Raúl E. Millán V.

+507 66701221
rmillan@outlook.com
https://www.linkedin.com/in/raulmillan/

Cybersecurity professional with experience in both tactical and strategic roles. I've worked on projects small and big with Internet Service Providers (ISP), Government organizations, and large customers in the private sector, with special emphasis on Cloud Security Architecture and operations.

Experience

2021 – 2022

Millicom-TIGO / IT Security Solutions Architect

PANAMA, PANAMA

Plan, organize, and manage third parties, to ensure the stable and secure operation of the organization's IT Security solutions at the regional level. Identify, select, design, implement, and document IT Security solutions and platforms to be adopted by all Millicom operations across 9 different countries where it operates. Work with key stakeholders within information technology and information security to identify risks and recommend control implementations.

Highlights:

Activities that involve all operations (9 countries)

- IT Security roadmap development and documentation
- Microsoft Purview Information Protection deployment
- Microsoft Endpoint Management (Intune) implementation in 3 countries
- Azure AD Conditional Access (MFA) documentation and adoption
- AzureAD/QRadar integration to include login and risk events
- AzureAD Event Hub and Log Analytics implementation
- AzureAD Workbooks implementation
- Office 365 tenant migration coordination and support (Guatemala)
- Trend Micro solutions suite (workstations, servers and cloud) deployment and adoption
- Email Security ecosystem (Office 365 + Greathorn) KPI development, solution documentation, configuration clean up and filter hardening.
- SPF, DMARC, and DKIM standardized implementation.
- Privileged Access Management (PAM) documentation and standardization
- NIST data privacy documentation (encryption)

Activities that apply only to headquarters offices (Miami)

- Active Directory architecture security assessment (AD RAP), findings and remediation
- Microsoft Defender for Identity proof of concept (UEBA)
- Internet browser standardization and documentation (retirement IE11 and Firefox)
- Oracle EBS SSO solution selection and documentation

- NIST Cybersecurity Framework implementation (CSF)

2018 – 2021

Cloud Security Architect / Consultant

PANAMA, PANAMA

Helping customers with the adoption, design onboarding, and securing cloud services (IaaS, PaaS, SaaS). Microsoft infrastructure security (on-prem and cloud) using the existing security ecosystem available on Azure. Design and implementation of ISMS programs based on standards such as ISO 27001/2. Internal and external penetration testing.

Microsoft infrastructure security (on-prem and cloud) using the existing security ecosystem available on Azure using available solutions within the Microsoft security ecosystem, like Security Center, Sentinel, Azure Monitor and Alerts, Azure Backup and Azure ATP (now Microsoft Defender).

Securing Microsoft 365 services by adoption of zero trust initiatives using tools like Azure AD, Microsoft Defender, M365 Secure Score, Microsoft Information Protection, Microsoft Cloud App Security, Microsoft Intune (Endpoint Manager), and Microsoft Insider Risk Management.

Cloud security assessment (Microsoft Azure, Amazon Web Services, Office 365).

Design and implementation of ISMS programs based on standards such as ISO 27001/2. Internal and external penetration testing, web application testing (OWASP) and vulnerability assessment.

Recent projects:

- Microsoft Information Protection implementation for a regional financial institution
- Azure infrastructure management for an IoT customer
- Office 365 migration of more that 250 mailboxes
- Microsoft Cloud App Security implementation with DLP rules
- Microsoft Enterprise Mobility + Security E5 implementation
- Microsoft Advanced Threat Protection implementation
- Microsoft Endpoint Manager PoC
- Checkpoint Cloudguard for Azure gateway deployment (formerly Checkpoint IaaS)
- Microsoft 365 Security assessment
- Azure SQL Database deployment and monitoring with transparent data encryption

2014 - 2018

Chief Security Officer / Panama Canal Authority

PANAMA, PANAMA

Supervision role (team lead) in charge of the Systems Security Unit, responsible for the development of the Cybersecurity program for a 10K employee organization, adoption of a threat modeling framework, selection, implementation, and operation of information security controls in general (firewall management, IPS, vulnerability assessment, endpoint security), VPN, indirect report to Risk Management & internal audit & compliance, business continuity plan maintenance and test, and cybersecurity awareness campaign management.

Implementation of SWIFT's Customer Security Program (CSP).

Responsible for Microsoft Azure and Office 365 operations and security; cloud adoption program (cloud committee formation), Modern Service Management Strategy & Roadmap for Microsoft Cloud Services.

