CISO-SIEM/SOC Manager

Personal details

Name: Alon Shoam | Family status: Married +2 | Phone: +972 54-6686407 | Email: alons@sec4cyber.com

Summary

✓ **Cyber Network Security Researcher & Architect** with Curiosity, Passion and Initiative.

- ✓ Deep experience with **SIEM/SOC** systems-establishing, Integration and implementation, including **mentoring** the **Cyber Defense and Response Center (CDRC),** managing and **Leading- teams.**
- ✓ Strong experience in **Networks Security** with a focus on– Firewalls. Web App Firewalls, DLP, EDR, DRP and BCP system Networking.
- ✓ Design a **solution** Deep **cyber security experience** across a broad portfolio of **security technologies** and platforms and **tools.**
- ✓ **TCP/IP, IPSEC, TLS, HTTP/S, Routing protocols**
- ✓ Deep Knowledge in **Cryptography and Encryption** methods (teaching cryptography at Ariel university)
- ✓ Strong experience in security, **cloud services and Linux Admin/programing.**
- ✓ Deep experience of **cloud platforms like AWS, Azure, and Google Cloud Platform.**
- ✓ create and maintain **NAS files** and **SAN storage** for **Linux filesystem** and **Oracle/MySQL/PostgreSQL, NoSQL dataspaces.**
- ✓ configuring static routing, implementing **FW rules** and installing and configuring **access** to **DNS, SMTP, Monitoring, Backup servers** etc.
- ✓ Deep experience in **troubleshooting sessions** (**cluster** active groups, fail-over, **LDAP, jumpers, Networking**, dual homing, **filers access,** etc).
- ✓ Strong experience **RedHat,** ESX, **VMWare virtualization**, **SAN/NAS,**
- ✓ Deep experience **software Security** in conjunction to WEB, Scope & Responsibility Cyber security.
- ✓ Strong experience in **Cloud security** architecture and Implementation in: **Amazon (AWS), Google (GCP), Azure.**
- ✓ **Risk assessment, Penetration testing** of IT Networks and Web Applications,
  - ➢ **Hardening** guidelines **weaknesses/ Vulnerabilities** and **closing gaps** in infrastructure and applications.

✓ **Penetration testing** of **Networks and Web Applications** – including REST/SOAP APIs and platform assessments.

- ✓ Deep experience in **Reverse Engineering** (**Malware)** Assembly tools: **IDA, OllyDbg, windbg,**
  - ➢ Research & Development with tools like: **Frida, IDA, GDB, MITM**
  - ➢ proven hands-on **software** experience in **hacking, breaking** and disrupting **complex cyber security products.**

✓ Strong experience in **reverse engineering** and debugging malicious code in **Real-Time** (dynamic and static files) using **virtual** or **physical debuggers.**

- ✓ Researching **Docker,** the world leading software **containers cloud** platforms and **Kubernetes - K8s,** design **Cloud/Cyber security solutions.**
- ✓ Researching **Linux kernel,** IOT device **- Linux RT Embedded Systems** and , hardening and design **kernel core system security protection**

✓ **Security Code Review (SSDLC)** - **C++, Java, Java Script, Python,** Developing and implementing Secure Software Development Life cycle, with **OWSP Benchmark Project Tools:**

- ✓ Strong experience in **Code scripting and Automation,** languages:
  - ➢ **C, C++, Linux-Bush**, **Python**, **PowerShell, Django, Flask, REST API, Java, Java Script, Node.JS, Jira, PLSQL(Query's).**

➢ **DevOps CI/CD: Git, Jenkins, BITBUKET(GIT), Java Spring Boot, Terraform, Ansible, Kubernetes - K8s, Virtualization, Web Services, Docker, PowerShell, Jira, OpenStack, OPENSHIFT.**

➢ **Amazon Web Services (AWS): EC2, RDS, S3, ElastiCache, ECS/EKS, Elastic Beanstalk, Spotinst, Cloud Formation, API Gateway** and their **management console**.

➢ **Google (GCP): App Engine, Compute Engine, Kubernetes Engine, OPENSHIFT,** Cloud Functions, Google **Open Source.**

➢ **Azure-DevOps, TFS, Azure Cloud**

➢ **Linux: BASH Shell Scripts, Ubuntu, Debian, Centos, RedHat, Kernel Programing,** Package Management (APT), **Apache, Tomcat**.

➢ **Mobile-Android Platform**

✓ **Big Data, Open source**, Oracle, **MS SQL, HADOOP, MongoDB, Redis, Spark, MySQL** DB and tools like **Elasticsearch.**

Deep knowledge of **Open source** Technologies like **Docker, Kubernetes**

✓ Strong **troubleshooting** and multitasking skills

✓ Strong **leadership** with excellent **Team mentoring** and driven people to meet **goals**.

