Abbate Antonino

Network/IT/DevOps & Security Engineer

https://it.linkedin.com/in/antoninoabbate
https://*github.com/ninoabbate*
https://hub.docker.com/u/aabbate
http://www.antoninoabbate.pro

Sarcedo (Vicenza), Via Monte Summano, 25 - Tel. 335 7495476 - antonino.abbate@thei.it - Data di nascita 08/03/1983

Chi sono

Sono appassionato di IT Operations e Sicurezza Informatica, sono una persona curiosa, mi piace acquisire conoscenze tecniche e migliorarmi continuamente. Prediligo l'approccio del "si può fare" premurandomi di proporre soluzioni al problema.
Da luglio 2017 ho avviato la mia ditta individuale THE I (www.thei.it), che fornisce i seguenti servizi:

- Ingegneria delle infrastrutture
- Systems integration
- Migrazioni ed aggiornamenti di datacenters / infrastrutture / servizi / piattaforme / applicazioni
- Deployments
- Project Management
- Information Security (PCI-DSS, ISO27001, NIST, OWASP)
- Service Management
- Cost Analysis, Cost Saving e relativa re-ingegnerizzazione
- Servizi di monitoraggio

Sono disponibile a collaborare come contractor (Partita IVA) in tutto il mondo.

Esperienze Lavorative

Operations Engineer

Vendini (100% remoto - 660 Market st. - San Francisco, California - USA) *03/2015 - oggi*

Faccio parte del team Operations di Vendini, mi occupo della ingegnerizzazione e gestione di tutte le infrastrutture informatiche che erogano servizi. Mi occupo altresì della valutazione ed implementazione di nuove soluzioni infrastrutturali.
Le attività principali sono le seguenti :
Gestire, configurare ed effettuare troubleshooting di apparati di rete e sicurezza (switch e routers Cisco, switch Arista Network, Load Balancers A10 Networks, Firewalls Palo Alto), Servers Dell, VMware ESX Servers, Servizi AWS (EC2, RDS, CloudWatch, S3, CloudFront, ecc.), Ambienti di sviluppo (Vagrant e Virtualbox), containers Docker, Sistemi Linux CentOS, Ubuntu e Sistemi Windows Server, NIDS (snort) e HIDS (ossec), SIEM (Snorby), MTA Message Systems Momentum, Source Versioning (git), Configuration Management (Puppet/Chef), Deployments (Jenkins), Continuous Integration (Codeship, Travis CI). Servizi esterni quali: Pingdom, Sendgrid, Twilio, Edgecast CDN, Queue-it, UltraDNS,

DNS made easy, Jira, Slack, GitHub, BitBucket, DockerHub, Pagerduty, Easypost,ecc..
Monitoring e Graphing: Nagios, Zabbix, Icinga2, Shinken, Cacti, Graphite, Prometheus, Grafana, ELK stack (Elasticsearch, Logstash, Kibana), Splunk.
La gestione dei sistemi include: Webservers (Apache, NginX), DBservers (MySQL, mariadb, Percona), InfluxDB, OpenTSDB, Redis, Bind DNS, NTPd, Sendmail/Postfix, rSyslog, Squid, iptables, OpenLDAP, Memcached, Couchbase, Sphinx, Consul, ecc.. e su piattaforme Windows: Active Directory, MS DNS, IIS, MSSQL, ColdFusion Application server, Fusion Analytics, ecc..
Effettuo attività di Vulnerability Assessment, Penetration Testing, Hardening, Security Governance (PCI-DSS), Patch Management, Asset Management, Identity & Access Management, Incident Response Plans. Configuration e Source management, Continuous Integration, Scripting e sviluppo software.
Fornire documentazione relativamente a risoluzione degli incidenti e gestione ed evoluzione delle infrastrutture.
Ho portato a termine svariati progetti utilizzando metodologie Agile seguendo l'approccio SCRUM. Effettuo saltuariamente la reperibilità.

