it-sa 2017

October 10-12 | Hall 9 | Stand 9.0-240
Nuremberg | Germany

ISRAEL
CYBER
ALLIANCE

THE ISRAEL EXPORT &
INTERNATIONAL COOPERATION INSTITUTE

Ministry of Economy and Industry
Foreign Trade Administration

Prime Minister's Office
National Cyber Directorate
National Cyber Bureau

THE ISRAEL EXPORT &
INTERNATIONAL COOPERATION INSTITU

Ministry of Economy and Industry
Foreign Trade Administration

Prime Minister's Office
National Cyber Directorate
National Cyber Bureau

Content

Click on company name or page number

Page

THE ISRAEL EXPORT &
INTERNATIONAL COOPERATION INSTITUTE

The Israel Export & International Cooperation Institute

The Israel Export and International Cooperation Institute is your premier gateway for doing business with Israeli companies. Established and funded by the government and the private sector, IEICI's expertise in technology and product scouting, joint ventures and strategic alliances with Israeli companies spans more than half a century. Whatever your field is, IEICI offers access to relevant businesses and government resources. With expertise in Israel's leading Industries, IEICI will provide the information you need to connect, negotiate and do business.

Mr. Achiad Alter ▪ Manager, Cyber Security
T +972 3 514 2971 ▪ **M** +972 52 889 1181 ▪ achiada@export.gov.il

Mrs. Maya Vaknin ▪ Production Manager for Int'l Exhibitions
M +972 50 492 9392 ▪ mayav@export.gov.il

29 Hamered St. ▪ Tel Aviv 68125, Israel ▪ F +972 3 514 2881
www.export.gov.il

Ministry of Economy and Industry
Foreign Trade Administration

Foreign Trade Administration

Israel's Foreign Trade Administration at the Ministry of Economy and Industry is responsible for managing and directing the international trade policy of the State of Israel. The FTA has 43 offices around the world. Out of which two are located in Germany.

The Economic & Trade Missions in Munich and Berlin are the representatives of the Israeli Ministry of Economy and Industry. Their primary mission is the promotion of business relations between Israel and Germany, facilitating trade, economic cooperation, investments and R&D collaboration. The teams located in Berlin and Munich assist Israeli and German companies and organizations in opening doors and providing market information to facilitate successful long term relationships.

Munich

Ms. Yifat Inbar ▪ Head of Economic & Trade Mission, Munich
M +49 89 543486506 ▪ munich@israeltrade.gov.il

Ms. Alisa Rubinstein ▪ Trade Officer Cyber Security
Economic & Trade Mission, Munich
M +49 89 54348 6557 ▪ alisa.rubinstein@israeltrade.gov.il

Berlin

Mr. Doron Abrahami ▪ Head of Economic & Trade Mission, Berlin
M +49 30 2064 4912 ▪ berlin@israeltrade.gov.il

Ms. Hanna Dwertmann ▪ Senior Trade Officer, Economic & Trade Mission, Berlin
M +49 30 2064 4912 ▪ Hanna.Dwertmann@israeltrade.gov.il

Prime Minister's Office
National Cyber Directorate
National Cyber Bureau

INCD - Israel National Cyber Directorate

Israel National Cyber Directorate (INCD) in the Prime Minister's Office serves as the Prime Minister's and Government's staff, which devises national cyber defense policy, promotes its implementation and provides recommendation on cyber-related matters. The INCD is responsible to create and improve national cyber security capacities and capabilities in order to overcome challenges emanating from cyberspace. The INCD strives to advance Israel's leading posture as a global powerhouse for cyber security-related research and development, by investing dedicated resources in the Israeli academy, human capital and cyber security industry. The INCD enhances the cooperation and synergy between the private sector, the government and international partners, in order to create a unique and dominant cyber security ecosystem in Israel.

