Lester Artis Jr.

Cell: 757-770-2878 | lesterartisjr@gmail.com | LinkedIn

Information System Security Officer and Recent College Graduate: Strong attention to detail, intuition, time management, technical ability, and people skills.

Security Clearance- Active Secret Security Clearance (2023).

- **Effective communication-** Able to thoroughly communicate both written and verbal to all audiences.
- **Relationship management-** Capable of cultivating strong connections with internal team and public.
- **Technical Skills**- Proficient in Windows and Red Hat Linux Operating System, Microsoft Office Tools, Programming languages (C++, Java, Python, Bash, SQL, MongoDB), Proficient with the latest cybersecurity vulnerability scanning tools (Wireshark, Nessus, Splunk, PowerShell, e.g.), Knowledge of Ethical Hacking, Penetration Testing, Intrusion Detection, and other security vulnerability principles. Knowledge of NIST standards, including NIST 800-53 Rev5, 800-137 and risk management framework. Knowledge of networking concepts, tools, and protocols. Familiarity with software development methodologies like Agile and Scrum.

EXPERIENCE

PioneerTech **Oct 2024-Present**

Database Administrator Suffolk, VA

Clearance: Secret

Hours per week: 40 hours per week, Full-Time

- Managed 32 Linux servers and 140-150 databases (PostgreSQL, EnterpriseDB, Oracle, MySQL), ensuring 99.9% uptime and system reliability through effective maintenance, monitoring, and performance tuning.
- Migrated 3 critical systems, including Livelink/OpenText from Oracle 19c to PostgreSQL 13, improving system performance by 30%, reducing licensing costs by 50%, and modernizing the infrastructure.
- Spearheaded the ongoing migration of 12 databases for JKO from Oracle 19c to EnterpriseDB 14/MySQL 8.0, ensuring full database compatibility and stability while maintaining 100% security and compliance adherence.
- Automated over 20 repetitive database tasks, including server creation, error checking, and certificate renewals, reducing manual intervention by 40% and improving operational efficiency, saving over 200 hours annually.
- Managed database backups and recovery for 150+ databases using Barman, RMAN, and native PostgreSQL tools, ensuring a recovery point objective (RPO) of less than 1 hour and recovery time objective (RTO) of 2 hours.
- Implemented stringent security measures by managing user access, authentication policies, and ensuring 100% compliance with internal security standards and STIG requirements.
- Performed troubleshooting for 50+ system failures and service-impacting issues, consistently resolving incidents within 4 hours and minimizing system downtime..
- Contributed to a knowledge transfer initiative, documenting over 50 critical processes and key responsibilities, ensuring a seamless transition for successors and preserving operational continuity.

United States Military Entrance Processing Command **Aug 2023-Feb 2024**

Information System Security Officer North Chicago, IL

Clearance: Secret

Hours per week: 40 hours per week, Full-Time (GS-2210-04)

- As an entry-level Cybersecurity Officer my responsibilities included managing an average of 30 System Access Requests and other various tickets per day in ServiceNow, demonstrating my ability to handle a high-tempo workload efficiently. Monitoring training and certification compliance via Army Training & Certification Tracking System, conducting vulnerability scanning and compliance assessments on workstations, servers, and software utilized within MEPS infrastructure, and drafting, finalizing, and retrieving approval on multiple government documents.

- Utilized Cybersecurity Tools utilized by the Risk Assessment team, including ACAS, Evaluate-STIG, and STIG Viewer, managed Nessus for Assured Compliance Assessment Solution (ACAS) as an administrator, handling asset updates and new asset creation, and completing the weekly inputs for DAN and MIRS 1.0. Assisted in updating the ACAS Asset groups to reflect the current state.
- Performed STIG reviews, Used EVAL-STIG (formerly SCAP) for automated security testing and ensured compliance assessments with PowerShell. Coordinated with other teams to analyze and validate Evaluate-STIG results with answer files for DAN internal assessment. Conducted SPLUNK STIG reviews for enhanced security monitoring.
- Performed critical tasks within eMASS, significantly contributing to the successful completion of Authorization to Operate (ATO) renewals, comprehensive risk assessment, effective risk management, and continuous monitoring processes. Updated documentation in eMASS for submission to Security Control Assessment Validation (SCA-V) and Program Information System Security Managers (P-ISSM).
- Participated in daily Scrum meetings to discuss progress, blockers, and coordinate tasks and updated tasks in JIRA upon completion.
- Assisted with the installation and configuration of SolarWinds, including actively monitoring logs, configuring custom queries, and managing auditing processes.
- Collaborated with C5ISR teams on cloud-based backend setup for scan zones.
- Used Command Network Defense tools such as Trellix, Tychon, Log Correlation Engine, and CBII to administer and monitor systems and networks. Completed cross-training amongst CND Team members to learn how to perform entry-level functions such as: Analyzing network traffic for potential threats such as Unauthorized Access, Phishing Attempts, Malware, etc., Assessing systems and networks for vulnerabilities, Monitoring security logs for unusual activity, Assisting in incident response per protocols, Configuring and managing firewalls and IDS/IPS, Supporting patch management for system updates, and Documenting and reporting security incidents.
- Created PowerShell scripts to perform various network assessment and vulnerability task to minimize threat surface of the network.
- Managed the 2875 process, ensuring proper documentation, review, and approval of user access requests in alignment with security protocols and compliance standards.
- Oversaw privilege level access assignments, maintaining strict adherence to least-privilege principles to mitigate security risks and protect sensitive information.

