Bassem Hemida | Senior Manager | CISO | Team Lead | GSE #301

Summary

A cybersecurity Senior Manager/CISO/Threat Management Lead 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.

- Design, Build and Manage global threat management capability for ING, while operating tactical, operational, and strategic threat informed defense approach on daily operations.
- Successfully planning, supervising, and managing multifaceted cybersecurity roadmap projects with multiple deliverables, complex dependencies and multi-million-dollar budgets.
- 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 IT and 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.
- 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.
- Accomplished exceptional performance in delivering superior cybersecurity services in energy sector.
- Teacher Assistant at SANS Institute for multiple classes.
- 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 NetWars {Core, Cyber Defense, DFIR} {2020, 2021}.

NATO – Locked Shields 2024

April 2024

Locked Shields is NATO's annual and largest international, real-time cyber warfare exercise. Bassem selected to be the advisory to lead and support team to protect and respond to attacks carried out against critical infrastructure of gas and power. During the exercise, Bassem Desing and guide the team to Implement defensible architecture maintained 100% available services of the critical infrastructure while monitor, detect and prevent attacks.

Area of Expertise

- Manage Threat Informed Defense
  Design and implement a threat-informed defense approach by leveraging various threat intelligence sources and tools to provide actionable insights to enhance detect, protect and response capabilities. Effectively communicate threat intelligence at all levels of the organization and work closely with security operations and incident response teams to ensure they have the necessary intelligence to detect and respond to threats.
- Incident Response and Threat Hunting Operations
  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 cyber security incidents.
  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.
- 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.
- 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.

Personal Info

Phone: +31625525070
E-mail: ping@bhemida.com
Website: https://bhemida.com
LinkedIn:
https://www.linkedin.com/in/bhemida
Location: Netherlands
Acclaims:
https://www.credly.com/users/bhemida

Public Talks

https://github.com/bhemida/SANS-NightTalks.git

- Using Offensive Operations to Defend Industrial Operations.
- Cyber Informed Defense.

Business Chemistry

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

Driver: Pursues Challenges and Generates Momentum.

Clifton Strengths DNA:
Strategic, Learner, Competition, Achiever and Adaptability.

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

Bassem Hemida | Senior Manager | CISO | Team Lead | GSE #301

Experience

CISO Global Threat Management Lead – ING Netherlands

08-2023 – present

Responsibilities

- Managing and leading a team of cyber security analysts, engineers for daily threat operations.
- Collaborate with incident response team in high profile incident management.
- Design threat management function to cover intrusion intel, threat intel, vulnerability intel and strategic intel to cover the intent, capabilities, and opportunities of applicable threat actors to the business.
- Contextual application of MITRE Attack Framework, Cyber Kill Chain, Dimond Model and Defensible architecture to enhance threat detection, incident response, and proactive cybersecurity measures.
- Define team operating model, objectives, and outcomes; Enable success across boundaries and integrate with different cyber security functions and capabilities.
- Hire and retain great people; understand their business chemistry profiles technical capabilities and invest in their development and improvements.
- Communicate complex and technical issues to diverse audiences, verbally and in writing, in an easily understood, authoritative, and actionable manner. Present to a wide range and size of audiences from IT Pro, to CxO, to business decision makers.
- Technical leadership and executive presence to establish Trusted Technical Advisor to influence senior decision makers to mature and promote security posture across the overall technology landscape.
- Process industry knowledge and external threat intelligence into actionable business communication.
- Support the evolution of both proactive and reactive detection and investigation capabilities.
- Maintain business operations: Deliver against metrics, KPIs for my business unit. Responsible for technical and executive level reports on cyber threats.
- Manage vendors technical and contractual terms and perform service evaluation to maintain receiving the excellence service level.

Cybersecurity Senior Manager – Deloitte NSE

10-2017 – 07-2023

Responsibilities

- Lead cybersecurity strategy, secure and vigilant projects.
- Lead incident response activities to include triage and analysis within IT/OT 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 intelligence.
- Develop an actionable roadmap and governance model to support security priorities.
- 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 financial and energy sectors.

Senior Cybersecurity Specialist – Deloitte ME

02-2016 – 09-2016

Senior Information Security Engineer - SecureMisr, Egypt

05-2015 – 01-2016

Senior Information Security Engineer - Diyar United Company, Kuwait

12-2013 – 04-2015

Information Security Engineer - RAYA Corporate, Egypt

01-2011 – 11-2013

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

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*

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.

Education

SANS Institute - Cyber Guardian

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

- **GIAC Security Expert (GSE) #301**
- **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)

GIAC SECURITY GSE EXPERT
GIAC EXPLOIT RESEARCHER & ADVANCED PENETRATION TESTER GXPN
GIAC NETWORK GNFA FORENSIC ANALYST
GIAC PENETRATION GPEN TESTER
GIAC CERTIFIED GCIA INTRUSION ANALYST
GIAC CERTIFIED GCIH INCIDENT HANDLER
GIAC SECURITY ESSENTIALS GSEC CERTIFICATION
GIAC WEB APPLICATION GWAPT PENETRATION TESTER
GIAC RESPONSE AND GRID INDUSTRIAL DEFENSE
GIAC INDUSTRIAL CYBER SECURITY GICSP PROFESSIONAL
OFFENSIVE security OSCE
OFFENSIVE security OSCP

Courses

- **SANS MGT553: Cyber Incident Management**
- **SANS MGT512: Security Leadership Essentials for Managers**
- **SANS MGT516: Building and Leading Vulnerability Management Programs**
- SANS FOR572: Advanced Network Forensics
- SANS ICS612: ICS Cyber Security In-Depth - Hold CTF Coin
- SANS MGT414: SANS Training Program for the CISSP Certification
- SANS SEC522: Application Security: Securing Web Apps, APIs, and Microservices
- SANS FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
- Windows Red Team Lab (Pentester Academy)
- Advanced Web Attacks and Exploitation (AWAE)
- Web Application Penetration Testing eXtreme (WAPTXv2)
- Microsoft Certified Systems Administrator