Alexandre Teixeira [alexandre.abreu@gmail.com]

Information Security professional with over 15 years of experience. Career includes senior roles in Security Architecture, Engineering and Operations, with the last 8-10 years focused on Threat Detection Engineering, Incident Response and SecOps. Currently working as an independent contractor (SME) in SIEM/Splunk domain for corporations in Europe.

Social Networks

https://linkedin.com/in/inode

https://medium.com/@ateixei // https://opstune.com/blog

https://twitter.com/ateixei (1300+ followers, mainly from Threat Detection and DFIR community)

https://github.com/inodee/

Education

BS degree Computer Science (2005)	UNIESP	www.uniesp.br	
Post-grad degree Computer Forensics (2010)	MACKENZIE	www.mackenzie.br	

Professional training include: Project Management, Splunk, FireEye, Cisco IronPort, Tanium EDR, CiscoFirepower. Latest ones:
- SANS MGT517: Managing Security Operations: Detection, Response, and Intelligence (Sep/2016, San Diego)
- MS Azure Sentinel & KQL Azure Sentinel Ninja: The complete level 400 (Sep/2020, Microsoft Academy)

Languages

Portuguese (native), English (fluent), Spanish (intermediate), German (basic)

Certifications

CISSP – ISC² Certified Information System Security Professional

SSCP – ISC² Systems Security Certified Practitioner

SANS GIAC **GCIA** Gold – Intrusion Analyst / **Network Forensics**

SANS GIAC **GCIH** – Incident Handler

SANS GIAC **GCFW** – Firewall Analyst

SANS GIAC GSEC – Security Essentials

Splunk Certified Architect v6

AESA – **ArcSight** ESM Security Analyst (former ACSA)

AEA - **ArcSight** ESM Administrator (former ACIA)

Expired certs include: GIAC **GCUX** (Gold), RHCE, LPIC-2, **Cisco** CCNA, SnortCP

Professional Experience

Threat Detection Engineer / Security Use Cases Architect

Feb 2017 - present — **Independent Contractor**

Working as an independent consultant since leaving Splunk to solely focus on security use cases design, build and management. I help organizations establish their threat detection engineering practice based on Big Data. **Data sources:** Active Directory/Eventlogs, Sysmon/EDR, Web Proxy, FW, H/NIDS, Office 365, Applocker, Linux audit, Mac xnumon, Vuln Scanners, Email, AWS Cloudtrail, DNS. **Integrations:** Threat Intel, SOAR, JIRA.

Customers: SWIFT (US), Swisscom, Telefonica (DE), Gassco (Norway) and Splunk partners (MSSPs). Multiple letters of recommendation are available upon request.

Senior Security Consultant/Engineer (EMEA Professional Services – PS)

May 2015 – Jan 2017 — **Splunk Inc.**

Responsible for developing custom, tailored content after threat modeling exercises with Splunk, enabling highly mature SOC/CERT/CSIRT teams leverage Splunk as a detection and hunting platform.

Main accomplishment: consultant of the year (2016) leading the biggest PS contract in EU (Telenor Norway).

Lead Security Engineer – EMEA Security analytics lead (previously Tier-3 SOC Analyst)

Sep 2012 – Apr 2015 — **Verizon**

Member of Verizon Cyber Intelligence Center (VCIC), the group dedicated to develop and deliver innovative Security Solutions to Verizon's customers. Mainly leading RSA and Splunk SIEM projects internally.

Main accomplishments: multiple “Ovation awards” received for driving automation (Unix scripting) and process improvements across Global SOCs; Self-though Splunk developer with dozens of dashboards and metrics reports delivered; SANS/GIAC evangelist, encouraging the team to get trained and certified.

Senior Information Security Consultant

Sep 2011 - Aug 2012 — **Kahuna Network Security Consulting**

Acting as member of ArcSight specialists team focused on SIEM consulting services for large organizations in the Netherlands, including project design, content building and support.

Main accomplishments: primary team member responsible for delivering ING's SOC ESM platform in Central Europe, with focus on content building (reports/dashboards) and on boarding new data feeds. Active brown bag sessions (knowledge transfer) facilitator.

Senior Security Architect

Sep 2010 - Oct 2011 — **Itaú BBA (corporate bank in LA)**

- Budget management, Information Security market research and products evaluation (PoC)
- PoC results comparison, management/board presentations
- Security projects delivery, training and handover

Main accomplishment: Web Security Gateways migration project owner, reporting to CIO. Responsible for market research, PoCs, design and implementation (plus handover) of the whole solution, based Cisco IronPort, integrated with Microsoft Active Directory.

IT Security Engineer

Aug 2007 - Aug 2010 — **Nextel Telecommunications**

- Project leader: SIEM ArcSight, EnCase, IronPort Anti-SPAM, Security Portal
- Risk Analysis for Marketing and Engineering projects
- Hardening / Security baselining for Unix operating systems and Cisco devices
- SecOps and Forensic tools evaluation (ArcSight, EnCase, other)

Main accomplishments: ArcSight project delivery, focused on compliance and auditing. Email relays migration project owner, based on Cisco IronPort technology.

Lead Security Engineer - Security Operations Center (SOC)

Aug 2005 - Jul 2007 — **BM&F BOVESPA (Brazil's Stock Exchange)**

- SOC/CSIRT Technical leader, assisting with SOC Engineers duties
- Incident Response Team support and training
- IDS/IPS tuning, Firewall administration (Cisco PIX and Stonesoft Stonegate)

Main accomplishment: fully integrated case management system development and delivery, based on LAMP stack (PHP and MySQL), with specialized charts and shift handover reports.

Previous roles include: ISP administrator, LAMP (Linux, Apache, MySQL PHP/Perl/Python) web developer.

Most recent and relevant Articles & Publications

Jira workflow for Detection Engineering teams (featured at 2020 SANS Summit and MITRE's ATT&CK 6th Workshop)
How rare is a rare HTTP agent? Context-rich alerts because of math (ML/Clustering based analytics)
Threat detection metrics: exploring the true-positive spectrum
SIEM use cases development workflow – Agile all the things!
DIY: In-house Threat Detection Engineering
Security Analytics: having fun with Splunk and a packet capture file (pcap) – **SANS/GIAC** Accepted Gold paper
Linux Repository: Implementing and Hardening – **SANS GCUX Gold paper**
Security Analytics: How to rank use cases based on the "Quick Wins" approach?
Exploring GCIH Certification – **Hakin9** IT Security Magazine article
Rodando o Snort: Preliminares, **Linux Magazine** (in Portuguese)
SANS Network Forensics Puzzle #2 proud semi-finalist (solution write-up)
Academic papers for Universidade Mackenzie – Computer Forensics post-degree (in Portuguese):
Robustez da Prova Digital – A Importância do Hash no Processo Judicial
Legislação Aplicada à Perícia Forense Computacional

Additional Info

- EU Blue card holder (high-skilled migrant) and permanent resident of Germany (Brazilian Passport)
- Invited Subject Matter Expert (SME) for **(ISC)²** workshops focused on SSCP/CISSP exams questions development, having visited SF, San Diego, Miami, Orlando, Chicago, Phoenix and other cities in US as an invited volunteer.
- Linux/Regex expert and aficionado, leveraging those since mid 1990s when working as a Network/Linux admin.
- Security Conference speaker: CyberUK in Practice – Liverpool, May 2016.
  Talk: "Blame it on you for the false-positives!" (slides)
- Brazilian Percussion and Cavaquinho (Brazilian Ukelele) enthusiast, drummer at http://chocobranco.de