CYBERSECURITY PROJECTS

Virtual Active Directory Environment in PowerShell

- Streamlined user account provisioning processes via PowerShell scripts, increasing efficiency and reducing human error risks.
- Configured RAS features for optimized remote access capabilities, enabling seamless distributed team and third-party connectivity.
- Maintained Windows DNS and DHCP services for efficient network resource allocation and name resolution, ensuring smooth network operations.
- Implemented file server quotas and NTFS permissions for strengthened data security and controlled access.

Cyber Risk Management Project

- Conducted cyber risk assessment of virtualized environments using Nmap, Nessus, and Metasploit to identify vulnerabilities, potential attack vectors, and provide prioritized remediation guidance.
- Leveraged CVE and CVSS scoring systems for effective vulnerability prioritization and resource allocation.
- Delivered detailed findings with automation scripts and supporting documentation for informed mitigation planning.

AI-Based Malware Detection

- Developed an optimized deep learning model using 1D CNN, Google Colab, and hyperparameter tuning for accurate and efficient malware detection from byte strings, enhancing proactive threat identification capabilities.
- Demonstrated application of cutting-edge AI techniques for malware detection
- Showcased ability to leverage deep learning for cybersecurity applications.

VPN Server Setup using AWS EC2 and Shadowsocks

- Deployed an AWS EC2 instance to configure a VPN server using Shadowsocks, enhancing secure communication.
- Installed and set up Shadowsocks on the server, configuring the IP address and password for optimal security.
- Implemented firewall rules using ufw to allow necessary ports, ensuring secure access and functionality.
- Monitored and restarted Shadowsocks services to ensure uptime and performance.

Automated AWS Backup and Logging for Oracle Database

- Designed an automated backup and logging solution for Oracle databases using AWS, enhancing data protection and monitoring efficiency.
- Configured AWS CloudWatch Logs to track database activity and trigger real-time alerts on critical events, improving incident response.
- Implemented AWS Backup with lifecycle policies, automating snapshots for streamlined retention and archival.
- Optimized long-term storage costs by leveraging Amazon S3 with Glacier for efficient backup archival.
- Developed Bash scripts to automate database backups, log monitoring, and disaster recovery, reducing manual intervention.
- Enforced least privilege access using IAM policies, securing backup and restore operations against unauthorized access.
- Strengthened security and compliance by implementing encryption and access controls, ensuring data confidentiality and integrity.

PostgreSQL Database Deployment on AWS using ECS Fargate

- Deployed a containerized PostgreSQL database using AWS ECS with Fargate, enabling scalable and serverless database operations.
- Built and stored PostgreSQL Docker images in AWS ECR, ensuring efficient version control and streamlined deployments.
- Configured ECS task definitions with 2048 MiB memory and 1 vCPU, optimizing resource allocation and performance.
- Integrated Amazon CloudWatch Logs for centralized log management, improving real-time monitoring and troubleshooting.
- Secured sensitive environment variables using AWS Secrets Manager and Parameter Store, enhancing data protection.
- Automated backups with AWS Backup and AWS RDS snapshots, ensuring data resilience and disaster recovery.
- Configured AWS VPC networking for isolated and secure container communication, enhancing system security.
- Managed ECS resources and automated deployments using AWS CLI streamlining infrastructure provisioning.

EDUCATION and CERTIFICATIONS

Old Dominion University; Bachelor of Science in Cyber Operations (May 2024)
CompTIA Security+ (06/17/2024)
AWS Certified Cloud Practitioner (Expected March 2025)
Endpoint Security Solution (ESS) Administrator 201 Certificate (9/11/2023)
Endpoint Security Solution (ESS) Advanced Administrator 301 Certificate (9/11/2023)
Assured Compliance Assessment Solution (ACAS) Certificate (10/17/2023)

Extracurricular Activities

Member of CS2A- Old Dominion University Cybersecurity Student Association 2019-Present
Member of Coastal Virginia Cybersecurity Student Association 2019-Present