# JEFFERY HUNTER

**310 West Michigan Street #621, Indianapolis, IN 46202· 818 599 8199 ·**[**hunter.jeffery@live.com**](mailto:hunter.jeffery@live.com)

**Please visit my LinkedIn Profile -** [**http://www.linkedin.com/pub/jeffery-hunter/7/489/696/**](http://www.linkedin.com/pub/jeffery-hunter/7/489/696/)

**Profile**

Experience with a wide variety of computer and security systems in corporate environments, as well as consulting services. Twelve-plus years of multi-platform server management with Windows and Unix-type operating systems; including AIX and multiple distributions of Linux. Solid background in security appliances and software including SIEM, Firewalls, SSL Firewalls, Web Appliction Firewalls, encryption, databases, and IPS as well as Internal PenetrationTesting and Security Assessments including SOX and PCI DSS.

**Summary of Qualifications**

Secure enterprise systems in a heterogeneous OS environment including Windows, Mac, AIX, and Linux

Evaluate and recommend corporate policies and procedures compliant with SOX and PCI security requirements from a network, systems, data-leakage and risk analysis perspective as well as internal and external SOX and PCI assessments

Manage IDS, IPS, HIDS, SIEM and Logger, IPtables, Appliance-based Firewalls, Web Application Firewalls, Vulnerability scanners, Load-Balancers, and other critical security infrastructure from multiple vendors

Design and deploy Security Infrustructure that works together to produce high-reliability positives and customize SEIM connectors and processes for correlation of data feeds to gain additional intelligence and remediate threats

Primary Windows Domain Administrator and Network Security Engineer for William Hezmalhalch Architects

Experience with scripting languages including Ruby, Perl, Windows Powershell, and PS/SQL

**Professional Experience**

**October 2014 – Feburary 2015**

**Kinney Group – Indianapolis, IN**

***Splunk Development Engineer***

Develop Splunk apps and search and reporting content based on business requirements surrounding data analytics, industry standards and best practices, auditory requirements, and security infrastructure. Deploy and support Splunk to emerging customer base. Evaluate, test and harden Kinney Group software stack for ICD 503 accreditation to deploy at Federal and private industries. Make suggestions for internal audit and security infrastructure leveraging existing technologies. Assess and recommend new technology partners.

**July 2010 – October 2014**

**Personal Consulting Services**

**Direct contract for Security and Infrustructure and Subcontractor for IT Security – Los Angeles, CA**

***SoCal Edison, Block Alternatives Racing, City of Lakeland Police Department, Experian, IPC, others***

***Many customers can not be disclosed, as NDA’s with reseller forbid it for a term of 5 years***

I specialize in architecting and deploying solutions enabling customers to get value from their Imperva WAF, BlueCoat Proxies, Juniper Switches and Firewalls, Citrix WAF and WAN accelerators, McAfee IPS, HP TippingPoint IPS, ArcSight, QRadar, LogRythm, Splunk and other SIEM and security appliances, including Cisco ASA, Fortinet, Checkpoint Firewalls, Palo Alto and other Firewalls. Architecture, initial installation, configuration, hardening, and deployment of supporting hardware and servers. Help establish security practices based on close working relationships with clients, while utilizing partnerships throughout the industry to expand clients options. With significant experience architecting and deploying critical security infrastructure from multiple vendors, I have the capacity to see complex projects through from initial planning to completion. I meet customer objectives without requiring the dedication of multiple IT system administrators and compromising their regular duties. Communication is vital to a successful engagement, with collaboration and knowledge transfer a primary concern during my work.

**Feb 2013 – July 2013**

**Korn/Ferry International – Los Angeles, CA**

***Senior Security Engineer***

Assess, evaluate and make recommendations to CIO, CTO and business management regarding security nd compliance gap analysis, emerging technologies, policy and procedures, and employee training; which led to approximately $80,000 in savings as a product up for purchase was not functional in the environment at Korn/Ferry. Configure and manage all security appliances and infrastructure critical to Korn/Ferry’s security posture. Inform management of possible attack vectors and provide risk-analysis to enable an informed decision to be made. Architect, deploy, create custom content and Flex-Connectors using previously purchased but never utilized ArcSight appliances to detect vulnerabilities and recommend remediation steps to relevant IT parties. Configure and Deploy Citrix WAN Accelerators, Maintain or build new Linux and Windows servers for security use. Recommend and deploy Cisco ASA Firewall rules and policies. Establish effective communications across disparate groups and offices all over the world to effectively place Korn/Ferry’s security policies at the forefront of daily operations, while receiving feedback from team members about concerns they are seeing at their local sites. Protect Korn/Ferry’s Web Application security by designing best-practice based coding procedures, using tools such as Vericode and others, and enforcing a policy of least required access along with tight perimeter controls.

