Justin R. Lew

(718) 506-6340

justinlew1000@gmail.com

LinkedIn Profile - https://www.linkedin.com/in/justinrlew/

Personal Website - https://justinrlew.github.io/index/

I'm a **cybersecurity professional** with a **B.S. in Cybersecurity and Information Assurance** and certifications including **CompTIA PenTest+, CySA+, and Security+**. I'm expanding my expertise by preparing for **CISSP, CRISC, and CEH** while also volunteering at soup kitchens to give back to the community.

I have **hands-on experience in SOC operations, IT support, and network security**, including **SIEM log analysis, threat investigation, firewall configurations, and compliance documentation** (NIST, ISO 27001, SOC 2, PCI-DSS). I've contributed to **incident response, security awareness training, vulnerability assessments, and audit support**, helping improve security workflows and compliance readiness.

Passionate about **problem-solving and cybersecurity**, I stay current on evolving threats and best practices. I'm eager to apply my **technical skills and analytical mindset** in a **collaborative security environment**.

Bachelor of Science, Cybersecurity and Information Assurance
Western Governors University, Graduate

Experience

GRC Analyst *First Horizon Bank (Nov 2024 – Feb 2025)*

- Assisted in a **security compliance project** supporting internal **SOC 2, PCI-DSS, and ISO 27001** audits, ensuring **100% audit readiness** within a **4-month engagement**.
- Conducted **third-party risk assessments** for **15+ vendors**, identifying **5 high-risk** and **10 medium-risk** security gaps, leading to remediation plans that improved vendor security postures.
- Supported **internal and external audits** by compiling **200+ compliance artifacts**, reducing audit preparation time by **30%**.
- Helped refine **incident response plans, security playbooks, and risk management reports**, improving **incident resolution times by 20%**.

- Assisted in developing **compliance documentation** and responding to **30+ customer security questionnaires**, ensuring alignment with regulatory requirements.
- Worked cross-functionally with **SOC analysts, engineering, legal, and HR teams** to enhance governance and compliance initiatives.
- Delivered **monthly security awareness training**, contributing to a **25% improvement in phishing resilience rates** based on internal simulations.
- Monitored **regulatory updates and industry trends**, providing **quarterly reports** that refined **internal compliance strategies**, reducing non-compliance risks by **40%**.

SOC Cybersecurity Analyst I *Webster Bank (May 2024 – Nov 2024)*

- **Monitored and analyzed** over **10,000 security alerts per month** using **SIEM tools** (Splunk, QRadar, Microsoft Sentinel), reducing false positives by **25%** through improved filtering and rule tuning.
- Conducted **triage and investigation** of **100+ security incidents**, escalating **30+ critical threats** that led to **zero data breaches during tenure**.
- Investigated **unauthorized access attempts, malware detections, and suspicious network activity**, improving incident containment times by **35%**.
- Assisted in **incident response efforts**, supporting **5 major security incidents**, helping contain threats within **2 hours on average**, exceeding the company SLA of **4 hours**.
- Performed **weekly vulnerability scans**, identifying **50+ vulnerabilities**, with **90% remediation rate** in collaboration with IT teams.
- Maintained and reviewed **daily security logs**, identifying **8 recurring security misconfigurations**, leading to targeted policy updates that reduced repeat incidents by **20%**.
- Provided **detailed security reports** on **100+ security events**, ensuring compliance with regulatory and governance requirements, reducing compliance violations by **15%**.
- Assisted GRC teams by **mapping security events to compliance frameworks**, improving audit response efficiency by **30%**.
- Helped refine **incident response playbooks**, reducing incident triage time by **20%**, leading to faster response times and enhanced security posture.
- Participated in **security awareness programs**, helping train **200+ employees** on phishing detection, leading to a **20% improvement in phishing detection rates** in simulated tests.

Network & Security Operations Specialist *SUNY Security Operations Center SOC (Dec 2023 – May 2024)*

- Monitored **situational security** by gathering intelligence from internal and external sources, correlating data for real-time threat detection.
- Conducted **risk analysis on security threats** (weather events, geopolitical issues, cyber incidents) impacting corporate operations.
- Assisted in **firewall configurations, intrusion detection/prevention**, and network security monitoring.
- **Created reports on potential risks**, advising security teams on **incident mitigation strategies**.

IT Support Specialist *Queens Library (Aug 2023 – Dec 2023)*

- Provided **technical support to security teams**, ensuring **secure access to monitoring tools and SOC platforms**.
- Monitored **access control systems, security logs, and endpoint protection software**, identifying anomalies in user activity.
- Assisted in **security awareness training on phishing detection**, reducing social engineering incidents by 20%.

Help Desk Technician Tier 1 *Community Healthcare Network (May 2023 – Aug 2023)*

- Provided compassionate and patient **customer service** by delivering technical assistance to employees in an approachable manner.
- Offered compassionate and professional **technical support across live chat, email, and phone channels.**
- Supported **onboarding** processes, ensuring seamless access to company systems
- Assisted with basic **troubleshooting** tasks, such as **resetting passwords** and helping users navigate software applications.
- **Escalated** more complex technical problems to senior team members or Tier 2 support.