Mr. Roi Yarom ▪ Policy Planning
National Cyber Bureau
Israel's Prime Minister's Office
M +972 52 838 9523 ▪ RoiYa@pmo.gov.il
www.pmo.gov.il

Cyber Sector

The IEICI's Cyber Security Sector - Since the creation of the internet and cyber space, Israeli security experts and engineers have been fighting at the forefront of cyber defense against cyber-crime, preventing and detecting online fraud, intercepting computer espionage, protecting critical infrastructures and minimizing vulnerabilities of national, municipal, commercial and private sectors. As a world leading cyber power and a major player in the world's cyber security field, Israel's cyber security industry develops a wide range of cutting edge and creative solutions for the constantly increasing threats in the cybernetic field.

Israel's multitude of cyber security solutions address the needs of millions and protect the lives of billions through innovative solutions.

The IEICI's Cyber Security Sector represents over 300 companies in the cyber security arena. Israeli Cyber Security companies offer technologically advanced and field-proven products, which are amongst the most innovative solutions.

IEICI holds the most updated and comprehensive database of the Israeli based Cyber Security companies, which allows it to achieve end to end ties solution pack and connections, according to a specified need.

The sector successfully partnered with key players worldwide and is cooperating with foreign governmental ministries, agencies, as well as industry entities in order to promote private-industry joint ventures and international partnerships with Israeli cyber security companies.

Mr. Achiad Alter ▪ Manager, Cyber Security
T +972 3 514 2971 ▪ **M** +972 52 889 1181
achiada@export.gov.il

Ms. Yaara Sabzerou ▪ Marketing Coordinator, Cyber Security
T +972 3 514 2805 ▪ **M** +972 50 822 8357
yaaras@export.gov.il
www.export.gov.il

BUFFERZONE

BUFFERZONE Security

www.bufferzonesecurity.com

Endpoint Security

Company at a Glance

BUFFERZONE is a patented virtual container solution that isolates web browsers, email and removable storage and prevents threats from entering the organization. Without restricting or inconveniencing employees, BUFFERZONE complements your existing endpoint security platforms to prevent the advanced threats that evade conventional security solutions.

Technology & Products

The BUFFERZONE virtual container protects any content source that you define as potentially insecure including web browsers, email attachments, Skype, FTP and even removable storage. With BUFFERZONE, you can define granular containment policies according to network segment, file location or file tag, digital signature, and URL/IP source. BUFFERZONE is transparent to both the application and the end-user, yet completely seals off threats from the rest of the computer. It isolates the entire application environment – memory as well as files, registry and network access. Any infection attempt will be confined to the boundaries of the container, and will not reach the endpoint.

Back to Content

CORONET

Coronet

www.coro.net

Cloud Security | Intelligence | WEB and application security | Risk and Compliance (GRC), Secure ICS and OT

Company at a Glance

Usage of services outside the perimeter spans three domains: the device, the network, and the cloud service itself. Coronet is the one platform designed exactly for that: Secure any cloud service usage, on any device, running any OS, connecting through any network.

Technology & Products

Coronet's all-in-one SaaS Solution enables and secures cloud services for the full security chain Device posture Running natively on any OS, Coronet ensures OS integrity, safety and device health and will even recommend proactive prevention acts to ensure that the device is not compromised. Network posture No need for any hardware. Coronet ensures that the network or infrastructure the user connects to is safe and not compromised, and that there is no malicious activity around the user, for both Wi-Fi and Cellular, on private and public networks. Cloud service posture Coronet verifies the integrity of the cloud service, provides proactive prevention against risky configurations, and enables the organization to easily define risk-based policy for accessing services.

Take Control, Get CyBot

Cronus Cyber Technologies

www.cronus-cyber.com

Incident management - SIEM /SOC | WEB and application security | Penetration Testing | Vulnerability Managment

Company at a Glance

Cronus aims to bring back control to the CISO, for the first time the company can see an actual visual map of all the possible validated routes hackers could take to bring their network down, focusing on key business processes and critical assets. Cronus is fully commercial in Europe.

Technology & Products

Cronus provides autonomous applicative and infrastructure penetration testing. CyBot is a patented machine-learning solution installed as a virtual machine on private or public cloud. CyBot can be deployed globally to provide a map of global Attack Path Scenarios with a focus on your business processes with a one click integration to your SIEM. No need for human cyber expert to install or interpret data and it will not crash your network. CyBot will give you visibility to your main threats so you will be fully prepared and protected against the next attack.

