Abbate Antonino

IT SECURITY & OPERATIONS ENGINEER

https://it.linkedin.com/in/antoninoabbate

Gualdo Tadino (Perugia), Frazione S. Pellegrino - Tel. 335 7495476 - ninoabbate@gmail.com - Date of birth 08/03/1983

Who I am

I am an IT Operations and Security passionate, I like to improve my knowledge and to face the daily challenges, I prefer to do the things instead of saying “it can’t be done”, taking care to propose technical solutions to resolve the problem.
I would like to have the opportunity to work on a Management role in IT Operations and Security areas, what I can guarantee is passion, commitment, availability, competence and a big desire to get involved in a interesting project.

Experience

Operations Engineer

Vendini (via Jessup s.n.c. - Gualdo Tadino (PG) - 660 Market st. - San Francisco (CA) - USA)

03/2015 - Today

I'm part of Vendini Operations team, I'm focused on monitoring, logging and security solutions, but not limited on these areas. I do often evaluations of new technologies and applications to improve our infrastructures.
- Main activities -
Engineering, management, configuration and troubleshooting of: Network and Security devices (Cisco switches and Routers, Arista Network switches, A10 load balancers, Palo Alto firewalls), Dell and VMware ESX servers, AWS services (EC2, RDS, ELB, S3, CloudFront, etc...), Development environments (Vagrant and Virtualbox), Docker containers, Linux (CentOS, Ubuntu) and Windows Servers, NIDS (snort), HIDS (ossec), SIEM (Snorby), MTA Message Systems Momentum, Source Control (git), Configuration Management (Puppet/Chef), Deployments (Jenkins), Continuous Integration (Codeship, Travis CI). External services: Pingdom, Sendgrid, Twilio, Edgecast CDN, Queue-it, UltraDNS, DNS made easy, Jira, Slack, GitHub, BitBucket, DockerHub, Pagerduty, Easypost,etc..
Monitoring and Graphing: Nagios, Zabbix, Icinga, Shinken, Cacti, Graphite, Grafana, ELK stack (Elasticsearch, Logstash, Kibana), Splunk.
Systems management includes all services correlated: Webservers Apache,NginX, DBservers MySQL, mariadb, Percona, Redis, Bind DNS, NTPd, Sendmail/Postfix, rSyslog, proxy Squid, iptables, OpenLDAP, Memcached, Sphinx, etc.. and on Windows: Active Directory, MS DNS, IIS, MSSQL, ColdFusion, Fusion Analytics, etc..
Vulnerability Assessment, Penetration Testing, Hardening, Security Governance (PCI-DSS), Risk Assessment, Patch Management, Asset Management, Identity & Access Management, Incident Response Plans.
Configuration and Source management, Continuous Integration, Scripting and (not so often) programming. Working using Agile methodologies following the SCRUM approach. Oncall duties.
Writing documentation and wiki, incidents management, Post Mortems, technical solutions.

I've completed and put in prodution two projects:

- Corporate IDS infrastructure
- Corporate Logs Monitoring infrastructure

IT Security & Compliance Engineer

Xaos Systems - *Consultant at Telecom Italia (Rome - Acilia, via Macchia Palocco 223)*

12/2013 – 02/2015

I am been the IT Security & Compliance responsible for Telecom Italia Sparkle, Network Operations department.
The main goal was to make the customer pass the external Security Audit, so my duties were thus to verify the current status of IT compliance in production infrastructures and to resolve the security gap before the external audit.
To do so I performed a Risk Assessment and an internal Security Audit. The results of these two activities helped the customer to focus on security issues and made me continue the activities doing a Gap Analisys and a Remediation Plan which were focused on: Patch Management, Hardening, Network flows revision, Users revision and Security documentation.
I helped the customer during the external security audit and I have been successful to make pass them the audit.
Since i was part of the production Network Operations team, I have been involved on management of all customer infrastructures: over 500 servers that provided mobile and network services, these applications run on Linux, HP-UX, Solaris and Windows Server, there were also database servers MySQL and Oracle. The monitoring was done using HP OVO, we managed trouble tickets with Remedy.

