Eric Passeno

Portfolio: Eric Passeno | Cybersecurity | GitHub: eric-cyber-git · GitHub

---

SUMMARY STATEMENT

CISSP-certified Cyber Defense Analyst with 5+ years in IT and nearly two years leading threat detection and response efforts. Specializes in SIEM, endpoint telemetry, and automation to monitor and mitigate risks in dynamic enterprise environments. Proven ability to fortify infrastructure and safeguard data by leading detection strategy, centralizing tool ownership, and collaborating cross-functionally to build resilient cyber defense architectures.

Certifications

- CISSP (July 2025)
- Trellix ENS Expert Rules Learners Course (April 2024)
- CompTIA Security+ (January 2023)
- CompTIA Network + (July 2023)
- ISC2 Certified in Cyber Security (December 2022)

Technical Skills

- SIEM (Splunk, Log Forwarding, Correlation)
- IDS/IPS, SOAR, EDR
- Detection Engineering & Log analysis
- Data Loss Prevention (DLP)
- API Security & Automation
- Threat Monitoring & Incident Response
- Digital Forensics
- Scripting & Programming (Python, PowerShell)
- Identity Access Management (IAM)
- Cross-Team Security Collaboration
- Governance Frameworks: NIST CSF, NIST SP 800-171, CMMC, CIS Controls

Leadership Scope

Drive continuous improvement of security operations through automation, simulation exercises, and stakeholder feedback. Regularly engage in security readiness activities and champion knowledge sharing across departments.

PROFESSIONAL EXPERIENCE

IT Security Analyst, October 2023 - Current
Williams International, Pontiac, MI
Major duties include:

- Support Data Loss Prevention (DLP) and Insider Risk mitigation efforts by analyzing data movement, access patterns, and endpoint telemetry across Windows environments.
- Spearhead cyber threat monitoring and incident response across enterprise Windows environments, applying MITRE ATT&CK to drive correlation and visibility.

- Leverage endpoint and network telemetry to detect suspicious data access and movement, enhancing insider threat visibility and DLP posture.
- Manage security data pipelines by connecting systems via APIs and log forwarding (e.g., syslog), enabling aggregation and event correlation in the SIEM. Routinely develop Python workflows that query SQL data, parse and enrich results, and feed output into detection and response automations.
- Act as centralized owner of key security tools including SIEM, EDR, and automation platforms, driving roadmap, deployment strategy, and day-to-day optimization.
- Led threat detection and response efforts, including incident triage, forensic analysis, and attacker timeline reconstruction using Sysinternals and event artifact correlation.
- Develop REST API automations and Python scripts to enrich threat intelligence and enable near instant response actions, minimizing analyst overhead and accelerating detection-to-response cycles.
- Stay abreast of emerging threats and attacker tradecraft to evolve detection logic and enhance cyber resilience.
- Perform system administration of security tools, generate security content, drive tool capabilities, and ensure operational excellence.
- Develop threat hunt hypotheses using MITRE ATT&CK and emerging TTPs to proactively uncover hidden threats.

Macomb Community College | Computing Tech | March 2023 – October 2023

- Make use of scripting and automation to reduce overhead and increase efficiency while improving the reliability of information systems.
- Ensure that computers are deployed with secure configurations using CIS controls and other industry best practices to inform configuration selections.

Centaris | IT Systems Technician | March 2022 – March 2023

- Manage Identity lifecycle for users by creating new user accounts and provisioning access following principle of least privilege.
- Performed periodic access reviews and account removal following established procedures.
- Supported and contributed to security patching for software and hardware, typically in response to a known exploit.
- Performed routine admin tasks within O365 Admin Portal while supporting hybrid and cloud environments.

HTC Inc | Service Desk Team Lead | May 2021 – April 2022

- Drafted and implemented secure support policies (e.g., password resets, access escalation) to enforce least privilege.
- Performed routine user audits to ensure that processes and procedures surrounding PII and PHI where being followed. Present findings that are concise and effective to senior leadership and stakeholders.

HTC Inc | Service Desk Analyst | June 2019 – May 2021

- Escalated and diagnosed high-volume incident trends through root cause analysis and team collaboration.
- Supported business-critical software rollouts and trained end users to ensure smooth adoption.

KEY PROJECTS & CONTRIBUTIONS

- Engineered and developed a Python automation leveraging regex and SQL to analyze VPN logs in real time to auto mitigate brute force activity with nearly 100% true positive and 0 false positives.
- Created PowerShell scripts to automate forensic artifact collection from Windows hosts, and a companion Python parser to generate a centralized, analyst-ready incident workbook which enabled quick assessment of insider risk scenarios and data movement investigations.
- Self-trained in our EDR's scanning engine to author and deploy nearly 100 custom behavior-based signatures mapped to MITRE ATT&CK, significantly enhancing endpoint visibility and threat detection coverage.
- Designed and deployed Privileged Access Management controls aligned with Zero Trust principles to reduce insider threat risk.
- Assumed ownership of Trellix EDR, SIEM, and IAM tools, defining strategic roadmaps and optimizing configurations to maximize signal fidelity, coverage, and operational efficiency.
- Led post-incident review cycles and incorporated feedback into threat detection tuning, enhancing accuracy and incident handling efficiency.
- Supported vulnerability management program through log analysis, prioritization workflows, and tuning in Rapid7 InsightVM; collaborated with IT to remediate critical findings and improve asset coverage.
- Led PoCs for log aggregators, SIEMs, and SOAR platforms to evaluate and mature the security stack through hands on testing and data-driven comparison.
- Partnered with Systems Development Team to determine the most effective and efficient method for bot mitigation on our web applications.

EDUCATION

Bachelor of Science - Information Technology, Dec 2023
Walsh College, Troy, MI | GPA: 3.78
Associate of Applied Science - Network Security, May 2019
Macomb Community College, Warren, MI | GPA: 3.3