THE HUMAN READINESS COMPANY
CYBEREADY

CybeReady

www.cybeready.com

Identity Management and Fraud | Risk and Compliance (GRC) | Training and consultant | Phishing Security

Company at a Glance

We enable organizations to transform their security culture by strengthening their first line of defense: employees. Where others see end users, we see individuals. Where they find limitations, we find opportunities. We constantly adapt to our customers, delivering the best security learning experience that influences company culture, processes and practices.

Technology & Products

CybeReady solves security's most pervasive and unpredictable problem: employee behavior. We provide a data-driven learning experience through an automated adaptive solution that solves our customers' security challenges by minimizing the risk of phishing. With CybeReady, ease-of-use and optimal results go hand in hand, freeing up your staff's time to tackle other critical objectives. Our state-of-the-art smart learning engine constantly adapts personalized simulations and just-in-time training content in direct response to your employees' actions. As phishing attempts evolve, so does our technology, which constantly formulates new attacks and varied content-driving up engagement rates and providing you with proven results in the process.

Back to Content

Cynet

Advanced Threat Detection & Response

Cynet Security

www.cynet.com

Intelligence | Incident management - SIEM /SOC | Identity Management and Fraud | Risk and Compliance (GRC) | Perimeter and APT Security | Forensic and Analytics

Company at a Glance

Cynet is a pioneer in advanced threat detection and response. The Cynet 360 platform simplifies security by providing one rapid, easily integrated solution for Endpoint Detection & Response, UEBA, Network Analysis, File Analysis, Deception, Threat Intelligence, Forensics, Incident Response, 24/7 Monitoring and more.

To learn more, visit: www.cynet.com

Technology & Products

The Cynet 360 advanced threat detection and response platform simplifies enterprise security by providing a holistic answer to all the organization's protection and prevention needs. Cynet 360 decreases security spend by providing multiple capabilities in a single solution, while putting less drain on organizational resources, manpower and budget. Additionally, the 360 platform provides the highest level of enterprise security by correlating indicators across systems, thus increasing visibility and accuracy of detection throughout the organization, without the need for multiple cyber security solutions.

Cytegic

www.cytegic.com

Intelligence | Risk and Compliance (GRC), Forensic and Analytics

Company at a Glance

Cytegic's cyber risk platform provides an automated end-to-end solution that encompasses the entire scope of cyber risk management. Cytegic's scientific approach provides digital-related risk oversight across the entire organization. The cutting-edge patented technology provides best in industry cyber risk management with unprecedented accuracy, agility and friendliness.

Technology & Products

The ACRO Suite is comprised of:

CDSS - Cyber Decision Support System correlates external threat landscape, internal control maturity and organizational business profile to generate continuous cyber risk assessment, action items for risk mitigation and financial impact analysis. CDSS enables managers to simulate "what-if" scenarios and allocate resources optimally to mitigate risk for each asset.

CyMA - Cyber Maturity Assessment module automates the collection, processing and analysis of maturity of cybersecurity controls. With a multi-standard reporting and dashboard capability, CyMA allows to quickly and automatically assess the cybersecurity readiness of the organization.

DyTA - Dynamic Trend Analysis module is an automated intelligence fusion and analysis platform that identifies geopolitical and industry related threat trends. DyTA generates cyber-threat forecasts based on built-in pattern analysis capabilities.

empow

You have it in you.

empow Cyber Security

www.empownetworks.com

Intelligence | Incident management - SIEM /SOC | Risk and Compliance (GRC) | Perimeter and APT Security | Forensic and Analytics | orchestration

Company at a Glance

empow's security platform enables deciphering the intent of actors and events, and orchestrates optimized investigation and remediation/mitigation actions accordingly. This reduces the noise and false positives in security systems, automates investigation and dramatically accelerates the time to resolution of security incidents. All while using the security tools you already have.