IT Security & Compliance Engineer

Xaos Systems - *Consulente per Telecom Italia (Sede di Roma - Acilia, Via Macchia Palocco 223)*

12/2013 – 02/2015

Ho ricoperto il ruolo di responsabile Security & Compliance per Telecom Italia Sparkle dipartimento Network Operations.
L'obiettivo principale per cui sono stato impiegato nel gruppo di Performance and Network Maintenance è stato quello di verificare che tutte le infrastrutture informatiche di Telecom Italia Sparkle garantissero i requisiti di sicurezza previsti dalle normative vigenti e dalla Compliance IT del gruppo, in previsione del successivo audit di sicurezza. Per fare ciò mi sono occupato preliminarmente di effettuare le seguenti attività: Inventory di tutte le infrastrutture, inventory di tutte le utenze, revisione di tutte le policy di sicurezza aziendali in vigore, revisione di tutte le attività di Risk Assessment, Vulnerability Assessment e Penetration Testing già effettuate. Successivamente (prima dell'audit) ho provveduto ad effettuare Patch Management , Hardening, revisione dei documenti e nomine del gruppo, revisione delle utenze, revisione dei flussi di rete, verifica dei certificati SSL. In fase di audit ho partecipato attivamente alla risoluzione di tutte le richieste degli auditors facendo sì che l'audit venisse superato positivamente. Durante le attività di sicurezza sono stato anche impiegato nella gestione di tutte le infrastrutture di esercizio di Telecom Italia Sparkle. Principalmente si trattava di sistemi (circa 500) che fornivano servizi di telefonia mobile e servizi di rete IP: applicativi forniti da vendors quali F5, Italtel, Urmet, Alcatel-Lucent, Openmind Networks. Sistemi Linux e una minima parte HP-UX, Solaris e Windows Server, vi erano anche in gestione database server Oracle e MySQL. Effettuavo anche il monitoraggio delle infrastrutture tramite HP OVO ed utilizzavo Remedy TTMS per la gestione degli incidenti.

Network Engineer

Xaos Systems - Consulente per Telecom Italia Sparkle (Sede di Roma - Acilia, Via Macchia Palocco 223)

10/2013 – 11/2013

Le attività svolte per questo progetto nel gruppo Network Operations Delivery & Assurance di Telecom Italia Sparkle includevano attività di Project Management, configurazione di tutti i routers (Cisco 887) per DSV Saima Avandero (ubicati in varie località in Italia), configurazione e testing

della connettività tra Telecom Italia Sparkle e la rete DSV (per tutte le sedi). Pieno supporto al cliente (fornendo anche la documentazione di installazione) in modo da garantire la connettività tra i vari apparati del cliente ed internet. Configurazione delle piattaforme interne di Telecom Italia Sparkle per la gestione degli apparati (DNS, Syslog, Nagios, Cacti, Cisco Works). Sono stato coinvolto anche in altri progetti in cui si richiedeva la conoscenza di: WAN, VPN (Ipsec, ISAKMP, tunnels) e AAA (Cisco Secure ACS).

Network & Security Engineer

Xaos Systems - Consulente per MiBACT Direzione Generale per i Beni Librari, gli Istituti Culturali ed il Diritto d'Autore (Sede via Michele Mercati 4, Roma)

07/2013 – 08/2013

Le attività svolte nel presidio di rete e sicurezza consistevano nel configurare e gestire l'infrastruttura della Direzione Generale per i Beni Librari, gli Istituti Culturali ed il Diritto d'Autore. Le mie mansioni sono state quelle di monitorare l'intera infrastruttura tramite DartWare Intermapper, configurare la piattaforma McAfee ePolicy Orchestrator (che gestisce i seguenti software McAfee Antivirus e Antispyware Viruscan Enterpise, McAfee Intrusion Prevention System, NAC Security Manager, Site advisor enterprise) per il monitoraggio delle postazioni di lavoro del ministero, configurazione e gestione Switch Cisco Catalyst 3550, Catalyst 4506, Firewall Fortinet Fortigate 3600A – 50A – 60C (configurazione policies e troubleshooting), McAfee Intrushield NIDS M-1450 (configurazione, troubleshooting, tuning), Piattaforma di network security logging, reporting e analisi FortiAnalyzer.

