# RAMIN (Robert) AKHAVAN

**SECURITY BIO:**

Mr. Akhavan has effective hands-on experience working in various facets of electronic security, IT Infrastructure Security Architecture and Secure Application development practices in addition to Security Governance and “security practice” creation and management proficiency. As a former Professional Services consultant and CISSP Trainer, he has experience in all facets of large, diverse information technology architectures, implementation and security efforts such as hands-on involvement with the establishment and successful execution of worldwide computer emergency response teams while at fortune 50 companies or consulting to customers evangelizing proper threat-modeling and Risk Management practices for achieving compliance (PCI, SOX,SSAE-18, GDPR, ISO27K1, NIST, etc.). These encompass functional design, development, and measuring the success of information protection capabilities in areas such as software DAST and SAST methodologies for app security, incident response functions, secure network implementation/engineering, network security monitoring, security assessment techniques, gap analysis reports, data encryption (including PKI), policy development, quality assurance and compliance/pre-audit preparation, augmentation and re-prioritization activities. Essentially he is the rare candidate that has worked and trained students and colleagues in the 5 domains of Information Security in depth. He specializes in Infosec team overhauls for large fortune 50 enterprises and “build from scratch” Security Practice for startups in “Green Field” opportunities. Many former employees and colleagues ask for opportunities to come work for him in order to holistically understand best practices in Information Security and Compliance.

**Summary of Experience: Summary of Aptitudes:**

|  |  |  |
| --- | --- | --- |
| **- Fortinet Inc.** | Director of Information Security & Compliance | **- Information Risk Management  - PCI DSS, SOX, HIPAA, ISO 27K1, GDPR & GLBA - Security Frameworks, Policies & Procedures  - IT Audit & Compliance Management - Vendor Risk Management  - Cyber Security & Attack Mitigation - Incident Response & Investigations  - Information Security Project Lifecycle Management - Data Privacy & Protection  - Strategic Technology Planning** |
| **- Amazon (Lab126)** | Architect/Manager Security Operations |
| **- Zendesk.com** | Security Architect/Compliance Officer |
| **- Walmart.com (E-Commerce)** | Lead Sec. Eng./Sec. Architect/Interim Sec. Mgr. |
| **- Cypress Semiconductor** | Senior Systems and Security Consultant |
| **- TCS/Kivera-Mobile Navigation** | Senior Systems and Security Consultant |
| **- Siegeworks (now Optiv)** | Technical Training Director/Training Developer |
| **- Skybox Security …** | Professional Services |

**Detailed Experience:**

|  |  |
| --- | --- |
| **● Fortinet Inc. [Sunnyvale, CA]** | **08/2015-Present** |
| **Director of Information Security & Compliance (HQ)** |  |

As the Director of Information Security & Compliance, I am in charge of global policy and procedure development, on-prem systems/networks security, cloud operations security, IT infrastructure and applications security review and enterprise risk management. The team that I developed is part of the backbone of our networks’ integrity, ensuring that our customers and developers have secure and reliable experiences including internal/external customers. The primary focus is driving security programs at the business level and serving as a deeply skilled and knowledgeable SME and resource for all security activities within Fortinet, the number two firewall maker in the world.

