

# Rodney Hall

Austin, Texas

Rodney7Hall@gmail.com | 313-433-4625 | <https://rodney-hall.github.io/cybersecurity-portfolio/>

Cybersecurity Analyst (Entry-Level) | OT/ICS Focus

## EDUCATION

---

### Master of Business Administration (MBA) – Cybersecurity Management

Davenport University

*Expected Graduation: December 2026*

### Bachelor of Science in Psychology

William Penn University

*Graduated: 2022*

## CERTIFICATIONS

---

CompTIA Security+ (CE)

AWS Certified Cloud Practitioner

Microsoft AZ-900

Industrial Control System Cybersecurity (ICS-300) – CISA / DHS

Google Cybersecurity

## TECHNICAL SKILLS

---

**Security & Monitoring:** Incident detection, triage, and escalation; log analysis and alert investigation; evidence collection and ticket-style documentation; risk assessment and threat modeling.

**OT / ICS:** IT/OT segmentation and Purdue Model alignment; OT asset inventory and risk documentation; protocol awareness (Modbus/TCP, BACnet); OT network traffic analysis using Wireshark; availability-first, non-intrusive security concepts.

**Systems & Platforms:** Windows Server and Active Directory (AD DS, DNS); Azure fundamentals including Azure RBAC and Entra ID; Red Hat Enterprise Linux (RHEL) and Linux CLI; Windows Remote Desktop; VMware.

**Tools & Technologies:** Wireshark; Jira (ticketing/workflows); McAfee (endpoint security exposure).

**Scripting / Data:** Python; SQL.

## PROFESSIONAL EXPERIENCE

---

### Mercedes-Benz Dealership – Austin, TX

December 2025 -PRESENT

#### Valet / Key Control Associate

- Logged and tracked vehicle/key inventory with high accuracy in a fast-paced environment (process-driven operations)
- Followed documented procedures and maintained detailed records to support daily readiness and auditability
- Coordinated with multiple teams under time pressure while prioritizing safety and customer experience

### The Hallway Realty – Detroit, MI / Remote

January 2023 - PRESENT

#### Real Estate Agent / Operations Lead

- Managed CRM-based workflows and maintained accurate client records; standardized processes to improve follow-up consistency
- Produced clear documentation and status updates to support team execution and operational handoffs

**Wayne State University – Detroit, MI**  
**Graduate Assistant / Football Operations**

March 2023 - March 2024

- Supported football program operations, including film breakdown, practice coordination, and data organization
- Assisted with recruiting logistics, player evaluations, and administrative tasks
- Demonstrated leadership, accountability, and decision-making in a high-pressure team environment

**Northern Illinois University – DeKalb, IL**  
**Division I Student-Athlete (Quarterback)**

January 2017 - December 2019

- Balanced full-time academic responsibilities with Division I athletic commitments
- Developed discipline, preparation habits, and performance under pressure
- Collaborated within a team-based environment emphasizing communication and accountability

---

## PROJECTS AND COURSEWORK

### OT/ICS Foundations Mini-Lab (Purdue Model & IT/OT Segmentation)

- - Mapped Purdue Model Levels 0–5 and documented IT/OT boundary controls (firewalls, OT DMZ)
- - Summarized OT risk priorities (availability and safety) and segmentation impact on blast radius reduction
- - Developed an OT incident escalation checklist covering evidence, scope, severity, and stakeholders
- - Produced a BAS/OT segmentation diagram (IT → OT DMZ → BAS management → controllers → field devices)
- - Created an OT asset inventory and risk template capturing owner, Purdue level, protocol, criticality, firmware, and remote access

### OT Network Traffic & Threat Detection (Wireshark – Modbus/BACnet)

- - Analyzed Modbus and BACnet PCAPs using Wireshark with protocol-specific display filters
- - Established baseline request/response behavior and identified abnormal indicators
- - Correlated Modbus request/response pairs to interpret command intent and device behavior
- - Captured evidence-backed screenshots and produced ticket-style findings with recommended next steps
- - Authored an OT alert triage SOP (NDR-style) covering baselining, noise vs. incident criteria, safe containment, and escalation

### Windows Server / Active Directory Fundamentals Lab

- - Built a Windows Server 2022 domain and implemented basic identity and access controls
- - Created users and groups and validated authentication activity via Windows Security logs
- - Practiced remote administration and documented repeatable access request procedures

### Security Operations Fundamentals

- - Investigated alerts and performed structured incident triage
- - Analyzed suspicious activity and mapped findings to attacker behaviors
- - Practiced reporting, escalation, and SOC-style documentation

### Phishing Email Analysis & Incident Response Lab

- - Identified phishing indicators including sender anomalies, URLs, and attachments
- - Extracted IOCs and documented incident findings and response actions

### **Google Cybersecurity Certificate Labs**

- - Conducted SIEM-style incident triage and alert investigation
- - Performed risk assessments mapping assets, threats, and vulnerabilities
- - Used Linux commands to analyze files, permissions, and processes
- - Queried datasets with SQL to identify anomalous user and network behavior