

Resume of **Tracy R Reed**, CISSP, CCSK, RHCE, ATP  
858-349-5912 treed@tracyreed.org  
<https://www.linkedin.com/in/tracyrreed/>  
<https://calendly.com/tracyreed/>  
Long-term C2C Preferred

## Key Accomplishments

- Accepted into Toptal.com (screens for top 3% of applicants)
- Helped major software vendor reach their cloud vulnerability management SLA for first time
- Founded Detexian, designed/built event based IDS, earned \$500k+ 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
- Lead **PCI** compliance program, drafted corporate security policy at Edirect Publishing.
- 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

**Apr 2020 – Present**

Security Architect at **Unrisk Inc.**

Providing security architecture services to companies such as **PricewaterhouseCoopers** and **Splunk**. Provide cloud and container security tools and services for consumption by the larger organization. Worked with Twistlock for monitoring and vulnerability mitigation of containers, docker, kubernetes. Built software and service deployment pipelines with Azure DevOps. Harden AWS and Azure cloud environments. Manage and oversee vulnerability management program. Mentor junior security staff.

**Jan 2019 – Mar 2020**

Cloud Security Architect at **Trace3**

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).

**Jun 2018 – Nov 2018**

CTO at **Detexian**

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.

**Jan 2011 – Jan 2019**

Security Architect at **Copilotco**

Operated secure managed hosting company. Hosted infrastructure and managed compliance program for customers such as Resume Rabbit (PCI) and MedicFusion (HITRUST/HIPAA).

**Oct 2017 – May 2018**

Security Architect at **Twistlock**

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.

**Nov 2015 – Oct 2017**

Sr. Security Engineer at **InVision**

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.

**Oct 2011 – Nov 2015**

Sr. Security Engineer at **ServiceNow**

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. Worked 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.

**May 2009 – Oct 2011**

Sr. Security Engineer at **Edirect Publishing**

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 highly 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.

**Jul 2008 – May 2009**

OS Security Engineer at **Cutting Edge Networked Storage**

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.

**April 2007 - July 2008**

Sr. System Administrator at **Interactivate**

Led IT department transforming a messy and insecure environment with long history of trouble into consistent and highly reliable system. Saved a documented \$300,000 while providing the company with their best year ever for the IT department with no intrusions. Designed/deployed highly available and secure services including cost effective Xen virtualization with AoE SAN. Migrated critical services into more secure datacenter. Implemented configuration management policies, improved network monitoring, wrote documentation, and mentored system administrators. Migrated away from costly proprietary technologies towards open and in-house supportable technologies and nurtured technical skill development within the company.

**March 2006 - April 2007**

Sr. System Administrator **DrJays.com**

Build reliable and scalable infrastructure to keep the orders coming in. Maintained security for e-commerce operation and protected customer card data per PCI. Saw the company through a 70% growth year while building out new offices and moving the web, mail, database, and numerous other servers to a highly secure and cost-effective virtualized environment which maximizes return on hardware investment. Designed secure virtualization cluster with Xen with AoE SAN backend. Built call center phone system which handled 30 customer service agents during the busy Christmas season and is capable of handling many more while doing call distribution, recording, IVR, etc. using the Asterisk PBX. Integrated with three office locations around the US with a PRI (T-1) and external VOIP provider. Implemented system/network monitoring, log file analysis, cfengine system configuration, adhered to the best practices for building solid infrastructure advocated by Infrastructures.org. Deployed custom intranet website which included file sharing, blogging, and wiki which was used to document all of our systems and perform corporate collaboration and communication. Successfully recruited new employees via novel means to work as developers and system administrators. Won the largest bonus awarded in the company for that year.