**Responsibilities**

* Manage and drive all major security and compliance efforts
* Scope, design, and oversee deployment of security tools and architectures (including SAST/DAST for applications)
* Built and manage the security team, started with one direct report and grew the team to 8 (so far). Writing all job descriptions and structured interview processes.
* Lead Fortinet in employee information security training, certification and continuing education planning and reporting
* Promote and raise information security awareness to all facets among all project and department stakeholders
* Acting as a trusted advisor and SME to senior management by identifying critical security issues and recommending risk-reduction solutions (Yes, even security companies such as Fortinet need guidance and consultancy in the major 5 domains of Infosec given that their area of expertise is mostly just networks)
* Participate on automation of the incidents prioritization, false positives identification, trending, correlation, etc.
* Oversee application and infrastructure penetration tests including physical security review and social engineering tests
* Participating on selecting, developing and interconnecting SIEM tools with sources of security incidents as well as other information systems
* Work with existing Cloud Operations groups to implement and imbue Continuous Security Deployment and Integration within the various Clouds (Public, Hybrid and Pure) in all environments as it relates to security
* Build the SOC (Security Operations Team-different than Security Engineering Team) whose directive is to monitor external information sources for new vulnerabilities and attack techniques (we are a large target in this respect)
* Develop reports for internal customers relating to security including vulnerability assessments and risk matrices.
* Work alongside IT team to ensure security controls on IT infrastructure and applications are performing effectively
* Act as focal point for any investigations involving security; to prepare reports and note follow up actions
* Ensure our compliance related to security with any regulations or certifications we must adhere to (ISO 27001, SSAE-18, FISMA and GDPR). For the later, I lead the efforts by messaging and training internal stakeholders and (IT and engineering) internal communities and lead the efforts in the DPIAs to identify and deal with “European Citizen” data.
* **Executing risk assessments for internal and external (partner) systems.**
* **Negotiated saving of 45%+ on purchases of Infosec tools and materials.**

***[UBUNTU server 14, Oracle 12, MySQL 6.x, Win2K12, AD, Windows 10, VMware ESXi 6, OSX El Capitain, LockPath Keylight, Oracle GRC, Qualys, Skybox-Full Suite (Vul.Mgmt), Lancope StealthWatch (now Cisco), IXIA TAP aggregator, Forti-client, McAfee database agent at colo, “White-Hat Security” DAST, Forti-Analyzer, AccelOps, IBM Q-radar, Veracode SAST, IBM Appscan, Burp Suite, Core Impact Professional, Ping Identity-PingFederate & PingID, Phantom (Security Automation), LockPath KeyLight (GRC), Titus (data classification), Guardium (Database Firewall), BeyondTrust (Application privileged Access management, Jamf, NetWrix, CyberArc (privileged user proxy/access control), PWNIE (Wi-Fi security), Wrike for employee project/work tracking]***

|  |  |
| --- | --- |
| **● Amazon [Cupertino, CA]** | **08/2013-08/2015** |
| **Architect/Manager Security Operations (Lab126 – “Kindle” unit)** |  |

As the Information Security Manager/Architect, I was tasked with supporting the implementation and execution of the IT security program, with an emphasis on Information Security Engineering & Operational activities. The role reported to the head of IT and accountable for Information Security, Information Risk Management, and IT Compliance as well as Security Operations concentrating on security of web services as well as DLP for the unit’s (Lab126’s) Intellectual Properties across the globe. I had exposure to both a small (the Electronic Manufacturing Arm – Lab126) and the larger organization (Amazon Retail Fleet) and was able to leverage my previous experience in regulated environments, such as health care or financial services and e-governance requirements such as PCI, SSAE-16, SOX and HIPPA. **Essential duties and responsibilities include but are not limited to the following:**

**Information Technology Governance, Risk Management, and Compliance (20%)**

* **Designed and implemented of a new Infosec Control Catalog and Insider Threat Program**
* **Lead the joint effort to define and update configuration standards for key technology platforms.**
* **Executed risk assessments for internal changes, as part of SDLC and Change Management processes, and third-party vendors, document findings, and communicate findings to internal and external stakeholders.**
* **Participated in the design and implementation of the Business Contingency Management program.**
* **Designed and implemented processes and technology solutions to assess, monitor, and enforce compliance with internal and regulatory requirements, such as GxP, SOX, and others.**
* **Interfaced with external partners, customers, and other 3rd-parties for matters involving information security and information risk management.**

