**pedro casablanca**

8579 NW 23rd Manor N., Coral Springs, FL 33065

cell 561.460.5041 • pcasablanca\_cybershield@outlook.com

**InfoSec-Sys admin**

Insightful, results-driven InfoSec professional with notable success administrating a broad range of corporate IT-Security initiatives while participating in planning, analyzing, and implementing solutions in support of business objectives. Excel at providing comprehensive secure network design, systems analysis, and full lifecycle ‘Risk/Vulnerability/Threat project management.

|  |  |
| --- | --- |
| Technical Proficiencies |  |

|  |  |
| --- | --- |
| Platforms: | Windows 7/8/8.1/10, Windows Server 03/08/12 R2, UNIX (Solaris, HP-UX), Linux (Red Hat, Ubuntu), Mac OS, Android, iOS. |
| Programs: | PowerShell, Avaya IC, Citrix Xen, VMware, PRTG, Lync/Sametime, IS-CIA Authenticator, Sophos, Cisco Anyconnect, RSA Tokens, VMware, LogMeIn. |
| Database: | MySQL, BMC, Salesforce, NICE Audit, Oracle-IAM, Ecomm, AD/LDAP. |
| Security Tools: | McAfee, Symantec: DLP/MsgLab/SEP, Splunk, PaloAlto/SonicWALL, Nmap, Cisco FireSight, ForeScout, Tripwire/RSA: Security Analytics, Archer & Ecat-Forensic. Snort, Burp, Encase Ent, Nessus, Wireshark, Oracle IAM, Magnet, Kali-Linux, Acunetix, Rapid7, PhishMe. |

|  |  |
| --- | --- |
| Professional Experience |  |

**Sabadell Bank**, Miami Lakes, FL 9/2016 – Present

**Cyber Security Analyst**

Handle day-to-day tasks involving SOC next-gen monitoring, end-point protection, incident analysis, forensic investigation, and remediation for native, cloud & financial Ecommerce data.

**Key Contributions:**

* Employing LEM & NAC to safeguard the integrity and privacy of our information .
* Administration of user RSA accounts, data feeds, workflow, and report access.
* Perform RSA/SourceFire threat-hunting to identify patterns of misuse & abnormal behavior.
* Monitor on-going real-time review of events and incidents via SIEM RSA & ForeScout.
* Deploy PhishMe campaign to educate and improve security awareness & to ensure corporate compliance. This includes; brochures and mandatory online training.
* Managed the account verification process; including authorization & authentication.
* Validate integrity of systems and devices to prevent unauthorized access and minimize risk of compromise via RSA policies and rules. Firewall group policy & governance.
* Collaborate with all other IT functions to resolve security threats and correct deficiencies.
* Perform root cause analysis on security incidents PaloAlto, Cisco IDS/IPS and RSA.
* Monitor and analyze alerts received in SEP, NetWitness, FireSight, PhishLab & ForeScout.
* Use PaloAlto & Cisco IDS to generate reports and analysis to specific threats.
* Investigate and classify the alerts critical via RSA Archer & SecOps systems.
* Conducting analysis, Nessus vulnerability scanning and stop-gap assessments.
* Work with InfoSec vendors to perform pen-test simulations to evaluate any possible gap.
* On-going Symantec DLP administration; policies, analyze data-leak incident queue to determine if bank policies and procedures have been compromise.

**Verizon/terremark**, Miami, FL 9/2015 – 9/2016

**InfoSec Analyst/System Admin –** *Contractor/Project completed*

Recruited to establish enterprise-wide InfoSec program; oversee companywide efforts to identify and evaluate all critical systems. Define, deploy & monitor government compliance & correlate any (Advance Persistent Threat).

**Key Contributions:**

* Being part of five new IS-departments: Risk Assessment, Vulnerability, Penetration-Testing, SOC/Cloud Security Alliance and Security Engineering services.
* Incident handling procedures to detect, isolate and investigate potential information system (IOC) Indicator of Compromise using Snort and Tripwire SIEM. Maintain Cyber Assurance, Federal Compliance & data Governance. Symantec DLP administration.
* Running IDS analysis for medium & high sensor alerts using behavior & signature rules.
* Classified intrusion events, footprint all source/destination IPs, and validate the suspicious activities. Analyze web-app exploits & payload using Burp conversion tool.
* Evaluate vulnerability scans utilizing network scanning tools and software to notify system administrators of applicable Information Assurance Vulnerability Alerts.
* Track stats via Splunk to identify trends & mitigate spam & phishing attacks.
* Use forensic tool ‘RSA NetWitness’ to validate target response before and after exploit.
* Analyze alerts payload, IP Header and decode data to corroborate malicious content.
* Implement correlation rules & alarms to improve threat detection & incident response.
* Conducted dynamic analysis by collecting and analyzing threat intelligence: Recon, web-application, policy-violations, attempted-admin, Shellcode, etc…
* Monitoring network traffic, analyzing bandwidth requirements & provide Internet usage for forensic acquisitions for investigation as requested by (CERT, COOP and DR unit).

**walgreens co**, Miami Lakes, FL 11/2012 – 9/2015

**IAM Security Analyst/ DevOps**

Malware analysis/correlation, creation/escalation in Remedy, cloud mitigation to correlate Oracle IAM alerts and Salesforce audits. Central knowledge of IS end-point protection & compliance: PCI-DSS & HIPAA.

