DANIEL IVÁN BENAVIDES HENRRIQUEZ

CYBERSECURITY CONSULTANT

OBJECTIVE

Contribute to the growth and assurance of any business by applying my knowledge and expertise in Cybersecurity.

CAPABILITIES

- Basic Forensics knowledge
- Experience in Incident Response engagements
- Experience with multiple SIEM technologies for log correlation
- Experience with multiple XDR, EDR and SOAR technologies (analysis and implementation)
- Experience in designing advanced security policies based on threat intelligence reports
- Experience in designing playbooks for automation purposes
- Dominance of multiple Operating Systems
- English Level: Advanced (C1)
- Experience in Implementation of security policies based on ISO/IEC 27001:2013
- Network Security: Firewalls
- Scripting with Bash and Powershell
- Threat Hunting/Threat Exposure Checks
- Vulnerability Management
- Knowledge about Virtualization: VirtualBox, VMWare, Hyper-V, and AHV.
- Knowledge about Cloud Technologies: Azure and AWS.
- Public Speaker for important Cybersecurity communities such as Ekoparty

JOB SUMMARY

Senior Cybersecurity Consultant (Cortex XDR)

Palo Alto Networks (Remote) | July 2024 - Present

- Lead Endpoint protection deployment, operationalization, troubleshooting, training and Security Policy Tuning:

- *Analyze customer requirements, provide guidance & assistance throughout the customer life cycle to ensure a quick and successful product deployment.*
- *Design and implement advanced security policies based on machine learning, behavioral analytics, and threat intelligence to proactively detect and respond to emerging threats.*
- *Act as the product SME, working together with product and engineering teams ensuring our customers and partners get the most out of the products.*
- *Independently investigate and respond to complex security incidents, leveraging XDR and deep understanding of incident response methodologies.*

SOC Supervisor (Cybersecurity Engineer)

RSM US LLP (El Salvador) | December 2021 - June 2024

- Rank: L3 / Shift Lead / Threat Hunter / Incident Responder
- Main goal: monitor the infrastructure of almost 400 U.S clients (exclusively) in the Security Operations Center of RSM Defense (Unit26) against potential cyber threats and recommend them response actions in order to protect or mitigate confirmed security incidents
- SIEM management: ELK, Wazuh, Stellar Cyber
- EDR: Crowdstrike, SentinelOne, Carbon Black, MS Defender
- Malware Analysis
- Phishing Analysis
- Threat Hunting
- Threat Intelligence (OSINT)
- Alerts Triage: Critical, High and Medium alerts
- Tickets escalations to clients
- Provide assistance to Junior Analysts
- Cybersecurity Internship Program Lead

Sysadmin

Centro Nacional de Registros | September 2017 - November 2021

- Nutanix hyperconverged platform management.
- Service administration of: Active Directory, Apache, DNS, FTP, RDS, SMB, SMTP, SYSLOG.
- Server administration for teleworking.
- Digital certificate issuing server administration.
- Attention to incidents and requirements (tickets).
- Open Source tools configuration.
- Backup configuration and scheduling.
- Linux Server hardening (CIS Benchmark - Centos7, RH7)
- Windows Server hardening (CIS Benchmark - WS19)
- Implementation of ISO/IEC 27001:2013 security policies on servers.
- Installation of security updates on linux and windows servers.
- AV deployment on linux and windows servers
- Vulnerability assessment, exploitation and mitigation in windows and linux servers (Nessus/Tenable)
- Performance monitoring and traceability of servers.
- Problem solving tasks at a logical and physical level.

PERSONAL INFORMATION

- Nationality: Salvadorean (El Salvador)
- E-mail: tec.danielbenavides@hotmail.com
- Phone Number: +503 7235-5175
- ID: 05562883-7
- Address: Los Planes de Renderos, Panchimalco, San Salvador.
- LinkedIn: **https://www.linkedin.com/in/daniel-benavides-ba3659130/**

HOBBIES

- TryHackMe (Rank: Guru) **https://bit.ly/3xX9zHw**
- Blue Team Labs Online (Jr. Defender) **https://bit.ly/3KkhuRP**
- CTF Player
- Brazilian Jiu Jitsu Blue Belt
- Proves of concept about the new threats that are emerging in cybersecurity (OSINT + My own virtual lab)
- Attend to international cybersecurity conferences such as Ekoparty (Buenos Aires, Argentina)

ARTICLES

- How do I know if my page is vulnerable to SQL Injection?: http://www.noise-sv.com/como-saber-si-mi-pagina-es-vulnerable-a-sql-injection/
- Attacking outside the LAN: http://www.noise-sv.com/atacando-fuera-de-la-lan/
- Your trace on Twitter: http://www.noise-sv.com/tutorial-de-tinfoleak/

ACADEMIC RECORD

LISA Institute (Spain)

Cyberintelligence Expert

- Cyber Warfare
- Cyber Operations
- Cyber Threat Intelligence
- Cybercrime Investigation through OSINT
- Average Grade: 92.83%

Escuela Europea de Excelencia (Spain)

Information Security - ISO/IEC 27001:2013| June 2021 - November 2021

- Specialization field: Implementer and Intern Auditor
- Average Grade as Implementer: 9.25/100
- Average Grade as Intern Auditor: 90.02/100

Universidad Don Bosco

Bachelor of Computer Science Engineering | 2017-2021

- Average Grade: 8.5 (CUM LAUDE)
- Specialization field: information security and business intelligence.

Universidad Don Bosco

Computer Engineering Technician | 2016-2017

- Average Grade: 8.4
- Specialization field: servers and network management

CERTIFICATIONS AND COURSES

- Blue Team Level 1 (BTL1) by Security Blue Team
- Security Analyst Level 1 (SAL1) by TryHackMe
- Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA)
- AWS Certified Cloud Practitioner CLF-C02
- CompTIA Cybersecurity Analyst CySA+
- CompTIA Security+
- Certified in Cybersecurity (ISC)2
- Certified on Stellar Cyber for SOC Analysts
- Junior Penetration Tester Learning Path at Try Hack Me
- Cyber Threat Hunter Level 1 at Active Countermeasures
- OSINT Lab Foundations at Trace Labs
- Stellar Cyber Certified Associate at Stellar Cyber Online (Open-XDR solution for SOC analysts)
- Certified Network Security Specialist at the International Cybersecurity Institute. Certification ID: 20492821
- Scrum Foundation Certificate (SFC) at CertiProf. Certification ID: 43263946
- NSE1 Fortigate at Fortinet Security Training Center Online. Certification ID: zC7xcXg4cZ
- Executive Vulnerability Management at Cybrary.
- Introduction to Cybersecurity at GBM.
- NSE 4 Fortigate at Fortinet Security Training Center Online.
- Online network and data communication engineering course at Global Education Academy.
- Online Digital Signature course at Global Education Academy.
- NDG Linux Essentials at netacademy (Cisco).
- Nutanix Enterprise Cloud Platform Administration 5.1 course at GBM.
- Hyperconvergence with Nutanix: installation and configuration at Udemy.