Bassem Hemida | Cybersecurity Senior Manager | Subject Matter Expert

Summary

A cybersecurity senior manager with over a decade of technical professional services experience working with corporates and multinational organizations throughout Europe and Middle East in the financial, public and energy sectors.

- Successfully planning, supervising, and managing multifaceted cybersecurity roadmap projects with multiple deliverables, complex dependencies and multi-million dollar budgets.
- Ability to leverage an in-depth understanding of the strategy to plan, establish, and operate impactful and sustainable proactive and efficient detective, preventive, and predictive programs.
- Lead for Incident Response Retainer for multiple clients in energy sector; this includes onsite and offsite incident response activities to include triage and analysis within industrial environments and briefing customers on investigation results and recommended courses of action. Also, hunts within industrial environments; including initial planning phases, execution, and reporting phase
- Accomplished exceptional performance in the last three years in delivering superior cybersecurity services in energy sector.
- Enrolled in the SANS Red Team Cyber Guardian program designed for the elite teams of technical security professionals.
- Awarded Penetration Tester of the Year 2016 from EC-Council Foundation InfoSec Tech & Exec.
- Won the Champion of SANS Grid NetWars competition 2019. Also, won SANS Core NetWars, Cyber Defense NetWars and DFIR NetWars 2020.

Personal Info

Phone: +31625525070
Skype: +13218003471 - basemhelmy
E-mail: basem.helmy@hotmail.com
LinkedIn:
https://www.linkedin.com/in/bhemida
Location: Netherlands
Acclaims:
https://www.credly.com/users/bhemida

Languages

- Arabic - Native
- English - Fluent

Area of Expertise

- IT/OT Cyber Strategy
  Balance the requirements to be secure, vigilant, and resilient with strategic objectives and the risk appetite of the organization. Develop an actionable roadmap and governance model to support security priorities in an era where cyber is everywhere.
- Incident Response
  Manage security incidents by understanding common attack techniques, vectors, and tools as well as defending against and/or responding to such attacks when they occur. Concentrating on methods used to detect, respond, and resolve computer security incidents.
- Threat Hunting Operations
  Establish a proactive defense using different tools and techniques and hunt for threats in the organization's network or perimeter. Use threat intelligence and create hypotheses to hunt for known threats, inspect network traffic, identify malicious activities, and detect attack patterns.
- ICS / SCADA Security Assessment
  Design and audit ICS/SCADA network security architecture and align it with the internationally recognized security standard like ISA99 / IEC 62443 and NERC CIP. Moreover, perform in risk assessments of ICS related technologies and day-to-day cyber-related operations. Also, Perform ICS / SCADA security assessments to identify potential vulnerability malicious adversary scenarios that might significantly impact client operations.
- Digital Forensics and Intrusion Detection
  Perform advanced network forensic evidence collection and detailed Forensic examinations related to malicious activities and organization' policy violations. Investigate undetected malware, phishing, network intrusions, defacements, and DNS attacks.
- Red Teaming, Covert Operations and Cybersecurity Crisis Simulation
  Build a Red Team program and leverage Red Team exercises and adversary emulations to obtain a holistic view of an organization's security posture to measure, train, and improve people, processes, and technology for the organization
- Penetration Testing
  Perform multiple penetration tests, and targeting network-level, client-side-level, and web application-level attack vectors.
- Social Security Engineering and Phishing Campaigns
  Perform technical Social Security Engineering to inadvertently steal sensitive information such as usernames & passwords and/or exploit users' computers to gain a foothold into an organization network to be leveraged in a broader scale attack against the organization.

Business Chemistry

Pioneer: Thought Leadership, Seek Possibilities, Spark Energy and Imagination.

Driver: Pursues Challenges and Generates Momentum.

CliftonStrengths DNA:
Strategic, Learner, Competition, Achiever and Adaptability.

My CliftonStrengths themes explain the ways I most naturally think, feel and behave.

Awards

- **SANS DFIR NetWars 2022**
- **SANS Core NetWars 2020/2021**
- **SANS Cyber Defense NetWars 2020/2021**
- **SANS DFIR NetWars 2020**
- **Champion of SANS Grid NetWars *2019***
- **EC-Council Penetration Tester of The Year *2016***
- Third place in CyberLympics Competition - Africa Region - Forensics Round *2013*
- Second place in CyberLympics Competition - Africa Region - Network and Computer Defense 2013
- Third place in Imagine Cup Egypt in the software design category organized by Microsoft 2012
- Second place in Egypt CTF competition "Capture the Flag" 2011

Bassem Hemida | Cybersecurity Senior Manager | Subject Matter Expert

Experience

Cybersecurity Senior Manager - Deloitte
10-2017 – present

Responsibilities

- Lead cybersecurity strategy, secure and vigilant projects.
- Lead incident response activities to include triage and analysis within industrial environments and briefing customers on investigation results and recommended courses of action.
- Lead and build cyber defense capabilities in OT domain for Energy (O&G) industry clients.
- Plan, design and perform tactical network exploitations that simulate adversaries' tactics, techniques and procedures.
- Design Threat hunting hypotheses and conduct hunt operations based on threat intel and APTs TTPs.
- Develop an actionable roadmap and governance model to support security priorities.
- Challenges self and others to make an impact that matters for clients, colleagues, and communities.
- Looks for challenges and opportunities to grow team members' expertise and talents and encourages people to stretch their capabilities.
- Delivers exceptional client service; maximizes results and drives high performance from people while fostering collaboration across businesses and borders.
- Leads teams through the development of mitigation plans that are action oriented, efficient, and aligned with the client's risk tolerance and risk appetite levels.
- Design, build and operate cybersecurity crisis simulation for the top management of the organization in energy sector.

