support for enterprise users through ServiceNow tickets and LogMeIn Rescue remote sessions: password resets, account unlocks, permission changes, and MFA enrollment and troubleshooting
- Handled sensitive government data under NIST-aligned procedures and kept audit trails in ServiceNow
- Escalated suspicious logins, phishing, and account misuse; resolved VPN access issues with vendors

CERTIFICATIONS

Core: CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+), CompTIA PenTest+, CompTIA Network+, CompTIA A+, CompTIA Data+, CompTIA Project+, ITIL 4 Foundation, LPI Linux Essentials
CompTIA Stackable: Network Security Professional (CNSP), Security Analytics Professional (CSAP), Network Vulnerability Assessment Professional (CNVP), Secure Infrastructure Specialist (CSIS), IT Operations Specialist (CIOS)
In Progress: Hack The Box Certified Defensive Security Analyst (HTB CDSA), SOC Analyst path

EDUCATION

Bachelor of Science (B.S.), Cybersecurity and Information Assurance, Western Governors University (ABET-accredited program; NSA/DHS CAE-CD designated institution)
Capstone: Active Directory MFA lab with hardened Group Policy and controls mapped to NIST SP 800-53; wrote the stakeholder proposal, executive summary, and technical report covering implementation and test results

PROJECTS

CyberApply (personal project): Built a job aggregator that pulls listings from open-source job sites through their APIs, generates a resume tailored to each posting, and scores each match as a relevance percentage from keyword overlap with the resume