Network Engineer

Xaos Systems - Consultant at Telecom Italia Sparkle (Rome - Acilia, via Macchia Palocco 223)

10/2013 – 11/2013

I was part of Network Operations, Delivery & Assurance department at Telecom Italia Sparkle. Main activities were: Project Management, configuring all Cisco routers for Telecom Italia Sparkle's customer DSV Saima Avandero (located all over Italy), testing connection between Telecom Italia Sparkle PE (provider equipments) and DSV network, full support to customer (providing also documentation about hardware installation) in order to achieve full connectivity from customer equipments to internet and configuring Telecom Italia Sparkle's internal equipments (DNS, Syslog, Nagios, Cacti, Cisco Works) to manage all the routers. I've been also involved in other projects that required knowledge of WAN, VPN (Ipsec, ISAKMP, tunnels) and AAA (using Cisco Secure ACS).

Network & Security Engineer

Xaos Systems - Consultant at MiBACT (via Michele Mercati 4, Rome)

07/2013 – 08/2013

The main activities were thus to monitoring the network with DartWare Intermapper, providing Security services with McAfee ePolicy Orchestrator platform, Fortinet Firewalls Appliances Fortigate 3600A – 50A – 60C (configuration and troubleshooting), McAfee Appliance Intrushield NIDS M-1450 (configuration, troubleshooting, tuning), Fortinet FortiAnalyzer Network Security Reporting, Logging and Analyzing devices (configuration and troubleshooting), Switches Cisco Catalyst 3550, 4506 (configuration and troubleshooting).

Network Security & Systems Engineer

Xaos Systems - Consultant for Hewlett Packard at Bank of Italy (via Mario Bianchini 68, Rome - via Giamaica 7, Pomezia - Rome)

01/2007 – 06/2013

My role in this project was managing Bank of Italy's external network and services, providing also Security services.
I managed Hewlett-Packard servers (HP Proliant series) with Windows Server 2000, Windows Server 2003 and all the services correlated to be in charge to this server farm. My skills were thus to manage/configure TrendMicro InterScan Messaging Security Suite (Mail-relay servers), TrendMicro Interscan Web Security Suite (WebScan/Proxy servers), TrendMicro Server Protect and Control Manager servers, Dnews NNTP servers, Globalscape Secure FTP servers, Cisco Works severs, Juniper Netscreen 208 and 25 firewalls (configuration and troubleshooting), Cisco IDS 4235 and 4215 sensors (configuration, troubleshooting and tuning), Cisco 2950 switches. Above all I've been dealing with OpenSTM 3.2, a security correlation platform that has the will to handle, correlate and generate security alerts from differents security devices (IDS, Firewalls, TrendMicro products). I monitored all infrastructure with HP NNM - OVO (installation, configuration, troubleshooting and tuning) , Cisco VMS 2.2 with knowledge of IDSMC 2.1 module to deal with Cisco IDS sensors. MRTG graph collection and systems/security reporting (every day security, every month global infrastructure). Making Vulnerability Assessment, Penetration Testing and Auditing of all infrastructure were mandatory at least once a year, we used Nessus to perform these tasks.

Network Engineer

Xaos Systems - Consultant for Hewlett Packard at Wind (via Carlo Veneziani 56, Rome)

07/2006 – 12/2006

Main activities in DCN department were: configuring and managing Cisco, Intel, 3com and Juniper network equipments (over 500 nodes). Most of the time involved in L2/L3 troubleshooting in Wind DCN network, gaining knowledge of the following IP routing protocols: BGP, OSPF, EIGRP and also have knowledge of switching technologies in big environments.

Network Engineer

Xaos Systems - Consultant for Hewlett Packard at Prime Minister Council (via della Mercede 9, Rome)

01/2006 – 06/2006

Main activities were: configuring and managing Cisco, HP, Cabletron, Avaya network equipments. Most of the time involved in L2/L3 troubleshooting on Prime Minister Council network, gaining knowledge of the following IP routing protocols: BGP, OSPF, EIGRP and also have knowledge of switching technologies in big environments.

ECDL Instructor, Web developer

Unione Italiana Ciechi (via Brunaccini 1, palazzo Brunaccini - Alì - ME)

10/2004 – 08/2005

I taught ECDL modules to blind and visually impaired students, I've also developed their website in order to meet W3C standards (usability and accessibility), moreover I developed a stand-alone program (for microsoft windows) that describes (using automated synthetic speech) html pages browsing with Microsoft Internet Explorer.