**Information Security Engineering & Architecture (30%)**

* Defined a cohesive information security tools architecture that emphasizes integration, proper implementation and configuration of tools, and balance in-sourcing and outsourcing options.
* Evaluated information security requirements for planned initiatives and/or changes in the technology environment as part of the SDLC and Change Management processes.
* Defined configuration standards and configure information security tools, both in-sourced and outsourced, inclusive of event management and monitoring.
* Provided information security consulting services to internal users, both within and outside of the IT department.
* Personally Re-architected the following:
  + - Cloud Security: Implemented tools (e.g. Elastica) for our AWS VPCs + Virtual Network Segmentation
    - Compliance: Implemented Lockpath KeyLight for integration of mapping various framework’s controls
    - Database Activity Monitoring: Implemented Imperva’s SecureSphere database firewall
    - DLP: Implemented McAfee Total Protection for Data Loss Prevention for endpoint security
    - Encryption/File sharing: Migrated S3 buckets to Watchdox
    - Endpoint Security: Combination of Moka5 and PAN’s Global protect
    - IAM/Authentication: Implemented Sailpoint
    - Security Services:
    - SIEM/ Log Management: ArcSight
    - Threat Management [IPS/IDS, Network Security]
    - Web Threats [application and 2.0]
    - Vulnerability Management/ Pen Testing
    - Virtualization Security
    - Application Security
    - Mobile Security/ Mobile Device Security

**Information Security Operations (25%)**

* Overseeing the day-to-day administration and management of information security tools, both in-sourced and outsourced, as well as third-party/managed security service providers.
* Overseeing threat and vulnerability management processes, inclusive of vulnerability scanning, remediation efforts, notifications, etc.
* Review of system events and incidents on a daily basis.
* Lead investigation of potential incidents.
* Lead incident response processes as the incident coordinator.
* Served as the primary point of contact for information security operational matters, 24x7x365.
* Provide 3rd level support for information security tools and operational processes.
* Built and managed the security team. Writing all job descriptions and structured interview and annual reviews. (Supervision of 15 Information Security Engineers)

**Compliance (20%)**

* Support IT compliance activities for GxP, SOX, and PCI.
* Produced and gathered research as required.
* Monitoring and enforcement of compliance with corporate policies and control requirements as well as the Subsidiary’s governances.

**Vendor Management (5%)** Negotiated substantial discount with company vendors (Security Vendors), successfully reducing these cost by 40% (~$3.2 million)

***[UBUNTU server 12.04, Oracle 12, MySQL 5.x, Win2K12, AD, VMware ESXi 5, OSX MountainLion, Moka5 BareMetal, LockPath Keylight, Qualys 7, Sourcefire 5.x, PaloAlto Networks 6.x, PaloAlto GlobalProtect, Netskope (CASB), Gigamon Tap aggregator, McAfee DLP, Caspida, Cenzic, Burp Suite, Appscan, HP Fortify, SailPoint IAM, Watchdox, ArcSight, Asana for employee project/work tracking]***

|  |  |
| --- | --- |
| **● Zendesk.com [San Francisco, CA]** | **01/2012-08/2013** |
| **Security Architect/Compliance Officer** |  |

As the Security Architect, selected and drove the proper compliance frameworks for Zendesk’s Multi-tenant offering in order to meet our customers’ compliance and data assurance needs (SSAE-16 and internationally ISAE-3402 and later ISO 27001). I proactively worked with IT and Site (business site) to identify security risks and implement practices that meet standards for information security. Additionally I had to analyze and address monitoring and reporting practices that are exceptions to policy standards and manage overall risk. I was responsible for coordinating and leading information security activities across company & creating a broad-based IT security conscious culture (for not just the site, but in the headquarters as well…this is due to the propensity for this line of business to be “socially engineered” with tremendous amount of Phishing attacks). I also lead the compliance efforts for the security portions of SOX for our backoffice/financial systems. Other primary areas that I functioned as:

