William Grebenik

Sarasota, Florida | grebwv@hotmail.com | Phone: 321.830.0074
Military Veteran | Clearance: Former DoD Top Secret Clearance
DoD 8570 IAT Level III Certification
Web: https://www.linkedin.com/in/grebenik
Authorized to work in the US for any employer

Professional Summary

Cybersecurity professional with over 20 years of experience supporting government and enterprise environments. Specialized in endpoint security, vulnerability management, and compliance within DoD frameworks. Proven ability to manage, deploy, and optimize security solutions across Windows, Linux, and cloud platforms.

Core Competencies

Zero Trust Architecture | Endpoint Security | McAfee HBSS | ACAS | Microsoft Defender for Endpoint | Incident Response | SIEM | Microsoft Sentinel | CrowdStrike EDR | Rapid7 IDR | Vulnerability Management | Qualys VMDR | Rapid7 InsightVM | Cloud Security | Compliance Management| NIST | DoD Compliance | Microsoft Purview | Hyperproof | Azure Cloud | Linux and Windows Administration | Active Directory | Scripting (PowerShell) | Patching

Highlights

Led vulnerability management and remediation activities across cloud and enterprise environments, supporting continuous improvement of organizational security posture.

Administered and optimized security detection platforms, including Microsoft Sentinel and CrowdStrike EDR, to enhance threat detection, incident response, and operational readiness.

Integrated threat intelligence into vulnerability management and incident response processes, supporting proactive risk mitigation and situational awareness.

Supported compliance initiatives aligned with NIST, DoD, and industry frameworks, maintaining audit readiness and contributing to successful external and internal audits.

Managed endpoint security and access controls across Windows, Linux, and Azure cloud platforms, ensuring alignment with Zero Trust principles and best practices.

Developed and maintained detection logic and analytic queries in SIEM and EDR platforms to improve telemetry quality and reduce false positives.

Performed advanced security investigations, including phishing analysis, vulnerability assessments, and root cause analysis, to support incident response and remediation using Defender, Rapid7 IDR and CrowdStrike Falcon.

Provided guidance on cloud security, endpoint protection, and compliance requirements, translating complex risks into actionable recommendations.

Work Experience

Principal Consultant

EugeneZonda
Sarasota, Florida
Nov 2025 – Present

- Security audits & risk assessments
- Policy development and updates
- Governance and risk advisory

Vulnerability Management Consultant

Kontio Power, LLC
Sarasota, Florida
Jun 2025 – Present

- Security audits & risk assessments
- Policy development and updates
- Data Loss Prevention (DLP) & insider threat mitigation
- Cloud security architecture (Azure)
- Vulnerability management & remediation planning
- Regulatory compliance (HIPAA, PCI-DSS, GDPR, CCPA)
- Rapid7 SIEM
- Rapid7 Insight VM
- CrowdStrike Falcon
- PDQ Patching System
- Cisco Umbrella

Vulnerability Management Consultant

Robert Half Recruiters
Miami, Florida
Jan 2025 – May 2025

- Maintained BottomLine's Vulnerability Management Program.
- Migrated vulnerability management platform from Rapid7 InsightVM to Qualys VM.
- Developed Zero-Day vulnerability detection and reporting system.
- Performed vulnerability scans and risk assessments across enterprise endpoints.
- Monitored vulnerabilities in endpoints, databases, networking, and cloud services.
- Collaborated with IT and security operations to remediate system vulnerabilities.
- Integrated threat intelligence into vulnerability management processes.

Senior Cyber Security Engineer

BlackLine Systems, Inc.
Woodland Hills, California
July 2022 – October 2024

- Performed vulnerability management for OS and applications on-premise and cloud.
- Administered and deployed security tools including Microsoft Defender, Sentinel, CrowdStrike and Rapid7.
- Managed alerts and detection rules in Microsoft Sentinel and 365 Defender.
- Utilized Qualys and Rapid7 for CVE management and vulnerability analysis.
- Supported compliance using Microsoft Purview and Hyperproof.
- Conducted phishing analysis using Cofense Triage and Abnormal Security.
- Managed CrowdStrike EDR and Rapid7 InsightIDR SIEM alerts.

