Resume of **Tracy R Reed**

CISSP, CMMC CCP, CCSK, RHCE, ATP
resume@tracyreed.org
https://calendly.com/tracyreed/ https://www.linkedin.com/in/tracyrreed/ https://github.com/tracyreed
Video resume: https://bit.ly/47rFQoV

CCA exam pending
§170.11(b)(10) lead CCA requirements met:

- 27 years of cybersecurity experience
- Management: Cofounded Detexian, Owner of Copilotco LLC for 9 yrs, Unrisk for 4 yrs
- Many years of assessment and audit experience via Copilotco, Unrisk, Splunk, etc
- CISSP is a foundational qualification aligned to Advanced Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role

KEY ACCOMPLISHMENTS:

- Secured medical devices to IEC-62443 and managed External Attack Surface/Third Party Risk project with the Palo Alto Networks Xpanse product for **Kaiser Permanente**
- Secured Industrial Control Systems (ICS)/Operational Technology (OT)/SCADA/IoT per NIST SP-800-82, IEC-62443, and MITRE ATT&CK/D3FEND for Oakwest, Maverick Natural Resources, Northwest Natural
- Accepted into Toptal.com (screens for top 3% of applicants)
- Helped Splunk reach their cloud vulnerability management SLA for first time
- Co-founded Detexian, designed/built event-based IDS, won $560k VC funding
- Secured Docker/Kubernetes containers, gave presentations on container security with Twistlock
- Secured Amazon AWS Cloud environment to achieve SOC 2 type 2 certification
- UCSD Instructor: UNIX & Linux Security Fundamentals CSE-41272 and others
- Built SELinux policy using MCS/TE to fully confine a major “cloud” hosted Internet application. 45,000 web application instances confined with SELinux.
- Key participant in achieving FISMA/FedRAMP certification at ServiceNow
- Designed and deployed secure Private Cloud system with Ceph/OpenStack and Puppet/Ansible automation to provide security, high availability, and efficiency at Copilotco
- Extensive experience with system security monitoring via custom log analysis tools including Splunk and Elasticsearch/Logstash/Kibana

EMPLOYMENT HISTORY

Unrisk Inc. **Apr 2020 – Present**

Security Architect

Providing security architecture services to **PricewaterhouseCoopers, Databricks, Splunk, Kaiser Permanente, Maverick Natural Resources, Northwest Natural**

- Secured OT/ICS natural gas metering infrastructure for Northwest Natural, an Oregon utility company.
- Secured OT and assisted vulnerability management program and wrote vulnerability management policy for Maverick Natural Resources, a Texas-based oil and natural gas operations company.
- Ran vulnerability and risk management programs to provide cloud and container security tools and services for consumption by the larger organization.
- Work with Twistlock, Sysdig for monitoring and vulnerability mitigation of containers, Docker, Kubernetes at Kaiser Permanente.
- Implemented DevSecOps methodology in deployment pipelines with Azure DevOps at PwC
- Harden AWS and Azure cloud environments per CIS benchmarks, NIST, and best practices.
- At Databricks managed vendor and supply chain risk, evaluate security questionnaires, work with vendors to assure compliance.
- Secure IOT/ICS/OT per NIST SP-800-82, IEC-62443, for a manufacturing operation.
- Vulnerability management with Sysdig and Operationalized external attack surface management with Palo Alto Xpanse at Kaiser Permanente.
- Hosted infrastructure and managed compliance program for customers such as Resume Rabbit (PCI) and

MedicFusion (HITRUST/HIPAA).

- 2 year contact at Splunk where I wrote and administered the Splunk Cloud Risk Register Policy
- Performed enterprise-wide technology risk assessment and gap analysis of Splunk for the purposes of ransomware risk mitigation and corresponding decrease in cybersecurity insurance policy premium.
- In 5 months achieved full compliance with SLA for vulnerability management for the first time in the history of Splunk Cloud.

Trace3 **Jan 2019 – Mar 2020**

Cloud Security Architect

Customer facing security program consulting and leadership role providing world-class solutions for major corporations.

- Pre-sales and technical delivery of cloud security programs, solutions, security controls matrices, security solutions research, policy writing, cloud hardening (Azure and AWS), container life cycle security, gap analysis, directing technical teams to implement the security program as I defined it.
- Clients included PIMCO (AWS migration), Loan Depot (NIST/CIS/NYDFS500/PCI compliance in Azure), NetApp (security architecture for their next gen datacenter design).

Detexian **Jun 2018 – Nov 2018**

CTO

Designed and built the Detexian event based cyber threat detection system.

