
SUMMARY

An accomplished IT management professional with over 20 years of progressive technical and management experience consulting, implementing, and administering secure IT operations within complex working environments.

EXPERIENCE

- Experienced foundational knowledge with Enterprise Infrastructure technologies and products across all types of WAN/LANs in multiple verticals. Financial, Health Care, Gaming, Retail, and Government.
- Enterprise/Hybrid/Cloud based systems/networks and infrastructures including development/migration of on-premises to cloud systems.
- Desktop lifecycles/management/application distribution/security for large enterprises
- In depth expertise of all commonly used Operating systems, including Microsoft Windows, dozens of linux flavors, Macintosh, UNIX, and Novell.
- Internal/External penetration and vulnerability testing and assessment scanning.

EMPLOYMENT HISTORY

NOVACOAST INC.

SENIOR SECURITY ENGINEER, NORTH AMERICA.

2012 - PRESENT

Security Consultant to medium and large organizations.

- Staff Augmentation Director of Engineering, Architecture, and Incident Response for amazing, large Hospital System, Columbus Ohio. Management and Corporate responsibilities, Engineering Implementation management and direction, Security Consulting on all aspects of security program and interdepartmental engagement.
- Staff Augmentation Information Security Manager for Regional Hospital System, Santa Barbara CA. Ground up security program initialization and implementation. Staff and Consultant management over several initiatives.
- Incident Response Team Leader for organizational Breach Response and Virus Outbreak events in several verticals
- Security Program audit and development for PCI regulatory compliance.
- PCI-DSS QSA Audits and GAP Analysis. SAQ, ROC, and AOC documentation and review.
- LogRhythm SIEM, Threat Intelligence Implementation and customer support. LCDE Certification.
- Cloud Security Assessments and best practices consulting. Virtual network implementations.
- Data Loss Prevention enterprise wide implementations and consulting in several business verticals.
- Technical Risk Assessments including Vulnerability Management and Analysis, and Red Team Penetration Testing.
- SEE RECENT PROJECTS PAGE 5

SANTA BARBARA BANK & TRUST

SENIOR SECURITY ENGINEER, SANTA BARBARA CA.

2007 - 2012

Interfaced with key business owners and project leads to ensure rapid and secure implementation of internal banking applications with minimal risk. Engineered and implemented new security solutions to improve security posture.

- **Vulnerability Assessments:** Participated in the design and execution of network and application vulnerability assessments and infrastructure scanning, manual exploitation of known vulnerabilities (with OWASP top 10 and SANS 25 in mind), security audits and remediation activities.
- **Penetration Testing:** Infrastructure and application penetration testing (internal and external perspectives), security research, protocol analysis, password cracking, social engineering methods, OS hardening, infrastructure devices, wireless security, implementation of encryption and authentication methods.
- **Intrusion Detection (IDS):** Incident Response to malicious network traffic detected by IDS systems and vulnerabilities detected by scanners. Tracked and manually remediated such events. Documented via ticketing systems, and remediated via incident response procedures and investigations.
- **Regulatory Compliance:** Experience in using and/or implementing the generally accepted Information Security control frameworks (i.e., ISO 27001, COBIT, ITIL, and NIST) Experience conducting information security engineering activities in a regulated environment (e.g., SOX, GLBA, PCI, HIPAA)
- **VMWare:** Administer 35+ Windows/Linux guests and 4 ESXi5 Hosts in support of the Enterprise Security Department using vCenter and multiple tools (Veeam, VMMA, VUM) Automated staging, backup, remediation at host level. Fault Tolerance, High Availability, and automated distributed failover to shared storage.
- **Linux/Windows System Administration:** Scripted automation of windows, sysprepped imaging, Puppet, LAMP/WAMP servers, Backtrack, Netvision Active Directory Auditing, Novell eDirectory, Identity Manager.
- **Real Time Network Monitoring & Alerting:** Monitored enterprise events with Splunk, Snare, Netvision, Nagios, syslog, SNMP, WMI, vCenter, and custom correlation/scripting for automated alerting. Custom development of real time automated security dashboard for organization.

SANTA BARBARA BANK & TRUST

IDENTITY MANAGEMENT ADMINISTRATOR, SANTA BARBARA CA.

2007 - 2013

- **Identity Management:** Manage and administer automated XML framework and processes for provisioning users and password replication across several heterogeneous systems automatically; including AIX/Linux Local Users, DB2/MSSQL/MySQL Databases, and Active Directory.
- Interfaced with auditors and compliance officers to achieve compliance is various financial
- **PHP/MySQL/HTML/CSS:** (LAMP/WAMP) Implemented real time dash board for single information point of logs and databases by integrating Novell Identity Manager and MySQL.