Senior Cybersecurity Specialist - Deloitte
02-2016 – 09-2016

Responsibilities

- Perform advanced penetration testing for systems, network and web applications.
- Develop and implement deception environment for proactive detection.
- Perform social engineering including phishing and vishing.
- Perform incident handling and digital forensics.
- Perform ICS/SCADA assessment and penetration testing.
- Develop and deliver basics and advanced security training.
- Enhance the penetration testing and threat simulation executions.
- Supports team members' development needs through formal and informal coaching and knowledge sharing.

Senior Information Security Engineer - SecureMisr, Egypt
05-2015 – 01-2016

Responsibilities

- Perform advanced penetration testing for systems, network and web applications.
- Perform vulnerability management, security perimeter review and configuration assessment.
- Develop and deliver basics and advanced security training.
- Supports team members' development needs through formal and informal coaching and knowledge sharing.

Senior Information Security Engineer - Diyar United Company, Kuwait
12-2013 – 04-2015

Information Security Engineer - RAYA Corporate, Egypt
01-2011 – 11-2013

Microsoft Student Partner - Internship, Microsoft, Egypt
09-2009 – 12-2010

Microsoft chooses one skilled student from each institution at a time to serve as representatives. Microsoft Student Partners (MSPs) are student technology leaders, empowered to build Microsoft communities on their campus and share their in-depth knowledge and passion for technology with their fellow classmates. Spanning more than 100 countries around the world, MSPs receive:

- **Leadership Experience** - Host fun workshops, run hackathons and give demos on campus to grow a community of students.
- **Resume Building** - Enhance their promotional skills, add to their professional technology experience, and work alongside Microsoft professionals.
- **Exclusive Access** - Receive insider training, exposure to career opportunities, and access to the latest technology events.

Publications

- Compromising Domain Environment | *Pentest Magazine*
- Black-Box Penetration Testing Scenario | *Hakin9 Magazine*
- Penetration Testing Scenario | *Security Kaizen Magazine*
- Discover How the Attack Happened by Wireshark | *Hakin9 Magazine*

Bassem Hemida | Cybersecurity Senior Manager | Subject Matter Expert

Education

SANS Institute - Cyber Guardian: Red Team

04-2019 – present

SANS' Cyber Guardian program is designed for the elite teams of technical security professionals who are part of the armed forces, Department of Defense, or other government agencies whose role includes securing systems, reconnaissance, counterterrorism and counter hacks. These teams will be the cybersecurity special forces where each individual's role makes the team successful.

Egypt, Bachelor Degree in Computer Engineering

09-2007 – 06-2011

Graduation Project Name: DNS Spoofing Attack Detection and Prevention.
Graduation Project Grade: Excellent.

Certificates

- Project Management - Harvard ManageMentor
- GIAC Response and Industrial Defense (GRID) – Hold CTF Coin
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH) - Hold CTF Coin
- GIAC Certified Intrusion Analyst (GCIA) - Hold CTF Coin
- Global Industrial Cyber Security Professional (GICSP) - Hold CTF Coin
- Threat Hunting Professional (eCTHP)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) - Hold CTF Coin
- Offensive Security Certified Expert (OSCE)
- SANS Red Team Operations and Threat Emulation
- GIAC Penetration Tester (GPEN) - Hold CTF Coin
- SpecterOps Adversary Tactics: Red Team Operations (ATRTO)
- GIAC Certified Web Application Pen Tester (GWAPT) - Hold CTF Coin
- Offensive Security Certified Professional (OSCP)
- EC-Council Certified Penetration Tester (LPT)
- EC-Council Certified Security Analyst (ECSA)
- EC-Council Certified Forensics Investigators (CHFI)
- EC-Council Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate (CCNA) & (CCNA-Security)

Courses

- SANS ICS612: ICS Cyber Security In-Depth - Hold CTF Coin
- SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
- SANS MGT414: SANS Training Program for the CISSP Certification
- SANS FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
- Windows Red Team Lab (Pentester Academy)
- Offensive Security: WiFi Penetration Testing (WiFu)
- Advanced Web Attacks and Exploitation (AWAE)
- Web Application Penetration Testing eXtreme (WAPTXv2)
- Microsoft Certified Systems Administrator
- Assessing and exploit web applications with SamuraiWTF
- Symantec Critical System Protection