- Designed and implemented all IDS heuristics.
- Lead small team working with ElasticSearch, Hadoop, Spark, Logstash, Django, Python. Based in Melbourne, Australia.

Twistlock **Oct 2017 – May 2018**

Security Architect

Help customers architect their container security infrastructure and deploy Twistlock security software.

- Daily meetings with major corporation security departments, training/teaching, container security implementation.
- Docker, Kubernetes, OpenShift, Google Cloud, Amazon AWS, etc.

InVision **Nov 2015 – Oct 2017**

Sr. Security Engineer

Built security program to secure Amazon AWS environment for PCI and SOC type 2.

- Passed examination by Schellman audit firm to meet customer requirements which enabled sales.
- Built security program, conducted risk assessment, wrote policy, direct DevOps in systems hardening, network ACLs, patching. Implemented HIDS and SIEM using osquery, AlienVault USM for AWS.
- Monitored cloud environment with Cloudcheckr. Conduct quarterly access/entitlement reviews, firewall ACL reviews, etc.

ServiceNow **Oct 2011 – Nov 2015**

Sr. Security Engineer

Confined 45,000 instances of the sole revenue producing software product for publicly traded $12B company with SELinux.

- Supported PCI/HIPAA and FISMA/FedRAMP compliance programs with audit tools, audit support, security controls, logging infrastructure and analysis, system hardening.
- Collaborated with auditors to provide evidence of compliance. Negotiated remediations.
- Built security log review dashboard, assisted systems engineering team in building out many datacenters with complete set of security controls.
- Implemented Sourcefire IDS, Safenet key management, SED/LUKS full disk encryption, terabyte Splunk architecture, Exceedium Xsuite bastion hosts, log forwarding infrastructure, deployed OSSEC host-based intrusion detection system. Extensive documentation, IQOQ for healthcare, audit support.
- Won excellent quarterly bonuses and an award for security support in deploying new datacenters worldwide.

Edirect Publishing **May 2009 – Oct 2011**

Sr. Security Engineer

Led PCI compliance effort successfully implementing SAQ-C for ecommerce company.

- Wrote company security policy. Implemented customer SELinux security policies to confine proprietary applications.
- Implemented automated log analysis software to detect intrusion attempts and block them in real-time.
- Successfully thwarted a concerted effort by a team of attackers unknown to break into the company over a period of two years.
- Selected hardware for refresh, migrated old unsupported systems to CentOS virtualized Xen environment.
- Deployed 75+ virtual machines on universally available and PCI compliant infrastructure.
- Configure extensive Puppet/Nagios and automated log file monitoring and puppet configuration management infrastructure ensuring secure and compliance configurations.
- Managed relationship with merchant bank and provided evidence of compliance.
- Managed security scans, remediations, provided evidence to prove compliance. Worked to maintain constant compliance.

Cutting Edge Networked Storage **Jul 2008 – May 2009**

OS Security Engineer

Led the team which transformed old unsupportable software distribution into a maintainable piece of software with military customers requiring **STIG** compliance.

- Implemented new automated distribution build system. Migrated to new distributed version control system. Built company intranet for collaboration.

ADDITIONAL WORK EXPERIENCE:

Interactivate *Sr. System Administrator*	**Apr 2007 - Jul 2008**
DrJays.com *Sr. System Administrator*	**Mar 2006 - Apr 2007**
Copilot Consulting *Sr. System Administrator*	**Nov 2002 - Mar 2006**
MP3.com/Vivendi Universal *Sr. System Administrator*	**Feb 1999 - Nov 2002**
Cast & Crew *Sys Admin*	**May 1997 - Feb 1999**
CyberWorks *Sys Admin*	**Jun 1996 - May 1997**

OTHER TALENTS AND AFFILIATIONS

- Cybersecurity and Linux instructor at UCSD Extension
- FAA Certified Airline Transport Pilot
- Former Secretary, Plus One Flyers Inc., a non-profit mutual benefit flying club managing 60+ aircraft and 1300+ members.
- Member of EFF, LOPSA, SAGE computer/technology organizations and AOPA, BBP, EAA, Plus One Flyers aviation organizations.
- General Class FCC licensed amateur radio operator (KK6MPP)
- Hablo Español. Estudié Español dos años en la preperatoria y he tenido a muchas oportunidades de aprender de amigos y clientes. La mayoría de mi español es por habiendo tenido a muchos amigos y clientes Mexicanos.

PUBLISHED WORKS, PRESENTATIONS, CITATIONS, TALKS, SEMINARS

https://docs.google.com/document/d/1k7goayViUjQQmd8CxMj8SEhOGeouo9uV4VmiBN4i4Xg/