Jeff Holland - Senior Security Engineer

https://jeff-a-holland.github.io - jeff.a.holland@gmail.com

Skills

Programming: Python (Functional/OO), Powershell, Perl, Bash, RegEx

Other: Git/GitHub, REST APIs, Security Architecture, JIRA, Confluence

Cloud: Amazon AWS (EC2, Lambda/Chalice, SES, SecretsManager, IAM)

SIEM: Splunk, Exabeam, QRadar, SumoLogic, MicroFocus/ArcSight ESM

Vulnerability Analysis: Tenable IO, Tenable SC, AWS Inspector

Networking: TCP/IP, TCPdump, Netflow

EDR: Crowdstrike, CarbonBlack (Response/Protect), SentinelOne

Operating Systems: Linux, Windows, Mac OSX

Forensics: FTK

Misc: Security Metrics (RSA Archer), Security Compliance Frameworks (ISO 27001, SOC2 Type II, HIPAA)

Certifications

CISSP #53589 - **GPYC** Current - **GCUX** Current

Publications

SANS GIAC Gold Papers:

GPYC- Python Coder

GCUX - Linux/UNIX Security Administration

GCIH - Hacker Exploits and Incident Handling

GCIA - Intrusion Detection

GitHub:

Chaining Vulnerability Scans in Tenable IO Using Python

HP Protect Conference Presentations:

Extraction and Long Term Storage of ArcSight ESM Connector Statistics

Leveraging APT Indicator Feeds with Enterprise SIEM

Work Experience

Balyasny Asset Management - Chicago, IL - (Sept 2020 - Present) Sr. Security Engineer

- Software Development (Python and Powershell)

- SIEM content development and administration

- Vulnerability management automation

- Cloud (Use of AWS Lambda/Chalice for running serverless automation code)

Baker & Mckenzie - Chicago, IL - (Feb 2017 - Aug 2020) Security Architect (SOAR)

- Migrated on-prem Vulnerability Assessment application (Tenable SC) to the cloud-based version (Tenable IO). Utilized the REST API to fully automated creation, deletion and updates of all resources using Python playbooks for a global enterprise of 20,000+ assets and 200+ scan definitions.

- Wrote Python scripts to pull data from the Tenable IO and SC, parse based on office location/application, and create tickets for system owners where the systems were in scope for ISO 27001. Application kept a state table to prevent duplication of tickets, and removed entries from the state table based on PluginID and IP address once the vulnerability was mitigated.

- Wrote Python scripts to pull data from the vulnerability assessment application and report severity metrics for all repositories in the enterprise. Automated creation of a quarterly report in Excel format using the Python Library XLSXWriter.

 - Created and maintained a security metrics schema for all security products in their native format. Metrics were parsed with Python scripts into the common schema and imported into the GRC application for visualization and analysis.

- Federated single-server SIEM deployment (QRadar) to have multiple-appliance architecture.

Civis Analytics - Chicago, IL - (Aug 2015 - Feb 2017) Security Engineer

- Lead all security and compliance projects while embedded in the DevOps team.

- Chose and deployed security technologies to product company data and ensure SOC 2 Type II certification, including: SumoLogic (Log Consolidation and Analysis), SentinelOne (EDR), OSSEC (HIDS), AWS Inspector (Cloud Vulnerability Analysis), Nessus (On-Prem Vulnerability Analysis), and JAMF Pro (Endpoint Security Policy Enforcement).

- Served as the primary interface for all clients concerning security, audits, compliance questionnaires, etc. Lead the effort to obtain SOC 2 Type II certification.

Emmi Solutions - Chicago, IL - (2014 - 2015) Security Engineer

- Utilized AlienVault SIEM and OSSEC to monitor for incidents.

- Interfaced with clients on security audits and questionnaires. Worked with General Counsel on security-related initiatives.

HCSC (BC/BS of IL, TX, NM, OK, MT) - Chicago, IL - (2013 - 2014) Security Architect (SIEM)

- Security architect with enterprise responsibility for the ArcSight ESM deployment.

- Wrote custom connector parsers, added new log feeds, and interfaced with SOC team on SIEM updates and requests.

Leidos/SAIC - Chicago, IL/San Diego, CA - (2011 - 2013) Sr. Security Engineer

- Administered ArcSight ESM, including: Writing custom connectors and add new log feeds as new clients were on-boarded. Occasional consulting on ArcSight to clients of the MSSP business unit at Leidos.

- As part of a two-person project team, migrated a multi-terabyte ArcSight ESM Oracle instance to new hardware using SQL and Perl scripts.

Northwestern University - Evanston, IL - (2007 - 2011) Security Vulnerability Analyst

- Created and operated the vulnerability analysis program used as a resource to any University department that required assistance.

- Wrote a custom threat intelligence application in Perl to use threat intelligence signatures and Netflow and NAC logs to identify malware infected hosts on campus.

ArcSight, Chicago - IL/Cupertino, CA - (2005 - 2007) Security Consultant

- Security consulting on ArcSight ESM installation, administration, customization and training to customers.

Invacare - Elyria, OH - (2004 - 2005) Network Engineer

- Various network engineer duties (switching, routing, etc). Wrote custom code in Perl to automate the auditing of enterprise switches for switch-port to hostname assignments.

Raytheon - Garland, TX - (1996 - 2004) Sr. Security Engineer / Software Developer

- Various security engineering duties to include: Log analysis, intrusion detection, security architecture, security product evaluation

- Software developer in the algorithms optimization group

Education

Master of Science (M.S.), Mathematics, New Mexico State University (1996)

- Coursework in Algebra, Real and Complex Analysis, Statistics, Linear Programming - Emphasis in Linear Programming and Optimization

Bachelor of Science (B.S), Mathematics, California State University, San Marcos (1994)

- Coursework in Algebra, Analysis, Discrete Mathematics, Statistics and Probability, Number Theory, C Programming, Unix