Projects:

- Microsoft Local Administrator Password Solution (LAPS) PoC implementation
- Active Directory security program controls and improvement implementation (ADRAP)
- Azure Information Protection implementation for Office 365 users (4,000 mailboxes)
- Azure Key Vault (BYOK) implementation (for use of AIP)
- Cloud security standards development (administrative roles definition, resource and tag naming, reporting, performance metrics)
- Cloud resource consolidation (lift and shift, subscription consolidation, resource group design and management)
- VM deployment and management (both Windows and Linux)
- Azure Security Center implementation
- Cloud Identity management (automation accounts, develop administrative roles, design, and implement risk-based access policies)
- Deployment of Azure App Services for development and UAT, including Azure Database for MySQL
- Storage account for database and file storage (Azure Files)

2011 - 2014

Program Manager / National Authority for Government Innovation

PANAMA, PANAMA
Manager of the National Computer Security Incident Response Team (CSIRT), the National Computer Incident Response Team, helps government organizations with the coordination of the response of security incidents. The CSIRT is also responsible for the development of policies, guidelines and standards.

Co-authored the National Cybersecurity Strategy, coordination and development of the Cybercrime draft law, and acted as liaison with Council of Europe and the Organization of American States (OAS) for the accession of Panama to the Budapest Convention on Cybercrime

Support and coordination for the National Government Multiservice Network, NOC/SOC (Network Operation Center) and securing the AIG's internal IT infrastructure.

2009 - 2011

General Manager / Consultores de Seguridad Informática

PANAMA, PANAMA
Sales, presales, and security services consulting. Penetration testing, vulnerability analysis, and risk management services, vulnerability assessment. Development of business continuity and disaster recovery plans, development of information security plans, and network security architecture analysis and integration.

2007 - 2009

Managed Security Services Manager / Ximark Technologies

PANAMA, PANAMA
Penetration testing, risk analysis, development of business continuity programs for customers. Implementing Fortinet security solutions.

2001 - 2007

Managed Security Services Manager / Cable & Wireless

PANAMA, PANAMA

Information security incident response management and monitoring for customers. Development and implementation of standard operating procedures (SOP) and service level agreements (SLA) with both, internal and external customers.

Oversee the operation of the MSS Center, fully staffed with 10 people, while keeping the internal IT Security operations running.

Direct responsible for the development and delivery of the Managed Security Services products offered by Cable & Wireless Panama. Technical design and financial definition of the following services:

- Freedom Internet Security SOHO (Managed Firewall)
- Freedom Internet Security Residential (Bundled Antivirus for residential customers)
- Managed Enterprise Firewall / UTM (Web Filter, Antivirus, IPS, and VPN)
- Managed IPS (Intrusion Prevention Systems)
- Managed Antivirus
- Managed E-mail security (Antivirus and Antispam)
- Penetration Testing Services
- Vulnerability Assessment

Information Security Manager / Cable & Wireless

PANAMA, PANAMA

The IT Security team is responsible for implementing the security lifecycle model (Policies design, procedures, metrics, assessment, selection & implementation, training, monitoring and incident response) for Cable & Wireless Panama (part of Cable & Wireless PLC – www.cw.com).

Other tasks include:

- Recurrent digital assets risk assessment (penetration testing) and inventory (vulnerability scanning)
- User management (Access Control) for all business-critical applications
- VPN (point-to-pint and client-based) remote access management
- PGP Based e-mail encryption for sensitive data exchange between partners and other business units
- Datacenter environmental monitoring (temperature and humidity)
- Information Security Architect, high availability design of all network related components for corporate network and Internet Datacenter
- Security awareness program development
- Standards compliance (procedures and policy development)
- Network security, IPS and firewall administration
- Forensics
- Application security review before rollout to production
- Incident response
- Research & development
- Compliance with all local legal requirements regarding record keeping (e-mails) and investigation related data (phone fraud detection and Call Data Record)

Systems and Services Manager / Cable & Wireless

PANAMA, PANAMA
The System and Services Administration unit has the responsibility of providing technical support and development of new IT infrastructure for the Network Operation Center (NOC) and Service Operation Center (SOC) of Cable & Wireless Panama.