* ***Architect:*** Redo of the company’s Infrastructure security posture. Introduced DAST and SAST practices as part of augmenting the QA cycles looking for Code vulnerabilities. Created roadmap for SSAE-16 compliance.
* ***Production Support:***Worked with Operations, Audit and within own Compliance team to develop and train team on auditing and review methodologies and practices to identify and respond to anomalous or security related activities and proper incident response.
* ***Operational Security:*** Researched and reviewed security tools and frameworks to identify and investigate malicious or unauthorized activity. This included such tools as HIDS, NIDS, Log Analyzers, SIEM and other solutions to build out Zendesk’s Security posture and capabilities. Reviewed and redesigned network, infrastructure, and service architecture, ensuring solutions adhere to security policies and practices.
* ***Application Security:*** Came up with solutions for DAST and SAST for the company’s multi-tenant application offering
* ***Customer facing:*** Acted as main PoC in the coordination and standardization of responses to customer-provided security surveys/requests and questionnaires. Pre-sales resource for Customer Assurance inquiries.
* ***Vendor relations/management:*** Negotiated substantial discount with new vendor (Security Vendor) vis-à-vis existing hardware VAR, successfully reducing these cost by 30% (~$1.1 million)
* ***Manager:*** Supervision of 4 full-time employees (performing duties in Security operations, Web-App vulnerability and pen-testing)
* ***Compliance Officer:*** Wrote all of security and compliance policies. Implementation of GRC solution for security metric and risk assessment tracking. Oversaw implementation of controls for SOC2 (Type II) testing.
* ***Security Trainer/Advocate:*** Created and delivered security awareness training to employees and management.

*A sampling of the systems that I implemented:*

* Global Firewalling re-architecture via Next Generation Firewalls (Palo Alto Networks)
* Re-architecture of the Front End of the site via elimination of web proxy layer with F5 Viprion series
* APM: Opnet ARX for attack analytics
* IDS/IPS: Sourcefire
* VMware ESX/ESXi Virtualization firewalling: tuned previous implementation of vShield
* Application vulnerability (DAST) testing: Cenzic and NTOSpider
* SIEM: Q-radar with integration with e-Streamer for IDS and firewall logs plus web server logs.
* Oauth 2.x/SAML: see below
* SOA governance: Architected the Layer7 implementation for partners and third party integrations.
* Built and managed the security team, started with one direct report and grew the team to 7. Writing all job descriptions and setup of structured interview processes.

***[UBUNTU server10, Ruby on Rails, MySQL 5.x (Perconna), Win2K8, AD, VmWare ESXi 5, OSX Lion and MountainLion, LockPath Keylight, Qualys 7, Sourcefire 5.x, PaloAlto Networks, PaloAlto GlobalProtect, Q-radar, Cenzic, NTO spider, Veracode, Opnet ARX, Basecamp for employee work tracking]***

|  |  |
| --- | --- |
| **● Walmart.com [Brisbane, CA]** | **Full-time — 01/2010-01/2012** |
| **Lead Security Engineer/Sec. Architect/Interim Sec. Manager** |  |

As the Lead Sec Engineer/Architect, I was charged with the security upkeep of the number 4 retail web site in the world as well as all Wal-Mart global retail web sites (ASDA, ChinaGM, etc.). The security driver in the U.S. is primarily driven by PCI for such a large Level I Merchant. Here are the primary areas that I functioned as:

* ***Production Support***As part of my regular duties I provided 24/7 on-call security operational support on a rotational basis for the production Web environment and associated locations; Patch management; Password/Key management; Certificate management; Resolve business/customer support issues (Online Fraud, etc.). Investigate attempt at ddos and intrusion attempts.
* ***Project Consulting/Tasks Work*** I created, implemented and documented large security systems. I wrote comprehensive security policies, standards and procedures. I served as primary point of interface with Wal-Mart’s mothership corporate IT security organization in Bentonville, AK; Monitored ongoing incidents and threats, and ensured that the enterprise was protected appropriately. I had to work with other software development engineering teams to ensure that security requirements are satisfied for all projects and recommended architectural changes to satisfy same; Evaluated new technologies and present findings and recommendations to management. I drove vulnerability assessments and sometimes follow-up on the action items generated. I had Junior team members mentoring responsibilities, but if escalated, I needed to step in. I regularly evaluated complex business and technical requirements, and had to effectively communicate inherent security risks to non-technical business owners. I lead cross functional project teams (at the time of my departure I was working on 9 Projects). Provided guidance to members of the operational team (some of which were the offshore China team).
* ***Research*** I was the primary provider of “Infrastructure Security Technical Architectural Leadership” in the areas of design, operational methodology, implementation and maintenance of Wal-Mart’s web properties running in 24/7/365 environments (with 5 nine HA). The focus was on security design and revising the security plan to meet current business needs and compliance regulations hardest of which was worldwide PCI requirements. I drove or helped drive the selection, prototyping and implementation of applications and technical solutions to business problems; Interacted with internal and external technical leaders to develop original solutions that meet business needs with respect to availability, functionality, performance, capacity planning, scalability, reliability, realistic implementation schedules and adherence to architectural and security goals and principles.
* ***Cloud Security*** Participated as a key member of Walmart.com’s Cloud strategy (public and private) committee and made recommendation regarding security postures (operational &risk profiles) to technical management and business stakeholders.
* ***Vendor Management*** Negotiated substantial discount with company vendors (Security Vendors), successfully reducing these cost by 40% (~$5.7 million)

