Eric Phillpott

Email: Eric@Phillpott.com

linkedin.com/in/ephillpott

Experience

- **Security Analyst** — San Diego, CA
  Own Company (Formerly OwnBackup) — *June 2023 – Present*
  - **Vulnerability Management**: Reduced operational costs by $130K annually by developing and implementing a custom-built SAST solution.
  - **Data Analysis**: Leveraged statistical analysis and data science expertise to support the development of a cross-functional user access review workshop, resulting in more efficient access control management.
  - **SIEM Implementation**: Designed and implemented an event monitoring solution using the Elastic stack and Python to analyze high-volume log data and ensure comprehensive security monitoring.
  - **Security Automation**: Developed custom Apex security policies to automate DLP-related threat response capabilities, allowing for proactive identification and remediation of potential security incidents.
  - **Software Engineering**: Collaborated with cross-functional teams to implement a new Secure Scoring algorithm and Security Insights dashboard, improving threat detection and response capabilities by providing actionable insights into security events.
- **Cybersecurity Analyst** — Santa Clara, CA
  MapR — *November 2017 – August 2019*
  - **Security Governance**: Implemented a comprehensive infrastructure security program that improved security posture across endpoints, infrastructure, and SaaS applications.
  - **Log Analysis & Automation**: Developed Python-based automation for log collection and analysis, integrating data from diverse systems into an Elastic SIEM to establish a single source for security monitoring.
  - **Incident Response**: Led the detection, containment, and remediation of a security incident involving Dridex malware as Incident Commander, developing new incident response procedures that reduced incident resolution time by 15%.
  - **Threat Intelligence**: Collaborated with executive leadership to implement machine learning solutions for network traffic analysis, enhancing threat detection accuracy and network performance.
- **IT Security Analyst** — San Diego, CA
  FightersMarket.com — *March 2014 – October 2017*
  - **SIEM Implementation**: Developed and implemented a security analytics platform using the ELK stack to improve threat detection and response capabilities.

Education

- **B.S Computer Science** — San Francisco, CA
  San Francisco State University — *2023*

Skills

- **Security Operations**: SIEM Platforms (Splunk, Elastic), SOAR(Cortex, QRadar), Incident Response, Threat Detection (Security Onion, Suricata, OSSEC, YARA, VirusTotal)
- **Data Analysis & Log Management**: Rsyslog, Sysmon, CloudTrail, Windows Event logs, Firewall, EDR, Jupyter Notebooks, Apache Spark, Apache Hadoop, MatplotLib, Apache Drill, Databricks, Nessus/Tenable
- **Compliance**: PCI-DSS, FedRAMP (Moderate), HITRUST, ISO 27001, NIST CSF
- **Programming & Automation**: Python, Go, Terraform, SQL
- **Cloud Security**: Amazon Web Services (AWS), Google Cloud (GCP)