David E O’Neal

(501) 749-4031 | onealdavide@gmail.com | Cabot, Arkansas 72023
https://www.linkedin.com/in/david-oneal/

Professional Summary

Cybersecurity professional with 3+ years of operational security experience and a growing focus on Governance, Risk, and Compliance (GRC). Proven ability to reduce organizational risk through technical control enforcement, patch automation, and identity governance. Skilled at translating technical details into business risk impact through reporting, SOP development, and audit collaboration. Currently expanding expertise in NIST frameworks, FAIR risk modeling, and regulatory compliance to support GRC-driven security programs.

Professional Experience

Cybersecurity Consultant
Legato Security – Remote | Apr 2025 – Jul 2025 (Laid off due to company-wide reduction in force)

- Reduced organizational cyber risk for aerospace and industrial clients by designing and implementing enterprise patching and vulnerability management programs covering 279 endpoints across multiple environments.
- Managed vulnerability risk through Tenable/Nessus-based remediation, achieving 100% SLA compliance and reducing average remediation turnaround to 4–6 weeks, directly lowering exposure to exploitable CVEs.
- Created governance documentation for patching workflows, risk classification, and remediation procedures, strengthening audit readiness and compliance with security controls.
- Implemented a patching-as-a-service model that automated endpoint remediation, reducing operational risk, minimizing human error, and ensuring consistent monthly compliance with security policies.
- Enhanced governance and accountability by streamlining vulnerability tracking through JIRA and ticketing systems, providing clear risk status updates to technical teams and business stakeholders.

State IT Security Specialist
Arkansas Department of Public Safety – Little Rock, AR | Oct 2024 – Mar 2025

- Reduced compliance risk and improved audit readiness by maintaining 95%+ patch compliance across 500+ endpoints using PDQ Deploy and Patch Manager Plus.
- Produced KPI-driven dashboards to track high-risk vulnerabilities, enabling data-driven risk mitigation decisions and strengthening internal audit preparation for regulatory compliance.
- Administered identity governance in Active Directory, overseeing provisioning, deprovisioning, and periodic access reviews to enforce least privilege and mitigate insider threat risks.
- Supported governance initiatives by compiling and reviewing access control documentation for compliance audits, ensuring alignment with NIST 800-53 security control requirements.
- Partnered with IT leadership to communicate security posture improvements and residual risk to both technical teams and business stakeholders.

SOC Analyst
Bank OZK – Little Rock, AR | Oct 2021 – Jun 2024

- Minimized operational risk and alert fatigue by reducing false positives 40% through advanced tuning of Proofpoint, Microsoft Defender, and Cisco Secure Email Gateway detection rules.
- Investigated phishing, malware, Business Email Compromise (BEC), and data loss prevention (DLP) incidents, assessing business impact and documenting risk exposure for leadership.
- Conducted forensic investigations into potential data exfiltration using Forcepoint DLP and Behavioral Analytics, reducing fraud and data loss risks through rapid containment.
- Authored governance documentation to standardize Forcepoint DLP investigations, enabling consistent, auditable SOC response procedures.
- Collaborated with the security awareness team to refine phishing simulations and training, increasing organizational resilience to social engineering threats.

System Operations Analyst I
FIS Global | Little Rock, AR June 2017 – October 2021

- Maintained business continuity and minimized service disruption risk by monitoring enterprise systems with Splunk and responding to operational anomalies in real time.
- Coordinated cross-functional incident response during critical production outages, documenting root cause analyses to prevent recurrence and reduce systemic risk.
- Developed and maintained governance documentation for recurring operational issues, enhancing process consistency and auditability across teams.
- Liaised with offshore operations teams to ensure 24/7 coverage and compliance with service-level agreements (SLAs), mitigating downtime risk for high-profile client environments.
- Supported SLA compliance through proactive detection and escalation of performance issues, maintaining 99%+ uptime.

Technical Projects

Cybersecurity Lab – PSAA Course Capstone Project | Jan 2025 – Present

- Created a local virtual lab using VirtualBox as part of the Practical Junior SOC Analyst course from TCM Security to refresh cybersecurity skills and explore new tools.
- Set up a Windows and Ubuntu workstation to simulate a small enterprise network for hands-on practice.
- Gained practical exposure to incident response, log analysis, threat detection, and vulnerability scanning techniques in a controlled environment.
- Used the lab to sharpen detection engineering skills and expand experience with red and blue team workflows.

Education

M.S. in Cybersecurity
Maryville University of Saint Louis | Dec 2021

B.S. in Information Technology
University of Arkansas System eVersity | Nov 2019

Certifications and Professional Development

- AWS Certified Cloud Practitioner – In Progress (Expected 2025)
- Practical Junior SOC Analyst (PJSA) – In Progress
- GRC Analyst Masterclass (RMF, NIST 800-53) – In Progress
- SOAR Analyst – Google Cloud Siemplify (2024)
- XM Cyber Exposure Management – Completed (2024)
- VMDR – Qualys (2024)
- Insider Threat Detection – Teramind (2024)
- SANS SEC401 (GSEC) – Training Only
- FBI Citizens Academy – Little Rock Chapter (2024)

Key Skills

- **Governance, Risk, and Compliance:** NIST 800-53, RMF, CMMC, ISO 27001, PCI-DSS concepts; audit preparation and reporting; KPI development
- **Vulnerability and Patch Management:** Nessus, Tenable, PDQ Deploy, Patch Manager Plus, WSUS, Group Policy
- **Endpoint and Cloud Security:** AWS (EC2, S3, IAM – lab experience), Azure Sentinel, Google Chronicle, CrowdStrike Falcon, Microsoft Defender, Proofpoint, Cisco Secure Email
- **Identity and Access Management:** Active Directory provisioning, deprovisioning, access reviews
- **Automation and Scripting:** PowerShell (basic) for patching, reporting, remediation; familiarity with infrastructure-as-code concepts
- **SIEM and Monitoring:** Splunk (basic), Wazuh, Security Onion
- **Collaboration Tools:** JIRA, ServiceNow, Excel dashboards

Key Achievements

- Reduced phishing-related false positives by 40% through advanced detection tuning and email security hardening, improving SOC efficiency and lowering operational risk.
- Sustained 95%+ patch compliance across multiple environments through automation, directly reducing organizational attack surface and compliance risk.
- Assisted in third-party breach investigations, strengthening incident response processes and organizational resilience.
- Authored SOPs and governance documentation that improved team workflows and supported multiple compliance audits.
- Built a security lab from the ground up to reinforce endpoint security, SIEM tuning, and hands-on detection capabilities.
- Prepared, executed, and reported on an audit of NIST SP 800-53 cybersecurity controls, including stakeholder interviews, document review, and system testing to support compliance audit activities.
- Applied knowledge of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) to evaluate and improve security program effectiveness during training and practical projects.