*A sampling of systems that I implemented (actual list of projects too long list here):*

* Vulnerability management, network visualization and attack simulation: RedSeal
* Access Control: e-DMZ TPAM (now part of Quest software)
* Global Firewalling re-architecture via Next Generation Firewalls (Palo Alto Networks)
* Re-architecture of the Front End of the site via elimination of web proxy layer with F5 Viprion series
* Certificate management: Venafi
* Software source-code versioning system: WANDISCO (augmented vendor’s security posture vis-à-vis Wal-Mart security requirements in regards to access control and source code DLP)
* IDS/IPS: SourceFire (dispensed with TippingPoint)
* Web Application “strike” testing: BreakingPoint
* VMware ESX/ESXi 4.1/5.xVirtualization firewalling: Checkpoint VPN-1 Virtual Edition (7.x “Fastpath”)
* Application vulnerability (DAST) testing: replaced WhiteHat Security with Cenzic
* SIEM: ArcSight integration with e-Streamer for IDS and firewall logs plus web server logs.
* OAUTH 1.1: One of Walmart.com’s acquisitions (VUDU: high definition video streaming platform) required extensive access control and federation integration; I architected and augmented the access control integration necessary to make the Oauth integration work properly using the correct number of tokens and keys in order to allow access between the user databases of both newly sister companies
* SOA governance: IBM DataPower
* Sharepoint security: Implementation of Nexlab’s DLP solution for Sharepoint
* Application Security (SAST): Veracode

***[Solaris 10, RHEL ES 5.x/6/x, Win2K3, AD, VmWare ESX 4.1-5Beta tester, OSX Leopard and SnowLeopard, OpenSSL, Verisign Certificate management, BlueCoat, nCircle, Qualys, RedSeal, TinyCA, Imperva, PaloAlto Networks 4.9.x, Cisco FWSM, e-DMZ TPAM, IBMCode Secure, Veri-NAC, Guardium, SourceFire, Cenzic, Core Impact, Venafi, PaloAlto Networks, Breaking Point]***

|  |  |  |
| --- | --- | --- |
| **● Cypress Semiconductor [Santa Clara, CA]** | **Contract — 06/2008-01/2010** | |
| **Senior Systems and Security Consultant** |  |

Brought in to help the migration of various legacy systems to new production environments as well as review of these systems’ security posture. Administered company’s development and production environments. Development of authentication front-ending with OpenRadius for VPN and Internal WiFi (Cisco Aironet APs-WISM AP manager) client users to back-end of existing Slapd (SunOne Directory Server) with Radius in a load-balanced environment utilizing CISCO CSS 11000 Series Content Services switches; Migration of several core systems from Solaris 7 to 10 and Solaris 2.x to Linux (RHEL 4); Migration of 12 Netapp cluster nodes from 870 series to FAS 3020 clusters; Implementation of Sharepoint WSS 3.0 and MOSS server for collaboration between business units. Re-architecture of Cypress’s (headquarters) client and apps’ authentication and authorization services vis-à-vis NIS, LDAP, AD and single-sign-on with existing and to be created collaterals; Implementation of Qualys vulnerability scanners for local and remote scanning and vulnerability management. Received Qualys certification.

