Yossi Barishev

Information Security Professional

Profile

i'm a passionate cybersecurity professional with years of experience designing, practicing and managing cybersecurity & security teams within enterprises - specializing in creating and executing security strategies that balance the organizational risk tolerance and the business objectives.

Employment History

Senior Security Engineer at CyberArk , Petah Tikva, Israel

June 2019 — Present

As a senior security engineer I was tasked with hands-on responsibility over all of CyberArk's security solutions, being a subject matter expert for most of CyberArk's security solutions and the seniormost member of the SecOps team.

Under this position, I am performing the following:

- Hands-on management & enhancement of CyberArk's: Endpoint protection, EDR, DLP, IPS\IDS, Web proxy, mail filtering, SSL-VPN, NAC, Compliance Management, SIEM, FW & CyberArk products (EPM, PAM, SIM)

- Leadership of CyberArk's DLP program - including writing CyberArk's DLP architecture & process, implementing a market-leading DLP solution from end-to-end & working with CyberArk's upper management to tailor a suitable DLP policy.

Global SOC & IR Team Manager at CyberArk , Petah Tikva, Israel

June 2018 — June 2019

Managing CyberArk's Global Cyber Defense & Response Center, Leading a global team of security professionals tasked with assuring the continuous cybersecurity of CyberArk.
Among things, I was personally responsible for:

- Building & executing a multi-year project & financial strategy to enhance CyberArk security measures with the emphasis of increased visibility and automation in the SOC arena.

- Designing CyberArk's IRP including the performance of "dry" & "wet" drills to the security staff & table-top exercises for c-level/VP employees.

- Leading & delivering on numerous projects within CyberArk's security division, including - SIEM replacement, Compliance management solution implementation & EDR solution deployment

- As an additional responsibility - I was tasked with developing, from scratch, CyberArk's current risk management framework - resulting in a unique & highly effective quantitative risk management matrix.

- During this time I was also CyberArk's Physical security officer & was responsible for all of CyberArk's global physical security needs - from a policy level to a hands-on solution implementation level.

Details

+972507865848
yossi@zensec.co

Links

Linkedin

Skills

- SOC/CIRT Management
- Threat Hunting
- Reverse Engineering
- Digital Forensics
- Risk Management
- Procedure & Policy Writing
- Direct Management of Global Teams
- Scripting (Python, PowerShell, Bash, C++, JavaScript)
- Security Solution Implementation
- Project Management
- Work Plan Creation
- Security Awareness Solidification
- Really Good Guitar Player

Languages

- Hebrew
- English
- Russian
- German
- Arabic

Private Cybersecurity Consultant at Self-Employed, Israel

January 2017 — Present

- Providing incident response & digital forensics services to private institutions

- Performing CISO as a service role as a contractor on behalf of a security company in Israel

- Senior lecturer on CyberSecurity Subjects in israel's largest security colleges (See-security, HackerU)

- Developing and leading Israel's first Cybersecurity Engineering course - CSP in See-Security.

DIFR Team Leader & Security Professional at Intelligence Corps , Israel Defense Force

June 2015 — June 2018

Currently in active reserve duty in unit 8200

During my time in the intelligence corps I was leading a team of 2 forensic analysts, being responsible for incident response & forensics across all of IDF's branches, handling over 150 cases over a period of 3 years.

Along my DIFR leadership duties, I was personally responsible for a number of IDF-crossing projects & have received a citation (Tzalash) from IDF Intelligence corps commander Maj.Gen Herzi Halevi.

IT Technician & Security Administrator at GK&CO, Ramat Gan

March 2014 — June 2015

Providing IT Administration services for a medium-sized law firm including:

- Management of corporate IT services

- Configuration of security systems within the corporate network (Firewalls, GPO, UAC)

- Technical support for all IT-related issues

Education

Bachelor of Science in Physics, Technion - Israeli Institute of Technology

2012 — 2014

Did not finish - Financial reasons (about 2 semesters short)

CISO Course, See Security College

May 2017 — May 2018

CCSK, Cloud Security Alliance

2018 — 2018

Certified Forensic Examiner, IDF

2017 — 2017