DAVID REID

Monroe, WA | 501-259-4105 | dtreid30@gmail.com | Top Secret/SCI | Remote - West Coast Eligible

PROFESSIONAL SUMMARY

Cybersecurity operations professional and U.S. Air National Guard Technical Sergeant with 15+ years of military service and experience supporting security operations center (SOC) functions, incident response, threat hunting, detection engineering, cloud security, digital forensics, host/network defense, and enterprise endpoint operations. Senior qualified host analyst, crew lead, and Flight Chief with hands-on experience analyzing AWS cloud environments using Splunk and AWS-native security telemetry. Proven ability to investigate Windows and Linux systems, automate remediation with PowerShell and Python, and translate technical findings into risk-based recommendations for military, federal, and industry stakeholders.

KEY IMPACTS

- Cut endpoint remediation time by approximately 83%, from about 30 minutes to 5 minutes per system, by developing a repeatable PowerShell automation supporting sites responsible for roughly 5,000 laptops and desktops.
- Led host analysis and incident response operations as senior qualified host analyst, crew lead, and Flight Chief across two complete Cyber Protection Team (CPT) taskings, including a joint tasking with the 853 CPT.
- Conducted AWS cloud threat hunting and security assessments using Splunk, CloudTrail, CloudWatch, GuardDuty, Security Hub, IAM, VPC Flow Logs, AWS Config, S3, EC2, Security Groups, and NACLs to identify suspicious activity, scope incidents, and recommend remediation.

TECHNICAL SKILLS

Security Operations & Incident Response: SOC operations, SIEM monitoring, alert triage, incident handling, containment, eradication, recovery, case documentation, root-cause analysis, malware triage

Threat Hunting & Detection Engineering: MITRE ATT&CK, TTP analysis, threat hunting, detection gap analysis, detection tuning/support, Splunk, ELK Stack, Security Onion, Arkime, Hive

Digital Forensics & Endpoint Security: Windows/Linux host analysis, endpoint detection and response (EDR), Redline, Metasponse, Endgame, Sysinternals, FTK Imager, Volatility, ESXi

AWS Cloud Security: CloudTrail, CloudWatch, GuardDuty, Security Hub, IAM, VPC Flow Logs, AWS Config, S3, EC2, Security Groups, NACLs, cloud telemetry and configuration review

Scripting & Automation: PowerShell, Python, Bash, JSON/jq, endpoint remediation scripting, process automation, repeatable operating procedures

Enterprise & Networking: Windows administration, Active Directory, Microsoft 365, Cisco/Brocade switching, TCP/IP, network troubleshooting, CVA/H, Defensive Infrastructure Platform (DIP)

Leadership & Communication: Flight Chief, crew lead, team supervision, mentorship, analyst development, stakeholder briefings, incident documentation, customer and mission-partner support

PROFESSIONAL EXPERIENCE

Senior Qualified Host Analyst & Crew Lead / Cyber Warfare Operator

852 Cyber Protection Team (CPT) / 143rd Cyber Operations Squadron - Deployed / Lakewood, WA | Sep 2022 - Mar 2023 | Apr 2026 - Oct 2026

- Lead deployed defensive cyber operations as a senior qualified host analyst and crew lead, directing host-based investigations, incident response, analyst tasking, and mission execution.
- Triage and investigate security incidents across Windows, Linux, and network systems; perform scoping, containment, eradication, recovery, root-cause analysis, documentation, and mission-partner communication.
- Conduct threat hunting and security assessments across AWS cloud networks using Splunk SIEM and AWS-native services including CloudTrail, CloudWatch, GuardDuty, Security Hub, IAM, VPC Flow Logs, AWS Config, S3, EC2, Security Groups, and NACLs.
- Analyze CloudTrail events, GuardDuty and Security Hub findings, IAM activity, VPC Flow Logs, and resource configurations to identify anomalous behavior, scope incidents, document findings, and recommend remediation.
- Apply the MITRE ATT&CK Framework to map adversary tactics, techniques, and procedures (TTPs), structure investigations, identify detection gaps, and strengthen detection engineering and response recommendations.
- Use Metasponse, Redline, Endgame, Sysinternals, FTK Imager, Volatility, Arkime, Hive, ELK Stack, Security Onion, Metasploit, and CVA/H for endpoint analysis, digital forensics, network security monitoring, and defensive operations.
- Configure and operate the Defensive Infrastructure Platform (DIP), CVA/H weapon system, and Security Onion to enable deployed collection, analysis, and defensive cyber operations.
- Develop PowerShell and Python scripts to automate repeatable cyber and endpoint tasks, reduce manual workload, standardize remediation, and improve response consistency.
- Configure and troubleshoot Cisco and Brocade switches to maintain operational network availability, support data collection, and meet mission requirements.
- Completed two deployed CPT taskings, including one joint tasking with the 853 CPT, coordinating technical actions, investigative findings, and remediation recommendations with cross-functional mission partners.