***[Solaris 8, 9 and 10, RHEL ES 4.x, Win2K3, AD, OnTap 7.2, VmWare VirtualCenter, Sitescope, LAMP and LAMJ]***

|  |  |
| --- | --- |
| **● TCS/Kivera—Mobile Navigation Division [Oakland CA]** | **Contract then full-time — 12/2006-** |
| **Senior Systems and Security Consultant** | **06/2008** |

Supported both the development teams as well as the production environments for the company’s mobile navigation unit; Administration of company’s development and production environment; Re-architecture of TCS’s Storage Infrastructure utilizing Netapp FAS3020 and NFS tuning; Implementation of Virtualization infrastructure (VMware ESX 3.x) and reduced QA and operational cost by $0.75 million; Redo of security posture and sec. policies (vis-à-vis contractors’ network and PMI/authentication access rights); Migration of software versioning service for developers (from Clearcase 6.0.1 to ClearCase 7.0.1.1 on RHEL 5) and the training of software development staff in the utilization of the new system; Upgrade and re-implementation of company’s backup and DR posture. (Upgrade of Backup – Veritas Netbackup). Replacement of legacy firewalls with Checkpoint.

***[Solaris 10, RHEL ES 4.x & 5.x, Win2K3, OnTap 7.2, VmWare ESX, CleareCase 7.0.1, LAMP and LAMJ, Checkpoint NGX]***

|  |  |
| --- | --- |
| **● Siegeworks (now Optiv) [Livermore, CA]** | **1/2005-12/2006** |
| **Technical Training Director/Training Developer** |  |

Upon to returning back to Siegeworks, was designated the “non-ATC Technical Training Director” at Siegeworks/Fishnet. The students comprised of security personnel in Fortune 500 clients security departments; Developed security training curriculum, catalog and schedules for Siegework/Fishnet’s professional program directed primarily at Fishnets’ Fortune 500 clients’ IT security personnel in areas of SOX, SB 1386,CISSP Prep, Security Policy writing, Network penetration testing, Linux Security, etc. Developed course materials/labs (slides/readers/handouts/laptops and lab station materials); Provided a large portion of tech training to customers in-house (and at customer sites); Defined and tracked customer training needs/student progress via database; Coordinated customer training engagement/schedules; Used customer/students feedback in providing new courses and materials; Custom curriculum development for specific customers; Collaborated with partners who share similar visions and goals in the area of training to provide students a richer class experience via telephone conference discussion of case studies w/ vendor partners’ frontline engineers; Development of fishnet e-learning offering via “virtual machines” using VMware Workstation; Administration of company’s development and production environment

***[Solaris 10, Fedora 5.x, Win2K3 (server), OSX, MySQL, SQLserver2000]***

|  |  |
| --- | --- |
| **● Skybox Security [San Jose CA]** | **5/2004-4/2005** |
| **Professional Services** |  |

Professional Services consultant at Skybox *on loan from Siegeworks*; Administered company’s development and production environment; Evangelize Skybox products line (in front of customers and industry shows/events); Provided tech training to customers and VARs/Channels; Produced training material for above; Provided tech support during pilots and deployments of company’s LAMJ stack (Linux 9/Apache1.x/Jboss 4.x/MySql3, 4)-based product for customers’ production environments; Provided integration help and support with customers’ internal systems; Helped sales team forecast, track and report on attainment of sales objectives given customer interest; Augmented company intranet with knowledge base of product line; Developed training curriculum for channel partners; Define and track customer pilots and deployments; Provided feedback to development team on customer requests and bug reports.

***[Solaris 9, Fedora 4.x, Win2K3 (server), Jboss 4.x, Skybox view 2.0, and LAMJ]***

|  |  |  |  |
| --- | --- | --- | --- |
| **● Siegeworks (now Optiv) [Livermore, CA]** | | **5/2003-5/2004** | |
| **Business Development Manager / Technical Marketing Engineer** |  | |

Oversee “startups incubation” efforts for Siegeworks; Evangelized the latest Siegeworks’ security solution offerings; Act as a catalyst in lining up the development of 3rd party vendors' solutions with Siegeworks roadmaps; Provide the tech. security training to customers; Ensure the inclusion of methodology based implementation of technology in business systems; Define and track customer projects; Support and initiate engagement strategies and collaborate projects with customers and vendors; Drive internal and external technical resources to ensure customer projects are successfully executed; Act as a technical consultant and owner to drive and manage technology-driven customer projects; Product positioning; Instructing computer forensics, CISSP-Prep and SSCP Courses