**November 2002 – August 2005**

Independent Consultant

Focused on Linux security and open source software. Provide Linux related technical services all over the world including a particularly fun Linux based audio/video deployment in Hong Kong for DivX. Design/implement Linux servers for firewall, email, virus scanning, file server, database systems. Write custom **SELinux** policies to support proprietary applications. Set up company communication and collaboration infrastructure such as wikis (Zope/Plone) and instant messaging platforms (Jabber/IRC/IM). Conducted numerous training sessions to get the client's staff up to speed on their new systems. Provided VOIP services to small businesses. Specify and install on-site PBX systems as well as hosted PBX systems. Write custom telephony applications such as IVRs to take customer input and store in a database. Interface PBX systems to traditional PSTN using T-1 and POTS hardware. Interface PBX systems using IAX, H323, SIP VOIP protocols.

**Feb 1999 - Nov 2002****Sr Sys Admin at MP3.com/Vivendi Universal**

Helped transform tiny 10 employee company into a major force in the world of on-line music. Scaled infrastructure 1000x. Installed, configured, and operated very large disk and tape backup systems. Maintained network security including installation and maintenance of firewalls and security policy. Used MySQL database to manage massive amounts of MP3 music and customer data. Supervision of very large banner ad server installation and data processing responsible for the majority of company revenue. Maintained critical email, DNS, http, database, and various other systems. Install and maintain Linux and Solaris systems. In 1999 I recognized the need for a journalled filesystem in Linux, discovered ReiserFS, arranged MP3.com to provide funding for the journalling portion of ReiserFS and implemented the use of the filesystem on over 500 systems saving the company tens of millions of dollars over purchasing Veritas vxfs.

**May 1997 - Feb 1999****Sys Admin at Cast & Crew**

Administer HP-UX, SCO, and Linux machines and network across the corporate LAN spanning 5 offices across the US and Canada. Maintain reliability and security of Unix systems in a mission critical financial environment, supporting staff, troubleshooting and preventative maintenance. Interaction with the UNIFY database system. Performance monitoring and tuning of database servers. Maintaining DNS, mail, and user accounts.

**June 1996 - May 1997****Sys Admin at CyberWorks**

Primary responsibilities include ensuring reliability and security of Unix systems including Solaris and Linux, supporting staff and clients in all technical areas, maintaining the DNS, mail, mSQL and Oracle databases, and web server systems. Also did extensive CGI programming and HTML authoring.

Examples of personal source code, configs implementing security controls, security matrices, whitepapers, and references are available upon request.

**Other talents and affiliations**

- Cybersecurity and Linux instructor at UCSD Extension
- FAA Certified Airline Transport Pilot
- Member of the Kernel-Panic Linux User Group/San Diego Computer Society since 1998, served as President, Secretary. Regular presenter on a wide variety of security subjects.
- Former President, current member of the San Diego Computer Society
- 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 preparatoria 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://marketscale.com/industries/industrial-iot/the-raspberry-of-my-eye-electronics-engineers-vote-on-raspberry-pi-as-favorite-sbc/>

<https://www.socallinuxexpo.org/scale/16x/speakers/tracy-reed>

<https://extension.ucsd.edu/about-extension/tracy-reed>

<https://www.securitymagazine.com/articles/87943-payment-data-compliance-12-major-requirements-of-the-pci-data-security-standard>

<https://www.meetup.com/Open-Web-Application-Security-Project-San-Diego-OWASP-SD/events/158734172/>

<http://arstechnica.com/features/2002/08/warflying/>

<https://ideamensch.com/tracy-reed/>

<https://www.securitymagazine.com/authors/2287-tracy-reed>

<https://www.welivesecurity.com/2011/12/19/what-would-a-credit-card-breach-cost-your-company/>

<https://www.nextadvisor.com/blog/finding-a-hipaa-compliant-web-host/>

<https://www.esecurityplanet.com/trends/article.php/3933491/Is-Linux-Really-More-Secure-than->

<https://www.networkworld.com/article/3191804/security/healthcare-records-for-sale-on-dark-web.html>

[https://images.techhive.com/images/article/2016/12/medical\\_records\\_laptop\\_doctor-100699858-](https://images.techhive.com/images/article/2016/12/medical_records_laptop_doctor-100699858-)

<https://www.giac.org/paper/gsec/2278/evolution-war-flying/103978>