Certifications

- ISC2 CCSP: Certified Cloud Security Professional (August 2024)
- CompTIA PenTest+ (August 2024)
- Cisco Certified Network Associate (CCNA) (November 2024)
- Cisco Certified Support Technician (CCST) (July 2024)
- CompTIA CySA+ (June 2024)
- AWS Certified Cloud Practitioner (May 2024)

- CompTIA Project+ (April 2024)
- Google Associate Cloud Engineer (March 2024)
- ISC2 SSCP: Systems Security Certified Practitioner (February 2024)
- Microsoft Certified: Azure Fundamentals (AZ-900) (December 2023)
- LPI Linux Essentials (December 2023)
- ITIL 4 Foundation - IT Service Management (October 2023)
- CompTIA Security+ (October 2023)
- CompTIA Network+ (September 2023)
- CompTIA Cloud Essentials+ (August 2023)
- CompTIA A+ (July 2023)
- CompTIA IT Fundamentals (ITF+) (June 2023)

Key Skills & Technical Proficiency

Programming & Security Technologies

- **Languages:** Python, SQL, Bash, PowerShell, HTML, CSS, JavaScript
- **SIEM & Monitoring:** Splunk, Microsoft Sentinel, QRadar, Elastic Stack (ELK)
- **Threat Intelligence & Incident Response:** Cortex XSOAR, AlienVault OTX, VirusTotal, Hybrid Analysis, MISP
- **Network & Endpoint Security:** Palo Alto, Cisco ASA, Fortinet, CrowdStrike Falcon, SentinelOne, Microsoft Defender ATP
- **Firewalls & Intrusion Detection:** pfSense, Cowrie, IDS/IPS, VPNs
- **Vulnerability & Exploitation:** Metasploit, Nessus, OpenVAS
- **Authentication & Password Security:** Hydra, John the Ripper, Hashcat

GRC, Risk, & Compliance

- **Frameworks & Standards:** NIST 800-53, NIST 800-61, ISO 27001, SOC 2, PCI-DSS, MITRE ATT&CK, CIS Controls, GLBA
- **Risk & Policy Management:** Security Audits, Compliance, Incident Response, Risk Assessment, Policy Development
- **GRC Platforms:** Archer, ServiceNow GRC

Security Operations & Crisis Management

- **Incident Response & Threat Intelligence:** Risk Assessment, Escalation, Crisis Management Coordination
- **Security Awareness & Compliance:** Phishing Simulations (GoPhish), Threat Reporting, Training Programs

- **Cross-Team Collaboration:** Executive-Level Briefings, Global Intelligence Monitoring, Real-Time Threat Analysis

Documentation & Reporting

- **Platforms:** Confluence, SharePoint, Lucidchart, Visio
- **Network Monitoring & Analysis:** Wireshark, Nmap

Projects

1. **GRC Governance, Risk, and Compliance Projects**

These projects showcase hands-on experience in security policy development, risk assessment, compliance, and security audits.

GitHub Repository - https://github.com/JustinRLew/GRC-Governance-Risk-and-Compliance

---

2. **SOC Technical Writing Projects**

Created clear and organized technical documents for SOC (Security Operations Center) processes, helping make cybersecurity protocols easier to understand and use.

GitHub Repository - https://github.com/JustinRLew/SOC-technical-writing-projects

---

3. **Windows Active Directory Virtual Lab**

This project demonstrates the deployment and management of an Active Directory environment in a virtual lab. It includes setting up a domain controller, configuring DNS, managing users and groups, implementing Group Policy Objects, and integrating a client machine.

GitHub Repository - https://github.com/JustinRLew/Active-Directory-Virtual-Lab

---

4. **Remote Desktop Protocol (RDP)**

This project shows my ability to assist users in setting up and troubleshooting three popular remote desktop tools:

- Microsoft Remote Desktop Protocol
- Chrome Remote Desktop
- TeamViewer

GitHub Repository - https://github.com/JustinRLew/Remote-Desktop-Protocol-Project

---

5. **Phishing Simulation Tool**

This project involves building a phishing simulation tool using a custom HTML front-end interface, SendGrid, a Python Flask backend API, and Postman for testing API requests to demonstrate phishing attack methodologies.

GitHub Repository - https://github.com/JustinRLew/Phishing-Simulation-Tool

---

6. **Brute-Force Attack Simulation**

This project is a Python-based brute force attack simulation that demonstrates how brute force attacks work. The script attempts to guess passwords by hashing and comparing them to a stored hash.

GitHub Repository - https://github.com/JustinRLew/Brute-Force-Attack-Simulation

---

7. **Honey Pot – Creation & Deployment**

This project involves setting up a medium-interaction SSH honeypot using Cowrie to detect and analyze unauthorized login attempts (particularly brute-force attacks). The honeypot logs attacker behavior and provides insights into the threat landscape.

GitHub Repository - https://github.com/JustinRLew/Honey-Pot-Creation-and-Deployment

---

8. **SIEM Monitoring with Splunk**

This project demonstrates the implementation of a Security Information and Event Management (SIEM) system using Splunk. The purpose of the project is to monitor a simulated network, detect security threats, and respond to incidents in real-time.

GitHub Repository - https://github.com/JustinRLew/SIEM-Monitoring-Splunk

9. **Personal Firewall & Network Monitoring**

This project demonstrates how to configure a personal firewall and monitor network traffic on a Windows system. Windows Defender Firewall, PowerShell, Wireshark, and Nmap were used.

GitHub Repository - https://github.com/JustinRLew/Personal-Firewall-and-Network-Traffic-Monitoring

---

10. **Password Strength Checker**

Created a web-based password strength checker that evaluates passwords in real-time based on NIST guidelines. It provides visual feedback, displays password strength, and offers recommendations for improving password security.

GitHub Repository - https://github.com/JustinRLew/Password-Strength-CheckerPassword Strength Checker

Password Strength Checker App - https://justinrlew.github.io/Password-Strength-Checker/

---

11. **ServiceNow Workflow Project**

This project uses ServiceNow to create workflows for an IT Help Desk environment. It showcases automated incident workflows, a self-service portal, email notifications, reporting dashboards, and incident assignment rules.

GitHub Repository - https://github.com/JustinRLew/ServiceNow-project

---

Languages

English • Spanish • Chinese