***[Solaris 9, Fedora 4.x, Win2K3 (server), Analysis of various security startup products]***

|  |  |
| --- | --- |
| **● Centrata (now Lontra) [Redwood Shores, CA]** | **2/2002-5/2003** |
| **Quality Assurance: HA/Performance Manager** |  |

As performance/HA manager at Centrata Inc., I oversaw the infrastructure architecture of their flagship application and its security, high availability and performance implementation. Administered company’s development and production environment

***Internally*** Set off to redesign the infrastructure of the flagship application of the company by comparing and contrasting various topologies for the app through a bake-off—experimenting with Tomcat, Jboss 3.2.5 and Weblogic 6.1 which we eventually standardized on (migrating to 7.x and later); Redesign of the network topology of this multi-tiered JAVA 1.3.x persistent EJB based application (composed of firewall/F5 HA+/Iplanet webserver [SUNONE], Iplanet directory server 5.1, 2 layers of Weblogic server 6.1, 1 layer Weblogic integration, Oracle 8.1.7 in a Veritas High Availability cluster); Use of Rational Rose visual UML authoring tool (as part of "Rational Suite Development Studio for UNIX" by Rational Software). Research of the security consideration in Syndicating Content and recommendation for the architecture of the data flows vis-a-vis access control. These results were shared with the development team to Architect the data flows to reflect these constraints; Installation and integration of the "weekly build" on a High Availability stack and testing of the application for H/A. component failure to make sure that various application components would properly fail over; Data Load of "the performance stack" database from XML data files. Manipulation of XML "raw data" to reflect changes in weekly database schema changes; Wrote detailed Test Plans for performance and HA including detailed test cases and test specifications. Ensured that all test results are documented; Testing of application for overall performance using tools such as Silk performer 6.1 (Segue) and Grinder (freeware). Reporting of metrics of results to development staff for bug fixes or redesign of components; instrumenting JVM with Jprobe to investigate memory leaks; Lead the effort to implement the High Availability installation of the company’s flagship product (DCOS 4.0) using Veritas Oracle HA (VCS) for the persistence layer of this multi-tier application; Wrote the Installation and User Guide for the product; Maintenance of company’s CVS (version management) repository; Manager of 3 build engineers

***Facing customers*** Installation of the company's first customer (reference site) with this multi-tiered application; Troubleshooting of "first install" issues in integration with customers' environments; Wrote white papers for delineation of best practices in installation/implementation of product as a multi-offering solution; Provided feedback to development team on customer requests and bug reports; Defined and tracked subsequent customer pilots and deployments.

***[Solaris 2.8, RedHat 7.2-3, Win2K, Oracle 8i, Silkperformer 6.1, Jprobe, BEA Weblogic 6 & 7]***

**Education:**

*UC Berkeley* Biophysics & Psychology, BS (All coursework not completed)

*Checkpoint Software* CCSA and CCSE

*Palo Alto Networks* Essentials 1,2 and Panorama

*MCSE* With 3 optional modules (DNS, SQLserver, IIS)

*UC Berkeley Extension* Advanced Mail Administration, UNIX Kernel Internals (tuning and Networking), Enterprise Security: Issues for Effective Systems Development, Extranet Security: Public Key Infrastructure and VPN for support of Distributed computing on the web.

*Symantec Veritas* All Veritas Certified classes including FirstWatch and VCS.

*Baltimore Technologies* Have taken all company offered courses, including KeySteps PKI methodology

*BlueCoat* ProxySG Administrator, ProxySG Professional, ProxyAV

*Qualys* Certified on ver 6.x & 7.x

*Sourcefire Certified on 5.x*

*Currently* Working on my CISA certification

*SANS Institute/CIS* Various classes: Ranging from “exploitation techniques” to “20 Critical Security Controls”