Flight Chief / DSG Supervisor

143rd Cyber Operations Squadron, Washington Air National Guard - Lakewood, WA | Dec 2019 - Present

- Lead and mentor more than 10 Airmen as Flight Chief, managing readiness, training, task assignments, performance feedback, and analyst development while aligning team execution to mission objectives.
- Deliver technical guidance and training on cybersecurity procedures, incident response, host/network defense, operational security, and mission best practices.
- Improved career progression and mission readiness by mentoring Airmen through qualification and promotion requirements, contributing to two promotions to Senior Airman and one promotion to Technical Sergeant.
- Coordinate classified and unclassified cyber operations with military branches, federal agencies, and industry partners to share threat intelligence, align investigative actions, and support defensive response.
- Translate complex cyber activity into concise executive and technical briefings that communicate impact, risk, remediation priorities, and follow-on detection opportunities.

Desktop Support Technician - CLIN25 VIP

Leidos - Washington / Remote Support | Dec 2023 - Present

- Provide enterprise VIP desktop support for high-visibility users, troubleshooting Windows endpoints, Active Directory accounts, Microsoft 365, CAC authentication, software, connectivity, peripherals, and customer-impacting incidents.
- Manage incident intake, prioritization, escalation, documentation, and resolution against service-level agreements (SLAs), communicating status and solutions to technical and non-technical users.
- Developed a PowerShell automation that cut a Navy-wide endpoint remediation process by approximately 83%, from about 30 minutes to 5 minutes per system, improving support efficiency across sites responsible for roughly 5,000 endpoints.
- Apply Windows administration, command-line troubleshooting, PowerShell scripting, and endpoint remediation expertise to standardize support workflows, improve first-time resolution, and reduce manual effort.
- Partner with infrastructure, cybersecurity, and support teams to resolve recurring incidents, validate corrective actions, document durable workarounds, and reduce repeat issues.

Aerial Port Technician / Logistics Specialist / Supervisor

189th Logistics Readiness Squadron - Little Rock, AR | Apr 2010 - Dec 2019

- Supervised six enlisted personnel, coordinating training, work assignments, safety, accountability, and mission execution in a high-tempo logistics environment.
- Executed regulated air transportation operations including cargo rigging, airdrop preparation, joint inspections, passenger/cargo manifests, load planning, and special-cargo handling.
- Trained Airmen on mission procedures and heavy equipment, reinforcing procedural compliance, risk management, operational readiness, and leadership development.

VOLUNTEER EXPERIENCE

Volunteer Firefighter / Red Card Holder

U.S. Air Force Rapid Response Fire Protection Team

- Serve as a federally certified wildland firefighter (Red Card holder), supporting rapid deployment operations alongside active-duty fire protection personnel in high-risk, protocol-driven environments.

EDUCATION & CERTIFICATIONS

- Associate of Arts, Liberal Arts - Arkansas State University, Beebe, AR | 2014
- Community College of the Air Force Degree, Logistics - United States Air Force | 2017
- CompTIA Security+ | 2021
- CompTIA Cybersecurity Analyst (CySA+) | 2025
- Defensive Cyber Operations Course | 2023
- CVA/H Host Analyst Course | 2023
- Cyber Warfare Operations Course | 2022

PROFESSIONAL DEVELOPMENT

Preparing for CompTIA SecurityX (formerly CASP+) and Certified Information Systems Security Professional (CISSP) certification exams.