

Cindy Perry, CISSP, GCIH Oakland, CA cinders@freygirl.com

SUMMARY

Resourceful, versatile IT Security professional, able to quickly adapt to evolving, industry-specific applications, concepts and terminology. A team leader whose excellent management, organizational, problem-solving, communication and people skills provide support and direction in a hectic and complex arena.

Technical skills include:

- Security Tools: EnCase, FireEye, Tanium, Netscout nGenius, Wireshark, HBGary, CyberArk
- Databases: MS SQL, Informix, Greenplum (MPP), Splunk
- Platforms: AIX, Solaris, Linux, HP-UX, DEC/OSF1, z/OS, VMware, Windows
- UNIX tools: ksh, vi, emacs, awk, sed, sql, html, ssh, sudo, PowerBroker
- Desktop apps: MS Office, Lotus Notes, BMC Remedy, SharePoint
- DB Tools: SQL Server Mgmt Studio, Aginity, PGAdmin
- Dev Tools: Team Foundation Server, Archer

EXPERIENCE / ACHIEVEMENTS

2008 - present Kaiser Permanente IT

Mar 2017 - Present Cyber Security Data & Platform Service Engineer

Cyber Security Data & Platform Services

Recruited (as part of a re-org) into the Data & Platform Services team to support the (primarily) Splunk environment for the Cyber Security teams. Continuing my ongoing quest to find, collect, validate and ingest pertinent enterprise data into Splunk to enhance existing threat management capabilities. My experience in KP's Identity Management, Security Research, Incident Response and Internal Threat Intelligence brings to the team a fresh perspective as well as much needed subject matter expertise.

Apr 2016 – Mar 2017 Internal Threat Intelligence Analyst

Cyber Security Internal Threat Intelligence

Hand-picked to help create a new Threat Intelligence team to focus on the internal network security, correlating known external threats to specific vulnerabilities in critical KP environments. Partnering with myriad Technology Risk Organization (TRO) and application teams, we are charged with enhancing Cyber Security relationships, data access and increasing our visibility throughout the organization.

Mar 2015 - Apr 2016 Cyber Security Incident Handler

Cyber Security Threat Response & Investigations

Joined the KaiserPermanente Computer Emergency Response team (KCERT). Responsible for handling security incident escalations through all phases -- from identification and containment to recovery, eradication and lessons learned.

- Oct 2015 - Successfully completed Splunk Certified Knowledge Manager V.6 Training and Certification
- Nov 2015 - Successfully completed GIAC Certified Incident Handler (SANS) training and GCIH certification.

Jun 2013 - Feb 2014 Security Analyst/Developer

Cyber Security Research & Development

Recruited into an elite, new KP Cyber Security team that is focused on cutting edge work involving Big Data,

security modeling and analytics to more quickly and accurately hone in on actual security threats. Responsible for research and reporting, procedural and logistical support, and increasing the scope and validity of security intelligence within the Kaiser enterprise.

- Feb 2014 - Successfully completed CISSP training and certification.

Jan 2010 - Jun 2013 *Lead Technical Consultant*

Information Security, Identity & Access Mgmt (IAM) UNIX

Supporting Identity and Access Management for over 3500 myriad, geographically dispersed UNIX systems (AIX, Solaris, various implementations of Linux). Providing leadership, technical direction and support for all UNIX security projects and related compliance efforts.

Hired as temporary FTE after 18 months as contactor. Promoted to permanent FTE position after 3 months.

- Leading, motivating and mentoring team of Identity Management engineers.
- Managing and streamlining daily Remedy queues.
- Coordinating audit research and responses.
- Evaluated, designed and implemented replacement of existing central management product with a UNIX-to-Active Directory solution (QAS/VAS).
- Leading the UNIX-to-AD migration project, exceed reduction goal of 50% (250,000) of local UNIX accounts in one year.
- Assisting with establishing Technical Security Standards and enterprise-level implementation.

Jun 2008 - Jan 2010 *PrO Unlimited (contractor for Kaiser Permanente) UNIX OS Security Engineer*

Information Security, Identity & Access Mgmt (IAM) UNIX

- Successfully deployed BeyondTrust (Symark) products (PowerBroker, Password).
- Developed documentation to satisfy audit requirements for SOX and PCI certifications.
- Collected and reported OS security-related data.
- Identification and root cause analysis of security issues and vulnerabilities.
- Worked directly with the business/application-side customers to remediate UNIX security issues.
- Extensive shell coding and task automation

1996 - 2007 *Wells Fargo & Co.*

UNIX Production Quality Control

Proactive critical OS & security patch and security maintenance for over 3000 UNIX servers, serving 200+ Business Units across the enterprise. Extensive Korn shell programming to automate and streamline processes for system builds, account administration, data collection, database updates and system hardening/security compliance. Installation, maintenance and support of various layered security products: Quest VAS, OpenSSH, VAS, CyberSafe Kerberos AppSuite, Symantec ESM, sudo, Symark PowerBroker. Assisted peer engineering teams with software rollouts, troubleshooting and general UNIX support.

EMPLOYMENT HISTORY

Kaiser Permanente	Pleasanton, CA	Internal Threat Intelligence Analyst Cyber Security Incident Handle Security Analyst/Developer Lead Technical Consultant	2016 - now 2015 - 2016 2013 - 2015 2010 - 2013
Kaiser Permanente (PrO Unlimited)	Oakland, CA	(Contractor) UNIX OS Security Engineer	2008 - 2010
Wells Fargo & Co.	San Francisco, CA	Operating Systems Engineer 6 Operating Systems Engineer 5 Technology Manager 3 Applications Systems Engineer 5 Applications Systems Engineer 4 Sr. Systems Programmer	2005 - 2008 2004 - 2005 2001 - 2005 2000 - 2001 1998 - 2000 1997 - 1998
Wells Fargo & Co. (RealTek Innovations)	San Leandro, CA	(Contractor) Open Systems Security Analyst	1996 - 1997
22 Solutions, Inc.	San Francisco, CA	Independent Consultant	1996 - 1996
Montgomery Asset Mgmt.	San Francisco, CA	Systems Analyst	1994 - 1995
Blum's of San Francisco	Emeryville, CA	Senior Programmer	1991 - 1993
SBG Partners, Inc.	San Francisco, CA	Information Systems Coordinator	1989 - 1991