**April 2008 – May 2010**

**Accuvant – El Segundo, CA**

***Security Technologies Consultant***

Ensure compliance for customers about to become responsible for legally or industry protected data by providing gap analysis, assessing solutions, and implementing hardware and software. I worked to ensure client success, beyond simply installing products, by deploying proven methodologies and industry best practices, thus demonstrating the value and effectiveness of a new technology or solution and improving client security posture. Among my professional work with Accuvant, examples of major projects are the successful deployment of six large-scale ArcSight solutions which included ESM and Logger appliances and ESM software in various architectures, as well as a multi-campus upgrade from Cisco Pix to Juniper firewalls that interconnected thirteen sites together, allowing for management from a single NSM source that greatly enhanced IT's ability to scale as new locations came online. And Riverbed, Citrix, and Imperva deployments. Other engagements include compliance assessments to prepare customers for audit.

**August 2004 – March 2008**

**Princess Cruises Corporate Offices – Santa Clarita, CA**

***IT Security Analyst***

Install, administer, and maintain health for all security related servers, applications, systems, Imperva devices, Checkpoint Firewalls, and databases. Define and enforce security policy to ensure compliance with relevant legislation or controls; including PCI, SOX and Best Practices. Create content in ArcSight ESM to correlate data and detect anomalous activity. Work case flow through resolution. Maintain and upgrade application databases. Evaluate and recommend hardware and software to minimize security risks while keeping within budgetary confines. Resolve any possible breaches of policy and report findings to management and remediation teams. Promote a healthy security culture in the company through interdepartmental interaction and educating employees regarding social hacking ploys. I served on the Carnival Global Security Council to ensure consistent practices across all Carnival brands.

**August 2000 - November 2003**

**William Hezmalhalch Architects – Santa Ana, CA**

***Management Information Systems***

Windows domain administration, configuration of PC builds, backup, and maintenance. Maintain AutoCAD application

standards. Desktop support. Server and LAN configurations for corporate headquarters and satellite locations. MS

Exchange and Citrix server administration. Management of NAS solution. Basic telecom admin tasks.

**Systems and Technologies Overview**

ArcSight ESM, ArcSight Logger, McAfee IPS, QLogic, Snort, Nessus, Wireshark, NMAP, Imperva SecureSphere, Checkpoint Firewall, Fortinet, Linux, IPtables, SELinux, Firewalls, NetIQ Security Manager, SolarWinds LEM, Whole-disk Encryption, MS Windows Server, MS Exchange server, MS IIS, MSSQL, MySQL, Oracle, BlueCoat, Juniper NSM, Juniper SSL-VPN, Juniper Firewalls, Citrix Netscaler Load-Balancers and WAF, F5 Load Balancers, Riverbed Steelhead WAN Accelerators, TippingPoint IPS, Cisco Routers, Layer-3 Switches, Cisco ASA firewalls, OSSIM, Lieberman SSO and Key management software, RSA soft-keys and token deployment, VMWare (Director and Client), Splunk, Puppet, Software Defined Networking

**Certifications**

**Splunk:** ADVANCED SEARCHING and REPORTING

**Riverbed**: RCSA-W

**Juniper**: JNCP FW, VPN, SSL, NSM, and IDP

**ArcSight**: ACSA, ACIA

**Imperva**: IWSS

**Citrix:** Web Appliction Firewall and Load-Balancer (expired due to lack of certifiction upkeep as companies were converting to Imperva and Riverbed)

**Extended Education**

**California State University, Long Beach**

Completion of nearly 7 Semesters in the Aerospace Engineering program. I had extermely high hopes to become an Engineer at JPL, however while working part-time as a Windows Domain Admin and technologist at an architecture company to put myself through school, I was given the ultimatum to stay on full-time of be fired. After consulting with Engineers and test pilots from NASA Dryden, JPL, and the Boeing Delta rocket site in Seal Beach, I was convinced that the future did not look bright for space inquiry, and elected to put my degree on hold and pursue a career in Information Technology.

**Multiple Technical Training Programs**

Advanced ArcSight ACIA, CISSP 2 week training course, Riverbed Steelhead Deep-Dive courses, Citrix

Netscaler, Multiple Juniper products and solutions, Windows Server 2008R2 and 2012, and Imperva SecureSphere Deep-Dive for WAF, DAM, FAM, Sharepoint. Basic Cisco Routing/Switching, multiple Firewall vendors, Click Security, RedHat 5 training and TippingPoint.

**NASA APEX Glider Web Developement**

Project Manager for Technologies with the NASA Apex Project Web Development team. Working side-by-side NASA Dryden engineers, I expressed goal objectives and airfoil properties that drove the creation of one of the newer classess of very high altitude, unmanned reconnaissance glider technology to the public. This included web development and public speaking at NASA sponsored events.