Information Security Analyst

Net2Source Inc.
Somerset, New Jersey
Nov 2021 – Jun 2022

- Remotely worked for Net2Source supporting Becton Dickinson (BD) Medical Technology Company with their Vulnerability and Threats Information Security team.
- Identification and proactive mitigation of cyber threats, while collaborating with various teams within Information Security to support the company's strategic goals.
- Report and communicate vulnerabilities to determine objectives, scope, analysis, and the proper actions, needed to respond to security vulnerabilities.
- Collaborate on patch validation and reporting of remediation planning and compensating controls of mitigation to address open vulnerabilities.
- Developed Qualys custom dashboard for CISA Known Exploited Vulnerabilities.
- Developed PowerBI dashboards for Qualys Vulnerability scan results.
- Developed PowerBI dashboards for Microsoft 365 Defender reports.
- Monitors, tracks, responds, investigates, and reports in compliance to security requirements, and partners with the responsible parties to drive timely results and remediation.
- Performs analysis of cyber threats and process timely tasks to help mitigate the risk of exposure.
- Review daily intelligence feeds, working with different Security Operations teams to apply technical controls to detect and protect information systems.

Senior Cyber Security Engineer

Edgesource Corporation
Melbourne, Florida
Jul 2020 – Oct 2021

- Supporting the Department of State, Bureau for International Narcotics and Law Enforcement Affairs, Office of Aviation (INL/A), interchangeably referred to as DoS Air Wing.
- Providing IPS/IDS security and network defense on a global network using:
- Cisco Firepower Management Center (FMC) - centrally manage policy, unified management of firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.
- Cisco Web Security Appliance (WSA) – proxy management, whitelists to manage website access, content, traffic, protect against malware and zero-day attacks.
- Cisco Email Security Appliance (ESA) - protect users from spam, viruses, spoofing, phishing, and spyware attacks.
- Cisco Adaptive Security Appliance (ASA) – firewall management. Add/remove access rules. Manage WCCP redirection to WSA Proxy.
- Security Architect for implementation of edge source protection.
- Certificate management for Cisco appliances.
- Supported DoS Air Wing with IPS/IDS and endpoint security.
- Managed Cisco Firepower, WSA, ESA, ASA, and VMware vSphere.

Senior Systems Administrator

Raytheon
Doha, Qatar
May 2017 - May 2019

- Implementation, maintenance, troubleshooting, and upgrading systems hardware and software configurations, ensuring total operational and functional compatibility with interfaces, and interacting systems, subsystems, equipment, and computer applications.
- Systems include Windows Based Active Directory Domains, VMware, Video Surveillance Software, Cisco Switches/Routers, and Video over IP (Multicast and Unicast-based). Migrated Windows server operating systems.

Cyber Security Information Assurance Security Officer

Agile Defense, Inc.
Doha, Qatar
November 2014 - May 2017

- Cybersecurity management on a Citrix thin client infrastructure for the U.S. Air Force Combined Air and Space Operations Center in the Doha, Qatar. Ensured compliance with Department of Defense (DoD) and other agency guidelines. Executed technical protocols including troubleshooting Citrix PVS, ZDC, NetScaler, VMware vSphere, and Windows systems. Managed vDisk images for Citrix XenApp 6.5 farm via Provisioning Services supporting multiple classified networks with thousands of end users daily.

- Strengthened compliance with security findings and maintained system security and operations through building and updating client images on multiple classified network enclaves, as well as updating in-house applications.
- Maintained and supported a high-availability, multi-forest Active Directory environment consisting of several classified enclaves with servers running Windows Server 2008 R2.
- Performed patch management remediation on servers along with backups and recoveries; as well as SCCM/WSUS administration, software updates, packages distributions, and configuration management via VMware vSphere.
- Maintained all system's documentation, including workflows, run books, technical processes, standard operating procedures, and process knowledge databases.

CISO Theater Information Assurance Manager

Trace Systems, Inc.
Kabul, Afghanistan
June 2013 - April 2014

- Directed security team of 50 technicians on multiple bases, managing 50,000 systems across 3 government networks supporting 150,000 personnel. Partnered with senior leadership to promote, develop, and Implemented security policies and programs affecting all government networks operating in Afghanistan. Updated USFOR Afghanistan network policies and aligned them to NIST framework for future management.
- Executed Certification and Accreditation validation.
- Validated multinational account access to NIPR, SIPR, and Centrix networks for foreign military personnel to gain access to classified networks.
- Streamlined security processes and updated standard operating procedures to achieve trusted reporting systems for theater DoD compliance.
- Investigated and reported on Cross Domain Violations and Discharge of Classified Information.

Regional CISO Cyber Security Information Assurance Manager

Intecon LLC.
Mosul, Iraq
Mar 2006 – Oct 2011

- Managed IA Program across multiple bases in Iraq.
- Operated McAfee HBSS via ePO server and IDS tools.
- Maintained Retina Digital Server for vulnerability scanning.
- Supported DoD cybersecurity operations and compliance.
- Managed Information Assurance Program for U.S. Force's southern, northern, and western Iraq regions, leading a regional cybersecurity team across 3+ bases in Northern

Iraq. Oversaw all network security, compliance, security policy, and the Defense in Depth security program.