NOVACOAST INC.

PROJECT MANAGER & SECURITY ENGINEER, NATION WIDE.

2002 - 2007

Project Manager, Field consultant and Pre-Sales/Post-Sales Engineer with broad experience base and skillset with large network infrastructures; Microsoft, Novell, and Linux based products. Specializing in Netvision's NVMonitor, ZENworks, Identity Manager, Novell Audit and Sentinel. Created a security practice around monitoring products:

- **Organized and supervised** teams of engineers on software implementations while managing client expectations throughout both the sales and engineering/implementation processes.
- **Developed NVPAR** (Netvision Packaged Auditing and Reporting) **Security Practice** providing initial virtual sales demos and virtualized proofs of concept to implementation, documentation, training, and support.
- **Pre-Sales and Post-Sales** implementations of large scale desktop OS, application packaging and rollout efforts.
- Implemented Novell DirXML for large scale Active Directory and eDirectory synchronizations.
- Maintained **vendor and partner relationships**; Netvision, Novell, Symantec, and supported their sales representatives on sales calls nation-wide and numerous trade shows and conferences.
- Routinely assisted client/sales executives on sales calls and took part in the overall relationship with the client.
- Commissioned Engineer averaging **\$20,000 a month** in billable service and support time.

COMMISSION JUNCTION

SENIOR SECURITY ADMINISTRATOR, SANTA BARBARA CA.

2000 - 2001

- **Supervised/mentored team** of 4 engineers responsible for daily IT helpdesk, desktop, and server support.
- Administrator of 6 servers and 200 workstations. Responsible for the Microsoft and Novell Infrastructure: Administrator of Novell Groupwise, eDirectory, and ZENworks, Microsoft Active Directory, Symantec Anti-Virus, SMTP Mail Gateway, and Veritas Backup solutions.
- **Security policy development.** Documented policies and procedures, baselines, and systems configurations.

NOVACOAST INC.

SALES/SECURITY ENGINEER & PROJECT MANAGER, SANTA BARBARA CA.

1997 - 2000

- **Staff Augmentation Manager** of 6 subcontractors in desktop and server support for large government organization of 35+ locations for 18 months. Participated in interviewing, onboarding, and terminations of vendors and contractors within our placement services group.
- **Pre-Sales/Post-Sales** Engineer focused on Apple, Microsoft, and Novell core technologies/server operating systems and applications including desktop management lifecycles, directory technologies, databases, email, and more.

EDUCATION AND CERTIFICATIONS

- PALO VERDE HIGH SCHOOL BLYTHE CA 1988-1992
- UNIVERSITY OF CALIFORNIA AT SANTA BARBARA, B.A. LAW & SOCIETY – CRIMINAL JUSTICE 1992-1997

<u>CERTIFICATE</u>	<u>DATE</u>
1. Certified Novell Administrator 5 (CNA5)	April 11 th , 2000
2. Certified Novell Engineer 5 (CNE5)	June 20 th , 2000
3. Novell Specialist: Border Manager	February 26 th , 2001
4. Master Certified Novell Engineer (MCNE)	June 5 th , 2001
5. Certified Novell Engineer 6 (CNE6)	September 16 th , 2002
6. Microsoft Certified System Administrator 2000 (MCSA)	January 6 th , 2003
7. Citrix Certified Administrator (CCA)	February 27 th , 2003
8. CompTIA Linux+	May 22 nd , 2007
9. Certified Information Systems Security Professional (CISSP)	August 2009
10. Certified Ethical Hacker (CEH)	May 28 th , 2010
11. Microsoft Certified TS: (MCTS) Windows 7	May 17 th , 2011
12. Tenable Certified Nessus Auditor (TCNA)	August 11 th , 2011
13. VMware Certified Professional (VCP5)	May 28 th , 2012
14. VMware Certified Associate (VCA-WM)	October 30 th , 2013
15. VMware Certified Associate (VCA-Cloud)	October 27 th , 2013
16. VMware Certified Associate (VCA-DCV)	October 27 th , 2013
17. Symantec Sales Expert	
a. Symantec Control Compliance Suite (CCS)	September 21 st , 2013
b. Symantec Data Loss Prevention (DLP)	October 23 rd , 2013
c. Symantec Endpoint Protection (SEP)	October 24 th , 2013
d. Symantec Critical System Protection (CSP)	October 4 th , 2013
18. Symantec Sales Expert +	
a. Symantec Control Compliance Suite (CCS)	September 23 rd , 2013
b. Symantec Data Loss Prevention (DLP)	October 30 th , 2013
c. Symantec Endpoint Protection (SEP)	October 27 th , 2013
19. Payment Card Industry (PCI) Qualified Security Assessor (QSA)	May, 2014
20. Payment Card Industry Professional (PCI-P)	May, 2014
21. LogRhythm Certified Deployment Engineer (LCDE)	May, 2016