**Key Contributions:**

* Manage Vormetric SIEM encryption, AD policies & Group Policy Management.
* Track & monitor all network resources, cardholder data, & restrict physical access.
* Monitor and secure multiple (HBSS) environments via McAfee.
* Generate McAfee (ePO) queries and reports to collect various deployment statistics.
* Administer web-access management WAM privileges via Cloud Access Manager.
* Manage CheckPoint UTM administration, services, deployment, VPN & user creation.
* Implement McAfee DLP policies to detect & prevent unauthorized access.
* Deploy McAfee Agent, virus scan for Linux, Windows HIPS and Policy Auditor.
* Provides role mining, compliance attestation and recertification.
* Correlate any McAfee ‘HIPPA and PCI’ DLP & device control module alerts.
* Implement Privilege ACLs & RBAC for pharmacist & managers to manage Distro-lists.
* Govern access administration: (Provisioning, de-provisioning), access enforcements (authentication protocols, certification & logging monitoring etc.)
* Vulnerability & Pen-test execution; via Burp Suite and Rapid7.
* Providing desktop-based single sign-on (SSO), including support for single sign-on into legacy client applications via automated login form fill-in for work-home users.
* Evaluate Oracle Identity Federation: identity request/provider, Oracle SAML by supporting the Authentication, Attribute & Authorization assertions.

**Worldwide ticketcraft**, Boynton Beach, FL 9/2011 – 11/2012

**IT Network Security Admin**

Serve as a PEP policy enforcement point to handle user policy & rule requests. Use MySQL Query to manage client’s active directory. Manage correlation rules via IBM Tivoli (IAM) & Sentinel. Provide support for AD revocation list, (CA) & RSA tokens.

**Key Contributions:**

* Manage web-access privileges via Cloud Access Manager to enhance security.
* Monitor, maintain, and secure McAfee ePO host–based security system environments.
* Administer SonicWALL firewall: services, security trends, web-filtering, VPN & users.
* Implement XACML using set templates via company’s native SaaS LDAP App-launcher.
* Maintain encryption policies, Cisco VPN and Thin-Clients with Two-factor Auth.
* Mitigate SecOps & DevOps functionalities by monitoring McAfee: HIPS, PA, ACCM, RSD, DLP, VSE & Asset Baseline.
* Establish ethical vulnerability/pen-test using Kali-Linux & malware analysis.
* Enforce Data Governance module for both MySQL and Oracle distribution lists database.
* Capturing Internet navigation via Magnet Forensic Acquisition for ACL-assessments.
* Use Imperva SecureSphere to mitigate database vulnerability assessments in MySQL & Apache web service on RedHat Linux via Putty session.

**Tiger direct/CompUSA**, (Palm Beach/Deerfield Beach, FL) 10/2009 – 9/2011

**Security Admin Specialist**

Promoted to Sec-Admin after demonstrating my IT Tech Support skills. Installing, maintaining and upgrading PC/Server hardware, software, LAN/WAN & email systems. Implement CIRT/DevOps; QA, CRL encryption, AAA security, NERC CIP, & cloud encryption via Fortinet.

**Key Achievements:**

* Create and modify Kaspersky endpoint configuration & Rapid7-Nexpose assessments.
* Troubleshoots via Linux CentOS/Ubuntu; QuickBooks, MySQL, FTP Server & Apache.
* Install and instruct home-users on Checkpoint VPN secure client & RSA tokens.
* Promote and install Checkpoint host firewall on all our customers as required by B2B policies. Use Imperva Skyfence for cloud security and infrastructure correlation.

|  |  |
| --- | --- |
| Accomplishments/CyberInsight |  |

* Detected & contributed (ATD) mitigation data for 25-30 U.S. Government agencies.
* NOC & SOC team to monitor/administer IAM hardware & software.
* Part of the U.S. Department of Veteran Affairs SOC team, supporting Next-Gen centers.
* Administer; inventory, Lawson acquisition, Policy enforcer, budgeting, vendor mgmt.

|  |  |
| --- | --- |
| Hands-on Appliance |  |

|  |  |  |
| --- | --- | --- |
| * Avaya PBX | * Dell Wyse DVI | * Avaya/Cisco IP Phones |
| * Cisco Catalyst SIP | * Apple IMac | * HP ProLiant |
| * AT&T/Sprint Fiber Panel * Toshiba UPS Server | * Cisco Routers/Switches * TeleComm AC Unit | * HP Thin-Clients * UTM Security Appliance |

|  |  |
| --- | --- |
| Education & Credentials |  |

**Master of Science in Cyber Security & Assurance - *Pursuing***

Keiser University, Pembroke Pines, FL

**Bachelor of Science in Information Technology Management - *Graduated***

Keiser University, West Palm Beach, FL

**Security Clearance:** Active

**Compliance:** ISO 27001, NIST, PHI, HIPPA, GLBA, PCI & Government Security Assurance.

**Professional/Gov. Certification**

* + CompTIA – Computing Technology Industry Association
    - Security+ / Network+ / A+ - **IAM/IAT Level II *Certified***
    - U.S. Government Contractor: Awareness and Rules of Behavior - ***Certified***
  + CISSP – Certified Information Systems Security Professional **– IAM/IAT Level III *Pursuing***

**Professional Training/Courses**

* + ECSA – EC-Council Certified Security Analyst
  + CISSP – Certified Information Systems Security Professional
  + GIAC - Global Information Assurance Certification

**Professional InfoSec Community & Webinars**

NIST | ASIIS | NCJRS | CCIPS | ISSA | InfoSysSec | ISACA | FS-ISAC | OWASP | SANS DFIR