- Investigated and reported on Cross Domain Violations and Discharge of Classified Information
- Served as subject-matter expert throughout region for all IA policies, procedures, incidents, and audit compliance.
- Balancing the needs of network security and operational needs in a hostile environment.
- Assisted in building reporting system to brief senior leadership on risks to the theater network enclaves. Operated and monitored McAfee HBSS vis EPO server and IDS tools, identifying, and resolving threats to the network. This system provided a centralized system to secure Windows desktops across the theater. Continuously improved security from individual base enclaves to a theater-wide network enclave, through providing central offices for bases to work through their INFOSEC policies and procedures
- Supported information assurance operations of U.S. Army in Iraq in a contracted role. Utilized various tools to monitor, identify, analyze, and resolve malicious activity and network vulnerabilities.
- Implemented policy streamlining Help Desk procedures and improving response times for IA issues, including virus/malware infections and data compromise issues.
- Maintained and updated Retina Digital Server, executing security scans against 3,500+ Microsoft workstations and servers, and analyzing data to ensure updated IAVM patches.
- Overcame initial security challenges resulting from hastily built network with no patching or monitoring tools; slowly increasing security levels as procedures were built.

Senior Systems Administrator

ITT Federal Services International, Inc.
Nasiriyah, Iraq
Apr 2005 - May 2006

- Systems administer for three Windows Active Directory Domains in Iraq
- Migrated SIPR and NIPR domains to new forest.
- Migrated Active Directory 2000 domain to 2003 within same domain structure.
- Designed and deployed new DNS services in domain.
- Designed and deployed DHCP services in domain.
- Deployed new domain controllers on base.
- Built new image server for base using Norton Ghost.
- Reduced Exchange outages from daily outages to less than 1 hour per month in forward deployed military base.
- Migrating from Exchange 5.5 to Exchange 2003 on main network
- Reduced network vulnerabilities using Harris Stat scanner software from a high of 1583 to 0 in two months.

- Implemented a desktop baseline image program using Norton Ghost to reduce compliance issues.

Information Technology Consultant

Panthera Solutions, Inc.
Colorado Springs, Colorado
May 2003 – April 2005

- Installed and configured Windows technologies.
- Consulted with corporate clients in Information Technology issues.
- Active Directory Installation
- Virtual desktop deployment
- Microsoft Certified Trainer
- Trained clients in Microsoft MCSE Certifications.

Senior Systems Administrator

Agilent Technologies
Colorado Springs, Colorado
November 1999 - May 2003

- Agilent Technologies was spun off from Hewlett-Packard November 1, 1999.
- Lead team of 15 engineers, building, deploying, and supporting 1500 Windows NT/2000 servers deployed worldwide.
- Directed the team that designed, ordered, built, and installed over 400 servers in the first year as a new company.
- Developed Windows 2000 rollout plan for team.
- Deployed 63 Windows 2000 Domain Controllers worldwide for new Active Directory Domain.
- Managed projects for various national and international system implementations and upgrades.
- Traveled extensively to customer sites to install, implement, and upgrade systems.
- Escalation management for crisis resolution.

Systems Administrator

Hewlett-Packard Company,
Colorado Springs, Colorado
September 1996 - October 1999

- Lead team for Windows NT server support during rapid startup period.
- Successfully deployed approximately 80 servers in 10 locations in first six months of teams' inception (1996) in 10 locations in U.S. and Scotland.
- Procured over $500,000.00 of system hardware for project implementations in first year.

- Implemented system upgrades of Windows NT servers from 3.51 to 4.0.
- Supported 100 NT Servers internally to Hewlett-Packard with approximately 3.3 Terabytes of disk storage space in 11 locations after first two years of operation (1996-1998).
- Specified system requirements for NT file, print, and application servers.

Customer Engineer

Hewlett-Packard Company,
Colorado Springs, Colorado
July 1994 - May 1996

- Field service for H-P products and customers in western states.
- Extensive customer contact with large customer base.
- Travel to remote customer sites in three western states.
- Provided H-P quality service for regional area customers.
- Responsibilities included hardware/software support for UNIX and NT Servers, disk arrays, personal computers, plotters, laser printers and multi-vendor products.

Education

Master of Business Administration
Western Governors University, Salt Lake City, UT

Master of Science in Computer Engineering
Colorado Technical University, Colorado Springs, CO

Bachelor of Science in Computer Engineering
Colorado Technical University, Colorado Springs, CO

Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Cisco Certified Network Professional – Security (CCNP Security)
- ITIL v3 – AXELOS Global Best Practice
- Microsoft Azure Fundamentals
- Microsoft Azure AI Fundamentals
- Qualys Vulnerability Management Detection and Response (VMDR)