Technology & Products

empow's security platform radically upends traditional approaches by integrating with your existing network infrastructure and breaking down your security tools to their individual components – what we call "security particles™." This creates an abstracted new layer that sits above your existing security configuration, and turns what you have into what you need.

When empow identifies an event, a new, targeted security apparatus is instantly reassembled and deployed for each individual attack, in real time. This means quicker and smarter responses, with better correlation and insight. And the innovation is equally applicable to all flavors of attack campaigns.

empow gives you the confidence of knowing your security organization is responding in the right way, every single time. In parallel, empow's platform also provides transparency and visibility into the performance of the organization's security tools, in light of its risks focus, making sure security investments are optimally planned, executed and continuously evaluated.

Back to Content

GuardiCore

GuardiCore **www.guardicore.com**

Cloud Security | Risk and Compliance (GRC) | Forensic and Analytics

Company at a Glance

GuardiCore provides a highly scalable data center and cloud security solution that helps our customers more easily understand, monitor and control east west traffic and detect and respond to breaches faster. We also help many of our customers migrate securely to public cloud and secure multi-cloud and hybrid cloud environments.

Technology & Products

GuardiCore is a data center security company that helps businesses to effectively control east-west traffic and more quickly detect and respond to breaches. The Centra Security Platform is a single, scalable platform that covers five critical areas of data center security: visibility, micro-segmentation, breach detection, automated analysis and response. Our real-time breach detection capabilities feature high-interaction, dynamic deception technology that identifies active breaches with low false positive rates. A lightweight, distributed architecture scales to cover all traffic without impacting performance, and can support virtually any data center infrastructure.

illusive®

illusive networks

www.illusivenetworks.com

Perimeter and APT Security

Company at a Glance

illusive networks was founded in 2014, and already its solutions are used by multiple banks, law firms, technology, and telecom organizations around the world. illusive's chairman is the former head of the IDF's Technology & Intelligence Unit (the "Israeli NSA"), with Cisco and Microsoft as company investors, to name some.

Technology & Products

Deception technology is the most effective way to detect advanced attackers early. Using fake information such as user-credentials, servers, and websites, you can detect attackers before they reach sensitive data. To remain one step ahead, state-of-the-art, network-optimized deceptions automatically and dynamically construct a deceptive layer over your entire network, with zero IT footprint and no agents installed. By constantly creating an environment where attackers cannot tell real information from fake information, deceptions ensure that the data attackers collect is always unreliable. And if attackers cannot rely on collected data, they cannot proceed and the attack is neutralized.

Reblaze

Reblaze Technologies

www.reblaze.com

Cloud Security

Company at a Glance

Reblaze offers an all-in-one private virtual cloud-based solution (VPC) that includes IPS/WAF, DoS/DDoS protection, bot detection and exclusion, anti-scraping, and more. Using a unique approach, Reblaze monitors and cleanses the traffic before it reaches the customers' data-centers, and can easily work with existing security solutions. The solution requires five-minute setup, zero installation, and can be deployed even under an attack.

Technology & Products

Defeats DoS and DDoS Attacks From brute-force traffic floods to sophisticated application-layer exploits, Reblaze defeats all forms of denial-of-service attacks. Defeats Intruders, Hackers and Data Thieves Robust WAF/IPS modules identify and block attackers. Defacements, SQL injections, XSS, and other web attacks are prevented. Reblaze's sophisticated human detection and behavioral analysis algorithms filter out scraper bot traffic, preventing competitors and aggregators from harvesting your business data. Provides Numerous Other Benefits - CDN integration - accelerating your site's performance - Traffic control - filtering visitors by their city, country, network, data center, and behavior - Can act as an additional layer to your existing security - Many other benefits: load balancing, real-time traffic analysis, a complete DNS solution, and more.

SAFE-T
Smart Security Made Simple.

