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 motivated cybersecurity professional with a Bachelor of Science degree in Cybersecurity and Information Assurance and certifications including CompTIA PenTest+, CySA+, and Security+. In addition to preparing for certifications like CISSP, CISA and CRISC , I spend my free time volunteering at soup kitchens to help serve the community.

I have hands-on experience in SOC operations, IT support, and network security, where I've written incident reports, enhanced documentation workflows, and maintained compliance with NIST, ISO 27001, SOC 2, and PCI-DSS. I've contributed to security awareness programs, SOC playbooks, vulnerability assessments, and network monitoring to strengthen security operations.

My experience includes firewall configurations, SIEM log analysis, endpoint security, and troubleshooting network vulnerabilities. I stay current on cybersecurity regulations while delivering high-quality work and excellent service. Passionate about problem-solving and cybersecurity, I'm eager to contribute my skills to a dynamic team environment.

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

Experience

SOC Technical Writer *First Horizon Bank (Nov 2024 – Feb 2025)*

- **Monitored and analyzed** security events using SIEM tools (Splunk, QRadar, Microsoft Sentinel) to **triage potential threats** and escalate critical incidents.
- Developed **incident reports, security playbooks, and crisis response documentation**, aligning with NIST 800-61 and ISO 27001.
- Assisted in **real-time threat intelligence gathering** to **assess risks impacting corporate security** and employee safety.
- **Facilitated crisis communication** by coordinating internal updates and escalating high-priority incidents to executive leadership.

- Maintained compliance documentation for **SOC 2, PCI-DSS, and GLBA audits**, ensuring adherence to regulatory security requirements.

SOC IT Security *Webster Bank (May 2024 – Nov 2024)*

- **Monitored security incidents** using SIEM and threat intelligence platforms, analyzing event logs to detect suspicious activity.
- Responded to **emerging threats, vulnerabilities, and cyber incidents**, assisting in **incident containment and resolution**.
- Provided **logistical support for crisis management teams**, including conference call coordination, exercise facilitation, and security updates.
- Assisted in **travel security operations**, ensuring corporate employees received real-time threat intelligence during international travel.
- Developed **incident escalation procedures**, improving security response times by 30%.

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