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+** !

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)*

- Developed and standardized **SOC documentation**, including **incident response playbooks, security runbooks, and compliance reports**, aligning with **NIST 800-61, ISO 27001, and FFIEC guidelines**.
- Created structured **security incident reports** for SOC analysts and executive leadership, leading to a **30% improvement in post-incident analysis efficiency**.
- **Optimized knowledge management systems** by implementing **Confluence, SharePoint, and Jira**, cutting down **information retrieval time by 40%** and increasing analyst productivity.

- Partnered with **SOC analysts and security engineers** to document **SIEM configurations** (Splunk, QRadar, Microsoft Sentinel) and **log management procedures**, strengthening log correlation accuracy.
- Maintained up-to-date **security policies and compliance documentation** for **SOC 2, PCI-DSS, and GLBA audits**, contributing to a **100% compliance pass rate** and reducing financial risks.
- Enhanced **security awareness training materials** on **phishing prevention, social engineering, and secure coding**, leading to a **15% increase in training completion rates** among employees.
- Provided documentation for **security automation workflows (SOAR)** to streamline **incident response processes**, which helped **reduce mean time to respond (MTTR) by 20%**.

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

- **Provided IT support to SOC analysts**, managing secure access to **SIEM tools, firewalls, and forensic applications**, reducing ticket resolution time by **30%**.
- **Documented SOC workflows, security incidents, and system configurations**, improving knowledge transfer and reducing repeat issues by **40%**.
- **Assisted in endpoint security** by deploying and monitoring **EDR solutions (CrowdStrike, Microsoft Defender ATP, Carbon Black)**.
- **Supported firewall configurations and log analysis** for financial data protection, working with **Palo Alto, Cisco ASA, and Fortinet firewalls**.
- **Troubleshot VPN, MFA, and secure access issues** for SOC personnel, ensuring uninterrupted remote monitoring and response.
- **Developed compliance documentation** and security procedures, aligning with **ISO 27001, PCI-DSS, and SOC 2 standards**.
- **Assisted in security awareness training** on phishing detection and data security, contributing to a **20% reduction in phishing-related incidents**.

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

- **Configured and monitored enterprise firewalls, IDS/IPS (Palo Alto, Cisco Firepower, Snort), and VPNs**, improving **threat detection accuracy by 15%**.
- **Ensured proper log collection and SIEM integration (Splunk, Microsoft Sentinel, QRadar)**, reducing **false positives by 25%**.
- **Conducted network traffic analysis** using **Wireshark, Zeek, and NetFlow** to identify anomalies and escalate security threats.
- **Performed vulnerability scans with Nessus and OpenVAS**, helping reduce **critical vulnerabilities by 20%** through documented remediation efforts.

- **Developed network security documentation**, including **topology diagrams, firewall rules, and SOC best practices**, improving troubleshooting efficiency by **40%**.
- **Assisted in security hardening measures** for SOC workstations and lab environments, reducing misconfigurations by **30%**.
- **Wrote SOC playbooks and incident response procedures**, improving onboarding efficiency for new interns and junior staff.

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

- Responded to over 30 daily user inquiries via phone, email, and ticketing systems, earning a **95% CSAT** rating.
- Diagnosed and **resolved** network, software, and hardware issues, ensuring optimal system performance.
- Provided excellent **customer service** by explaining technical solutions in simple, user-friendly terms, achieving a 95% customer satisfaction rating.
- Improved customer confidence by simplifying technical concepts into clear, **user-friendly** explanations.

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

Certification	Date
CompTIA PenTest+	August 2024
ISC2 CCSP: Certified Cloud Security Professional	August 2024

CompTIA CySA+	June 2024
CompTIA Security+	October 2023
CompTIA Project+	April 2024
CompTIA Network+	September 2023
CompTIA A+	July 2023
ITIL 4 Foundation - IT Service Management (GR671577319JL)	October 2023
ISC2 SSCP: Systems Security Certified Practitioner	February 2024
LPI Linux Essentials	December 2023

Extracurricular Activities	Cyber Club Member: Actively participated in discussions and practiced hands-on cybersecurity concepts
Awards & Achievements	Excellence Award: Awarded for exemplary work in Managing Information Security coursework

Technical/Soft Skills

Programming Languages	Python, SQL, Bash, PowerShell, HTML, CSS, JavaScript
Customer Support & Ticketing Tools	Zendesk, ServiceNow, Jira Service Management
Productivity Tools	Microsoft Office
Customer Support Metrics	**Customer Satisfaction Score (CSAT):** ● Consistently maintained a CSAT rating of 90% through attentive and solution-oriented support. **First Response Time (FRT):**

	• Achieved an average first response time of 3 minutes for live chat inquiries. **Resolution Time:** • Resolved 80% of tickets within the same business day, improving overall user experience. **Ticket Volume Handled:** • Managed 25+ live chat and email inquiries daily while maintaining service quality. **Escalation Rate:** • Minimized ticket escalations to senior support to under 10% by providing accurate first-contact solutions. **Knowledge Base Contributions:** • Created 5 knowledge base articles to address recurring issues, reducing related inquiries by 10%. **Accuracy in Resolutions:** • Delivered correct solutions 95% of the time on the first response. **Feedback Implementation:** • Collaborated with the team to incorporate user feedback, reducing recurring issues by 15%.

Tools/Technologies

User and Identity Management	Active Directory (AD), Okta, LDAP (Lightweight Directory Access Protocol), Duo Security

Ticketing and Helpdesk Systems	ServiceNow, Jira Service Management, Zendesk, Freshdesk, Spiceworks
Remote Access and Troubleshooting	TeamViewer, Microsoft Remote Desktop, Chrome Remote Desktop, LogMeIn, AnyDesk
Virtualization and Cloud Management	VMware vSphere, Hyper-V, AWS Management Console, Microsoft Azure Portal, Spiceworks
Endpoint and Device Management	Microsoft Intune, Jamf, PDQ Deploy

Documentation & Reporting	Confluence, SharePoint, Lucidchart, Visio
Security & Compliance Frameworks	NIST 800-61, ISO 27001 SOC 2, PCI-DSS, MITRE ATT&CK, CIS Controls
Network Monitoring & Analysis	Wireshark, Nmap
Network & Endpoint Security	Palo Alto, Cisco ASA, Fortinet, CrowdStrike Falcon, SentinelOne, Microsoft Defender ATP
Threat Intelligence & Incident Response	Cortex XSOAR, AlienVault OTX, VirusTotal, Hybrid Analysis, MISP
Firewall & Intrusion Detection	pfSense, Cowrie
Vulnerability Scanning & Exploitation	Metasploit, Nessus, OpenVAS
SIEM	Splunk, Microsoft Sentinel, QRadar, Elastic Stack ELK
Password Cracking & Authentication	Hydra, John the Ripper, Hashcat
Phishing & Security Awareness	GoPhish, Have I Been Pwned

Projects

1. **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

---

2. **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

---

3. **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

---

4. **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

---

5. **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

---

6. **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

---

7. **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

---

8. **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

---

9. **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/

---

10. **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