Some of the tasks performed while on the post:

- Design, installation, maintenance and support of the IT infrastructure
- Tech support for 40 users of multiple applications
- Generation of periodic reports and statistics which measure the company's KPIs
- Support and implementation of the following IT platforms:
  - XMATE
  - TeMIP (http://www.emea.compaq.com/temip/)
  - Nortel OTM (Optivity Telephony Manager) and BCM (Business Communications Manager)
  - Avaya Visibility™ Management Suite (http://www.avaya.com)
  - Infovista Performance Management (http://www.infovista.com/)
  - Clarify CRM (http://www.amdocs.com/)
  - What's Up Gold

IT Infrastructure and Security Manager / Cable & Wireless

PANAMA, PANAMA
Datacenter administration, network management, project management, the establishment of SLAs between the IT and the business units, protection of email system, PKI, and vulnerability scanning.

Responsible for three (3) Datacenters, with more than 100 servers (UNIX/WINDOWS/LINUX). Project management for the implementation of multiple IT solutions, for a population of over 1800 users

Design, implementation and operation of the following IT solutions:

- Corporate IDS systems
- Multiple Checkpoint FW-1/VPN-1 NG gateways clusters
- Windows 2000 Active Directory Migration
- Antispam solution
- Critical platform monitoring
- Vulnerability assessment
- PGP encrypted mail and digital signature system
- LAN, MAN, and WAN network administration (CAMPUS)
- Checklist and standard operation procedure (SOP) implementation

2001

Systems Administrator / Morgan & Morgan

PANAMA, PANAMA
Sun Solaris systems administration, email solution administration, UNIX systems documentation, design and maintenance of group website, design and execution of monitoring scripts, detection and mitigation of cyber-attacks.

1999-2000

Developer / Grupo Informatica

PANAMA, PANAMA

Development and support of systems in Natural programming language (Software AG), integration with ADABAS database (Software AG), source code audit in preparation for the date change in the year 2000 (Y2K Taskforce)

1998

Technical Support Manager / Textiles Rio Lindo

TEGUCIGALPA, HONDURAS

Enterprise Resources Planning (ERP) modernization project evaluation, technical support of Windows users in a mainframe environment, network support

1997-1998

Technical Support / The Netsys Co.

TEGUCIGALPA, HONDURAS

Telephone and face-to-face technical support for Internet clients, installation and configuration of software for Internet connection, responsible for more than 500 clients in the Tegucigalpa area.

1995-1997

Developer / Interamerican Center for Tax Administrators

TEGUCIGALPA, HONDURAS

Analysis and development in Natural / ADABAS (Software AG) for OS/2 and UNIX, training on HP-UX and OS/2 operating systems.

Education

Bs in Computer Science / Universidad Tecnológica Centro Americana

http://www.unitec.edu

"FUNDAMENTALS OF INCIDENT HANDLING".

CARNEGIE MELLON SOFTWARE ENGINEERING INSTITUTE – WASHINGTON, USA.

"ADVANCED INCIDENT HANDLING".

CARNEGIE MELLON SOFTWARE ENGINEERING INSTITUTE – PANAMÁ, PANAMÁ.

"2014 INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY (301) TRAINING".

US DEPT. OF HOMELAND SECURITY – NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER – ICS CERT – IDAHO, USA. HTTPS://WWW.US-CERT.GOV/ICS/TRAINING-AVAILABLE-THROUGH-ICS-CERT#WORKSHOP

Certifications

AZ-900: AZURE FUNDAMENTALS

HTTPS://DOCS.MICROSOFT.COM/EN-US/LEARN/CERTIFICATIONS/EXAMS/AZ-900

F5 CERTIFIED PRODUCT CONSULTANT

HTTP://WWW.F5.COM/SERVICES/CERTIFICATION/PROGRAMS/REQUIREMENTS.HTML

CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) / ISACA

HTTP://WWW.ISACA.ORG/TEMPLATE.CFM?SECTION=CISA_CERTIFICATION

CERTIFIED INFORMATION SECURITY MANAGER (CISM) / ISACA

HTTP://WWW.ISACA.ORG/TEMPLATE.CFM?SECTION=CISM_CERTIFICATION

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP) / ISC2

HTTPS://WWW.ISC2.ORG/CGI-BIN/CONTENT.CGI?PAGE=818

CERTIFIED ETHICAL HACKER (CEH) / INTERNATIONAL COUNCIL OF E-COMMERCE CONSULTANTS

HTTP://WWW.ECCOUNCIL.ORG/CEH.HTM

Conferences (speaker)