Employment Experience

2016 - Current: 1. Cyber Security Researcher & Architect, 2. CTO &Co' Founder SafeTrip (cyber) venture, at **Sec4Cyber LTD**

✓ Strong experience in security, **cloud services and Linux Admin/programing.**
✓ Deep experience of **cloud platforms like AWS, Azure, and Google Cloud Platform.**
✓ create and maintain **NAS files** and **SAN storage** for **Linux filesystem** and **Oracle/MySQL/PostgreSQL, NoSQL dataspaces.**
✓ configuring static routing, implementing **FW rules** and installing and configuring **access** to **DNS, SMTP, Monitoring, Backup servers** etc.
✓ Deep experience in **troubleshooting sessions** (**cluster** active groups, fail-over, **LDAP, jumpers, Networking**, dual homing, **filers access,** etc)
✓ Strong experience **RedHat,** ESX, **VMWare virtualization**, **SAN/NAS,**

✓ **SIEM/SOC systems-establishing** and implement including mentoring the Managing and Leading- **Cyber Defense and Response Center (CDRC) teams**.

✓ **Risk assessment, Penetration testing** of IT Networks and Web Applications,

➢ **Hardening** guidelines **weaknesses/ Vulnerabilities** and **closing gaps** in infrastructure and applications.

✓ **Penetration testing** of **Networks and Web Applications** – including REST/SOAP APIs and platform assessments.

✓ Deep experience **developing tools** to **automate security testing.**

✓ **Researching Docker,** the world leading software **container** platforms and

Design a solution for **Cloud Security** for **CISCO** cloud services.
Solid understanding of **SaaS and IaaS cloud** system architecture

2012-2016: CISO-SIEM/SOC Manager, Cyber Defense and Response Center (CDRC) at

Government Prime Minister's Office.

✓ **Security Code Review (SSDLC)** - Developing and implementing Secure Software Development Life cycle, with **OWSP Benchmark Project Tools:**

➢ **Networking & Security** with a focus on– Firewalls. Web App Firewalls, DLP, DRP and BCP system Networking, software and Security in conjunction to WEB, Scope & Responsibility Cyber security.

- ➢ Establishing and Leading and Managing **SIEM/SOC team**– **12Professional Cyber Analysts,**
  - ✓ Leading, Coaching and mentoring the team **Computer Security Incident Response Team (CSIRT).**

- ➢ Implements comprehensive Policies, Procedures and Guidelines, that conform to the goals and objectives established by the management and by regulatory laws Manage/coordinates the IT Department Business Resumption Plan and ensures that it complies with company's policy.

✓ **Risk assessment, Penetration testing** of IT Networks and Web Applications,

- ➢ **Hardening** guidelines **weaknesses/ Vulnerabilities** and **closing gaps** in infrastructure and applications.

✓ **Reverse Engineering** (**Malware)** Assembly tools: **IDA, OllyDbg, windbg,**

2010-2012: CTO-Security Researcher/Architect at a **Web Application Security Start-Up "**Applicure Technology"**.**

- ✓ **Fullstack (Backend)** Web App Development Code scripting and design.
- ✓ **DevOps –CI/CD/BUILD Pipelines, DEVOPS** processes, WEBSPHERE / **Apache/Tomcat.**
- ✓ Build and Lead **R&D** multidisciplinary **Agile - scrum teams**.
  - ➢ Build **flexible development teams** that can react fast to **changes**.
- ✓ Leading and **mentoring R&D Cyber Security** development teams,
  - ➢ Intensive work with R&D internal teams: Server, GUI, Algorithm, QA & Support/Operations
- ✓ **Product Managing** With a focus on Web Application/SAAS (Security Web Application).

- ✓ Part of the Executive **Leadership** Team
- ✓ Analyzes the **needs** of the **customers** and establishes priorities in all offices
- ✓ Respond to **product**, commercial, legal and technical queries from. Customers.

20**09**-201**0:** **CTO-IT- Networks Security group manager** at "KDE Group".

- ✓ **Leading** and **Managing Networking** & **Security** teams – 20 Professional engineers/ Consultants.

2002 – 20**09:** Outsourced by the Ness Technologies Group:

✓ **IT Manager, Networks & Information Security Team Leader** at Governments offices and Bank Leumi

Education

2001-2005: **(B.Sc.)** bachelor's degree in Computer science–graduate

"**Tel Aviv** University"

2001:**MCSE** – **Microsoft** Certified - Self Learning.

2004: **CCNA** – Cisco Certified - Self Learning.

2006: Team Managing - "Ness College"

2007: **Linux Admin/programming**

2012: **CISSP** – Information **security** worldwide certification

2011: **Symantec** - SSE, SSE+

2014: Defense Pro (**DOS -IPS**) – Radware

2014**: IBM WebSphere** – Data Power

Languages: Hebrew mother tongue, **Fluent English**, Basic Spanish/Portuguese, good Arabic.

Military Service: A warrior - sniper, an Officer – Platoon leader at a special unit in paratroopers.

Professional and personal references will be provided upon request