Network Security & Systems Engineer

Xaos Systems - Consulente per Hewlett Packard per il progetto SINTESI Banca D'Italia presso HP (Sede Via Mario Bianchini 68, Roma - successivamente in Via Giamaica 7, Pomezia)

01/2007 – 06/2013

Il mio ruolo in questo progetto prevedeva la gestione delle infrastrutture di Banca d'Italia maggiormente esposte su internet come i servizi di posta elettronica e navigazione, era a mio carico anche la gestione della sicurezza informatica.
Le attività svolte nel presidio includevano la gestione dei Windows Servers HP e tutti i servizi ad esso correlati: servizi di posta (TrendMicro Interscan Messaging Security Suite), servizi di WebScan Proxy (TrendMicro Interscan Web Security Suite), servizi NNTP (DNEWS), servizi SFTP (Globalscape), la gestione degli apparati di rete Switch Cisco 2950 (configurazione e troubleshooting), Firewall Juniper Netscreen 25 - 208 (configurazione e troubleshooting), NIDS Cisco IDS 4235 - 4215 (configurazione, troubleshooting, tuning). Monitoraggio di rete e sicurezza: piattaforma SIEM Openservice OpenSTM (Secure Threat Manager) (installazione, configurazione e troubleshooting), piattaforma di Node Management HP OVO (installazione, configurazione e troubleshooting) e NNM, CiscoWorks, Cisco VMS, MRTG. Effettuavo reperibilità 24/7. Attività di produzione report con cadenza giornaliera per quanto riguarda gli aspetti di sicurezza, e con cadenza mensile per l'intera infrastruttura. Provvedevo ad effettuare attività di Vulnerability Assessment almeno una volta all'anno utilizzando Nessus. Ho avuto un ruolo centrale nella migrazione di tutta l'infrastruttura avvenuta nel 2011 dal datacenter di Unicredit (Kyneste) a quello di HP Enterprise Services.

Network Engineer

Xaos Systems - Consulente per Hewlett Packard presso Wind S.p.a. (Sede via Carlo Veneziani 56, Roma)

07/2006 – 12/2006

Le attività svolte nel gruppo DCN di cui facevo parte consistevano nella gestione, configurazione e implementazione di oltre 500 nodi di cui era composta la rete DCN di Wind (svariati apparati di rete Cisco, Intel, 3com, Router Juniper Networks). L2/L3 troubleshooting.
Implementazione del core IP. Le attività richiedevano, tra l'altro, la conoscenza delle seguenti tecnologie e protocolli: IP routing (BGP, OSPF, EIGRP), LAN switching (VLANs, STP), Ethernet, Bridging.

Network Engineer

Xaos Systems - Consulente per Hewlett Packard presso la Presidenza del Consiglio dei Ministri (Sede via della Mercede 9, Roma)

01/2006 – 06/2006

Le attività svolte nel gruppo DCN di cui facevo parte consistevano nella gestione, configurazione e implementazione dei nodi della rete DCN della Presidenza del Consiglio dei Ministri (appartati di rete HP, Cisco, Cabletron, Avaya). L2/L3 troubleshooting. Implementazione del core IP. Le attività richiedevano, la conoscenza delle seguenti tecnologie e protocolli: IP routing (OSPF, EIGRP), LAN switching (VLANs, STP), Ethernet, Bridging.

Istruttore ECDL, Sviluppatore Web

Unione Italiana dei Ciechi e degli Ipovedenti (Sede Via Brunaccini 1, palazzo Brunaccini - Alì - ME)

10/2004 – 08/2005

Ho effettuato una collaborazione con il centro regionale Helen Keller nel periodo finale del percorso formativo universitario, le attività effettuate prevedevano l'insegnamento dei moduli ECDL ad utenti con disabilità visive e lo sviluppo del sito web del centro regionale Helen Keller seguendo le direttive di accessibilità consigliate dagli standard W3C. Come obiettivo finale per la tesi di laurea ho sviluppato un applicativo che descriveva i siti web in fase di navigazione, la descrizione veniva effettuata tramite una sintesi vocale.

Hard Skills

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

Soft Skills

Flessibilità
Lavoro di gruppo
Gestione del tempo
Motivazione
Leadership
Curiosità
Disponibilità
Comunicazione

Competenze Tecniche

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, 2FA, MFA, DuoProxy, SSL Management.
Attività di Hardening, Patch Management, Vulnerability Assessment, Penetration Testing, Incident Response Plans
Metasploit, Nessus.

Security & Compliance

Codice Privacy (D.lgs. 196/03), Provvedimenti del Garante per la Privacy, Compliance ISO 27001, PCI-DSS, OWASP, NIST.