Hard Skills

Project Management
Data Center
Iaas, PaaS, SaaS
Service Management
Disaster Recovery
Monitoring & Reporting
CRM (Customer Relationship Management)
Agile Methodologies

Soft Skills

Flexibility
Teamwork
Time management
Motivation
Leadership
Curiosity
Availability
Communication

Technical Skills

IT Security

Firewalls: Cisco, Juniper,Fortinet, PaloAlto, iptables
NIDS/IPS: Cisco, McAfee Intrushield, Snort,HIDS: Ossec, SIEM: Snorby,
OpenService OpenSTM (Secure Threat Manager),NAC: Cisco Secure ACS, RSA ACE/Server, VPN, AAA, PSK/PKI, 802.1x
Antivirus: McAfee ePolicy Orchestrator, TrendMicro Server Protect, Symantec Endpoint Protection, ClamAV
TrendMicro InterScan Web Security Suite, TrendMicro InterScan Messaging Security Suite
Hardening, Patch Management, Vulnerability Assessment, Penetration Testing, Incident Response Plans,Risk Assessment
Metasploit, Nessus.

Security & Compliance

Italian Privacy Code (D.lgs. 196/03), ISO 27001, PCI-DSS, OWASP.

Network Engineering

ISO/OSI Protocol Stack: IP, IPX, NetBIOS, IPv6
Routing: RIP, IGRP, EIGRP, OSPF, BGP
LAN/MAN: Ethernet, Token Ring, VLANs, R/MSTP, HSRP, VRRP
WAN: ATM, Frame-Relay, X.25
Appliance Cisco, Juniper, HP, Arista Networks, A10

WLAN

802.11 a/b/g/n, Radius 802.11 a/b/g/n auth infrastructure.

Network Management & Monitoring

HP NNM, OVO, Cisco Works, Cisco Prime Infrastructure, Cisco VMS, DartWare Intermapper, Nagios, Zabbix, Icinga, Shinken.

Reporting,Graphing,Logging

Fortinet FortiAnalyzer, TrendMicro Control Manager, MRTG, Cacti, Graphite, Splunk, ELK stack (Elasticsearch, Logstash, Kibana), Grafana.

Virtual Environments, IaaS, Containers

Vmware, Citrix, VirtualBox, Vagrant, Docker, Amazon Web Services

Source & Configuration Management, Continuous Integration, Deployment

Git, Puppet, Chef,Travis CI,Codeship, Jenkins

Operating Systems

MS-DOS/NT/Windows/Windows Server
Distribuzioni Linux/Linux Enterprise
HP-UX, Solaris
MacOS/X

DBMS,Cached,Indexers

MySQL, Percona Server, mariadb, Redis, Memcached, Sphinx

Scripting & Programming

Bash, Powershell, PHP, C, Java

Services

DNS, FTP, NTP, NNTP, Syslog, LDAP, DHCP, WINS, Network Load Balancing, Clustering, MTA,Webservers, Proxy, Antivirus, etc..

Education

University of Messina – Science Information Technology

09/2001 - 07/2005 Degree with 104/110 final grade

Principal skills acquired: Information technology basics, mathematical analysis, statistics analysis, Physics and Electronics.
Gained in depth knowledge of programming (C, C++, Assembler, Fortran);
Gained in depth knowledge of Databases, designing in SQL;
Gained in depth knowledge of Networking, designing networks, Network Security, Security policy implementation, with practice on Cisco appliances;
Gained in depth knowledge of Web, implementation of W3C standards;
Gained in depth knowledge of Operating Systems.

University of Rome "La Sapienza" - Science - Information Technology Master Degree Course

09/2005 - 07/2007 Some exams done (5/12). Course interrupted

Courses

Cisco Certified Network Associate (CCNA)
Cisco Fundamentals of Network Security
Cisco Fundamentals of Wireless Lans
Openmind Networks SMS Firewall
Cisco Prime Infrastructure
Indipendent course: Splunk
Message Systems University – Momentum 4
ITILv3

Projects

Vendini Logs Monitoring Infrastructure
Vendini Intrusion Detection Systems Infrastructure

Languages

Italian
Native

English
Read: Professional working proficiency
Write: Professional working proficiency
Spoken: Professional working proficiency

French
Read: Basic
Write: Basic
Spoken: Basic

References upon request