RECENT PROJECTS

Staff Augmentation

- Director of Engineering, Architecture, and Incident Response - Large Ohio Based Hospital System
- Information Security Manager - Regional Santa Barbara Based Hospital System

Security Assessment and Penetration Testing

- Security Assessment and Consulting for 3 of the top 10 banks in the world.
- Large Movie and Media company Incident Response to State Sponsored Breach
- Large Gulf Coast Casino: Internal Security Assessment/Penetration Test, and PCI Gap Analysis.
- Large West Coast Travel Agency: Internal Security Assessment/Penetration Test, and PCI Gap Analysis.
- Regional Hospital: Internal Security Assessment/Penetration Test, and HIPAA Gap Analysis.
- Large Las Vegas based Casino successful Penetration Testing

Symantec Data Loss Prevention

- Federal Department DLP Implementation and Tuning, Washington DC
- Nationwide Health Insurance DLP Implementation
- Nationwide Retail: Symantec DLP Risk Assessment and PCI Gap Analysis
- Fortune 100 Retail: Symantec DLP Internal Risk Assessment and Internal Proof of Concept
- Multiple Demos/Proofs of Concept for DLP

LogRhythm Security Information and Event Management (SIEM)

- Large Regional Hospital Implementation
- Large Casino Implementation and Support

WORK EXPERIENCE INFORMATION

Novacoast Inc.
1505 West Chapala Ave, Santa Barbara CA 93103
800-949-9933

Santa Barbara Bank & Trust
400 North Fairview Ave, Goleta CA 93117
(Acquired by UNION Bank 2013)

Skillset matched to [OhioHealth SANS Top 20 Initiatives](#).

1	Inventory of Authorized and Unauthorized Devices	Altiris/ZENWorks/SCCM and scripting background
2	Inventory of Authorized and Unauthorized Software	Altiris/ZENWorks/SCCM and scripting background
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	CISSP/PCI
4	Continuous Vulnerability Assessment and Remediation	Nessus Certified, Security Assessment/PenTesting background. All windows OS update and remediation/application deployment and distribution
5	Malware Defenses	Symantec SEP Certified, Threat and Malware Analysis
6	Application Software Security	Penetration testing, and development background
7	Wireless Access Control	Security Architect and Infrastructure background
8	Data Recovery Capability	Experience with multiple vendors
9	Security Skills Assessment and Appropriate Training to Fill Gaps	Over 20 certifications and 20 years of experience
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Networking background, CISSP/QSA
11	Limitation and Control of Network Ports, Protocols, and Services	Networking background, CISSP/QSA
12	Controlled Use of Administrative Privileges	Identify Management Background, BeyondTrust Implementation
13	Boundary Defense	Heavy SIEM with misc IDS and firewall background
14	Maintenance, Monitoring, and Analysis of Audit Logs	Logrhythm Certified, Splunk familiarity, ELKStack
15	Controlled Access Based on the Need to Know	CISSP/QSA Security background
16	Account Monitoring and Control	Netvision, Logrhythm, Novell Audit, Sentinel, Quest InTrust, Master Novell CNE
17	Data Protection	Symantec DLP Certified
18	Incident Response and Management	Response to multiple verticals for breach and virus
19	Secure Network Engineering	Security Architect and Infrastructure background
20	Penetration Tests and Red Team Exercises	Red Team PenTester and Responder

Upcoming Efforts at [OhioHealth](#)

Identity and Access Management PAM	6 Years of Experience Administering over 30 connected and synchronized systems. Extensive Active Directory experience and knowledge. Oracle administration experience. Implemented BeyondTrust for PAM. Years of Identify Auditing and Monitoring.
Payment Card Industry (PCI)	Current CISSP and PCI QSA. Performed numerous GAP Analysis and Remediation/Compliance efforts
Vulnerability Management	Dozens of PenTesting and Security Assessment engagements, with follow on Remediation - LAMP Stack Analysis of Vulnerability Results.
Splunk	Extensive LogRhythm SIEM experience implementation and administration. Splunk implementation and analysis experience for investigation and response.
Cloud	Amazon AWS security consulting, design, deployment of cloud based networks.