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 Networks

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, Icinga2, Shinken.

Reporting,Graphing,Logging

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

Ambienti Virtuali,IaaS, Containers,Orchestrators

Vmware, Citrix, VirtualBox, Vagrant, Docker, Docker Swarm, Kubernetes, Amazon Web Services, Google Cloud Platform, Microsoft Azure

Source Versioning, Configuration Management, Continuous Integration, Deployments

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

Sistemi Operativi

MS-DOS/NT/Windows/Windows Server
Distribuzioni Linux/Linux Enterprise (Suse, RedHat, Centos, Debian, Ubuntu, Alpine), HP-UX, Solaris, MacOSX

DBMS,NoSQL,Cached,Indexers

MySQL, Percona Server, mariadb, sqlite, InfluxDB, Redis, Memcached, CouchBase, Elasticsearch, Sphinx

Webservers,Application Servers,CMS

Apache, Nginx, IIS, Coldfusion, Wordpress, Drupal

Scripting & Programming

Bash, Python, Powershell, PHP

Servizi

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

Ulteriori competenze

MS Office, Google G Suite, Jira,Confluence, Bitbucket, Github, DockerHub, Remedy, Slack, Skype, JSON, REST APIs, Pagerduty, Sendgrid, Twilio, Pingdom, Edgecast CDN e molti altri servizi e applicazioni SaaS/PaaS

Formazione

Università degli studi di Messina – Facoltà di Scienze MM.FF.NN – Corso di Laurea in Informatica

09/2001 - 07/2005 Laurea conseguita con votazione finale 104/110

La formazione universitaria in generale mi ha permesso di approfondire i concetti base dell'informatica e delle scienze matematiche, statistiche, fisiche ed elettroniche, principalmente focalizzando uno studio mirato alla:

- *Conoscenza ed applicazione di linguaggi di programmazione (C, C++, Assembler, Fortran);*
- *Creazione e gestione di basi di dati con progettazione in SQL;*
- *Conoscenza e progettazione di reti di calcolatori e implementazione di policy di sicurezza con pratica su apparati Cisco;*
- *Conoscenza delle tecniche di usabilità e accessibilità dei siti web;*
- *Conoscenza approfondita sui sistemi operativi*

Università degli studi di Roma La Sapienza – Facoltà di Scienze M.F.N – Corso di Laurea Specialistica in Informatica

09/2005 - 07/2007 Corso di laurea interrotto dopo aver effettuato alcuni esami (5/12)

Tramite la formazione magistrale avevo l'obiettivo di approfondire il grado di preparazione in importanti settori dell'informatica moderna, quali l'algoritmica, la matematica discreta, l'informatica teorica, la progettazione del software, l'intelligenza artificiale, la multimedialità, le reti e la sicurezza.

Corsi

Cisco Certified Network Associate (CCNA)
Cisco Fundamentals of Network Security
Cisco Fundamentals of Wireless Lans
Openmind Networks SMS Firewall
Cisco Prime Infrastructure
Seminario Web: Splunk
Message Systems University - Momentum 4
ITILv3
Microsoft Azure for AWS Experts
Google Cloud Onboard

Progetti

Vendini Logs Monitoring Infrastructures
Vendini Intrusion Detection Systems Infrastructure
Vendini Transact/Encrypt Monitoring Infrastructure
Vendini Post-Mortems Tracker
Vendini Incident Management Tracker
Vendini Network Devices Automatic Backup & Notification
Vendini CrowdTorch Costs Analisys, Costs Saving & Re-engineering

Contributi Opensource:
Etsy Opsweekly (https://github.com/etsy/opsweekly)
Prometheus SNMP Exporter (https://github.com/prometheus/snmp_exporter)
Docker Morgue (https://github.com/ninoabbate/docker-morgue)
Docker Opsweekly (https://github.com/ninoabbate/docker-opsweekly)
Docker SNMP Exporter Configuration Generator (https://github.com/ninoabbate/docker-secg)
Nagios Plugins (https://github.com/ninoabbate/nrpe-plugins)

Lingue

Italiano
Madrelingua

Inglese
Lettura: Ottimo
Scrittura: Ottimo
Esposizione orale: Ottimo

Francese
Lettura: Base
Scrittura: Base
Esposizione orale: Base

Sono disponibile ad inviare referenze su richiesta.