JOSÉ OLYMPIO CASTRO

joseolympio@gmail.com (+55 61-981006438)
www.olysec.com

Interest Areas

CYBER SECURITY SPECIALIST, SOC ANALYST & INFORMATION SECURITY MANAGEMENT

PROFESSIONAL EXPERIENCE

Security Operation Center Analyst
Data Processing Federal Service - SERPRO - 07/2019 to present

- Work with great players in the market such as: Checkpoint, Mcafee, Arcsight, Cisco, InfoArmor, Symantec, Tenable, Microsoft and Red Hat.
- I contribute to build the Security Operation Center -SOC from scratch at SERPRO.
- I perform investigations on SIEM Arcsight, correlating events between security assets.
- Logs analysis for different platforms.
- Collect events of linux system by syslog and Windows by event viewer.
- Ability to monitor security systems and network for threats.
- Threat Hunting Models, MITRE ATT&CK Framework - Cyber Kill Chain, Pentest Kali Linux.
- Troubleshooting and Forensics network with Wireshark.
- Management Vulnerability.
- Investigate security incidents based on good practices NIST, ISO 2700 family.
- Administration, set and management security assets such as: Firewall, IPS, IDS, Anti-malware, SIEM, Threat Intelligence).
- Perform vulnerability analysis with Nessus.

Information Security Manager
Data Processing Federal Service - SERPRO - 04/2011 to 07/2019

- Ability in IT and information security project management.
- Management different security teams.
- Computer Security Incident Response Team -CSIRT consulting project for clients.
- Restructured CSIRT of Serpro.
- Security process mapping by Business Process Model and Notation -BPMN.
- Troubleshooting Incident Handling coordination.
- Elaborated Security Police and Standards for different Security themes.
- Contributed update Information Security Program.
- Alignment of information Security with Business strategic plan.
- Management Risk based on ISO 27005.
- Contributed with update Security Police based on General Data Protection Regulation -GDPR.
- Realized GAP analysis based on ISO 27001 standard to measure the maturity level.
- Mapping Information Security Governance process based on ISO 27014.
- The project manager from Open Source Malware Analysis Lab Project (https://www.cert.br/forum2018/agenda/).

Security Analyst
Data Processing Federal Service - SERPRO - 2009 to 2011

- Perform, management and implementation firewall checkpoint, IPS Intrushield Mcafee, Filter Ironport, vulnerability assessment Nessus.
- Support for different assets such as: routers, switches. Linux Servers, Windows Servers.
- Internal IT Audit based on ISO STANDARD 27001 / 27002.
- Security tests for Web Application and Network by Kali Linux.

Support Analyst
Weavers Networking Consulting - 2006 to 2008

- Development Microsoft network projects.
- Development Linux system / network projects.
- Automation in Linux system administration with Shellscript.
- Implementation different linux services such as iptables Firewall, proxy Squid, mta Sendmail, file shared samba, NTOP, VPN site to site and client to site, IDS snort , High availability RAID.
- Management Microsoft networks, implementation, and maintenance.
- Support Linux, Apache, Mysql, Php -LAMP.
- Support for routers and Switches LAN and WAN environment.

SUMMARY OF QUALIFICATIONS

http://www.linkedin.com/pub/a/a5/689

http://lattes.cnpq.br/5784509255653059

EDUCATION

Bachelor's Degree - Computer Science **– Centro Metodista Bennett - 2005**

MBA - Information Security Management **– Universidade Federal do Rio de Janeiro -2009**

Specialization's Degree (Lato-Sensu) - Forensics Computer **– Instituto de Pós-graduação - 2018**

Specialization's Degree (Lato-Sensu) - Cybersecurity and Ethical Hacker **- UNICIV - 2020**

LANGUAGES

Portuguese - Native speaker**.**
Brasas course – Proficiency English Certificate. Exchange in Canada - Toronto - ILAC -2014
Spanish - Intermediate.

CERTIFICATIONS

C-CISO - Certified Chief Information Security Officer – EC-Council
CISM - Certified Information Security Manager – ISACA
CCSA – Certified Checkpoint Security Administration - Checkpoint
CBCP - Certified Business Continuity Professional - DRI
COBIT 5 Foundation - ISACA
Auditor Lider - SGSI 27001 IRCA **-**BSI
MCSE+Security, MCSA+Security, MCDST, MCP- Microsoft
RHCSA – Red hat / **LPIC-1** Linux Professional Institute
Certified Computer Security Incident Handler - Carnegie Mellon University by CERT BR.
Certified Managing Computer Security Incident Response Team - Carnegie Mellon University

GENERAL SKILLS

- Leadership, proactive and good sense to integrate teams.
- Using budget resources designed to maximize return on investment-ROI.
- Ability to deal with complex environments and under pressure.
- Identifies opportunities to improve security controls for remediating or mitigating risks and assessing the residual risk.
- Complice with the best practices in IT and Information Security.
- I Keep constantly updated with regard to new technologies and trends.
- I like to share my experience and knowledge with my workmates and learn with them too.
- Ability to quicky adapt to the work environment.
- High time management and problem-solving abilities. Excellent communication and interpersonal skills.