- IEEE-COMSOC - Security as a Service – Panamá – July 2008.
- Workshop on prevention and investigation of cybersecurity incidents – current state of security in Panamá. November 2011
- Regional workshop on Cybersecurity. Montevideo, Uruguay. November 2013
- Cyber capacity building as a development issue: What role for regional organizations? Paris, France. March 2014.
- Cybersecurity Security Capacity Building – National Cybersecurity Technical Assistance Mission – Organization of American States – St. Kitts and Neves. September 2014.
- Cyber NEEDS and development: identifying the needs of Networks Enhancing the Economy, Development and Security (NEEDS) – European Union Institute for Security Studies – Brussels, Belgium – February 2015.
- Cybercrime, cryptocurrency and its real-world effects – 19th ANNUAL IBA TRANSNATIONAL CONFERENCE – Panamá – May 2016.
- Panelist Cybersecurity for Critical Infrastructure – Cybertech Panama – March 2017
- Critical infrastructure protection - Checkpoint Experience 2017 – Checkpoint Software Technologies – Las Vegas, Nevada – EEUU. – April 2017
- Panelist – Fortinet Cybersecurity Summit – Panama – July 2017
- Panelist – Internet Governance and IoT – Internet Society Panama Chapter – August 2017
- Sub-regional Workshop on Protection of Critical Infrastructure: Cybersecurity and Border Protection – Organization of American States – September 2017
- Panelist – First Internet Governance Forum (IGF) – Panama – October 2017
- Panelist – Second Internet Governance Forum (IGF) – Panama – July 2019
- Presenter – 4th Information Security and Fraud Prevention Forum – Zero Trust - National Banking Association – Panama – November 2019
- Presenter – 4th Cyber Security Forum – National Innovation Authority – Panama -October 2020

Affiliations

INTERNET SOCIETY (ISOC) – CAPITULO DE PANAMÁ

HTTPS://WWW.ISOC.ORG.PA/

ANTI-PHISHING WORKING GROUP (APWG)

HTTPS://WWW.ANTIPHISHING.ORG/

CLOUD SECURITY ALLIANCE

HTTPS://CLOUDSECURITYALLIANCE.ORG

Skills

- **Identity Management:** Active Directory and Azure AD
- **Cloud Computing:** Microsoft Azure Security Center, Azure Portal, Azure CLI, Azure Powershell,
- **Firewalls:** large scale implementations of CheckPoint FW-1/UTM-1 and Fortigate solutions.
- **Remote Access:** CheckPoint VPN-1/FW-1 SecureClient/SecureRemote, Fortigate, RAS, SSL VPNs, Microsoft Virtual Network Gateway, Microsoft Direct Access.
- **Web Application Firewalls:** Barracuda, Azure Web Application Firewall (WAF) on Azure Application Gateway
- **High Availability:** Azure load balancer, F5 LTM, Barracuda Load balancer, and plain old DNS 'round robin'.
- **E-Mail Security:** Barracuda Spam Firewalls, Greath Horn, Microsoft Defender for Office 365 (saft attachments, safe links, advanced anti-phishing, anti-spam, antimalware)
- **Desktop Security:** McAfee Enterprise, Trend Micro, Barracuda Webfilter, Microsoft Endpoint Manager (Endpoint Security)
- **Vulnerability Scanning and penetration testing:** Tennable (Nessus), Qualys (WAS), Rapid7 (Nexpose), Burpsuite, OWASP Zap, Bettercap (Wireless penetration testing), Metasploit, Cain & Abel, Kali Linux & related tools, King Phisher (Phishing Campaign Toolkit).
- **IDS/IPS:** TippingPoint, Snort, McAfee Intrushield IPS (large scale implementations), Fortigate (Internal network segmentation)
- **Operating Systems:** 20+ years of experience with Microsoft and Linux / UNIX operating systems
- **Networking:** Cisco, HP, Foundry switching and routing, Sniffer Technologies.

About Me

The promotion of good practices and formal technology processes allows organizations to adopt the necessary cybersecurity practices to ensure their operational continuity. Trying to send this message has become something personal, I have been able to see, firsthand, how organizations (and therefore people) suffer unnecessarily, for not knowing how to recognize this reality. Therefore, I do not waste every opportunity that is offered to me, to speak in public about the issues in and around cybersecurity.

Among the activities, I enjoy most are Crossfit, running, and hiking; I believe that physical activity helps to deal with problems that may arise, whether personal or professional.

You can find more information about me at https://the.raulmillan.com