Safe-T

www.safe-t.com

Data protection | encryption and recovery | Cloud Security | WEB and application security | Risk and Compliance (GRC) | Perimeter and APT Security

Company at a Glance

Don't let your or your customers' data continue to be compromised

Safe-T's High-risk Data Security (HDS) Solution is designed to mitigate data related threats. Including un-authorized access to data, services, networks, or APIs; as well as data exfiltration, leakage, malware, ransomware, and fraud.

Technology & Products

Safe-T Data's Integrated Data Security Platform (IDSP) provides the foundation for Safe-T's Safe-T High-risk Data Security (HDS) solution, providing it all the technology components required to create a true Cyber Dome. Enterprises that deploy IDSP can scale up according to business needs by adding key products and services that integrate seamlessly with the platform. The Safe-T IDSP enables customers to benefit from an advanced security architecture, policies and workflows, strong data encryption, high availability, roles management, reporting, and detailed audit trails.

<

>

GATESCANNER
By Sasa Software

Sasa Software

www.sasa-software.com

WEB and application security | Perimeter and APT Security | Content Security | CDR

Company at a Glance

Sasa Software is a leading provider of extensive content disarm and reconstruction solutions (CDR). Our Gate Scanner® products disarm incoming files and emails, protecting against known, unknown and undetectable threats, including ransomware. We protect over 160 enterprises worldwide, focusing on healthcare, governmental, financial institutions, and public utilities.

Technology & Products

Gate Scanner® mail, an additional layer of protection between your secure email gateway and mail server. Gate Scanner® Secure Browsing safely releases files from the secure browsing platform into the user's endpoint. Gate Scanner® Kiosk eliminates threats from detachable media. Solution deployed as a tamper proof appliance, at a central location. Gate Scanner® Desktop, all of the capabilities of the kiosk at the user's endpoint. Gate Scanner® Multi Source eliminates threats from B2B files transfers and files arriving to the organization from 3rd party applications. Gate Scanner® Injector is a one-way optical gateway to send files into a sensitive network.

SCADAfence

SCADAfence

www.scadafence.com

Secure ICS and OT | Building Automation

Company at a Glance

SCADAfence is a pioneer in securing Industrie4.0 networks in smart manufacturing and smart building sectors from cyber threats. SCADAfence's passive solutions for ICS/SCADA networks are designed to reduce the risks of operational downtime, product manipulation, proprietary data theft and ransomware attacks. The solutions provide detection of cyber-attacks, visibility and risk management tools.

Technology & Products

The SCADAfence Continuous Network Monitor (CNM) solution allows administrators to significantly increase their network's security level, while ensuring the peace-of-mind that no unnecessary risks are added to the operational environment (ICS/SCADA network). The solution is software-based and is available either as a virtual appliance or as a network appliance. The installation process requires no downtime to the operational network, and system algorithms are automatically configured without any input from the user. SCADAfence CNM offers full visibility of day-to-day operations and real-time detection of anomalous behavior, based on deviations from normal behavioral profiles. Once a deviation is detected, the user receives a real-time alert.

SecBI www.secbi.com

Threat Hunting

Company at a Glance

SecBI's Autonomous Investigation™ technology detects all affected entities in compromised networks, using unsupervised machine learning to analyze network security log data for unknown incidents. With no appliances or agents, SecBI is easily deployed, delivering immediate results and shorten response times to allow organizations to adhere to strict notification deadlines.

Technology & Products

SecBI is an advanced threat detection software solution that ingests log data from network security gateways, and applies unique clustering and detection algorithms to detect threats that other vendors miss. Because SecBI's machine learning technology analyzes every piece of incoming and outgoing log data, it is able to cluster related forensic evidence into a single incident and provide a full narrative of the attack, including all users, devices, communication patterns, and more. This process eliminates fragmentation, investigation fatigue, and excessive searching.

SECDO

Secdo **www.secdo.com**

Incident management - SIEM /SOC | Forensic and Analytics | Incident Response

Company at a Glance

Secdo is the first preemptive incident response solution, slashing IR time to minutes. Gain unmatched historical thread-level endpoint visibility, automatically investigate and validate any alert and visualize the forensic timeline and attack chain back to the root cause. Then, rapidly and surgically respond and remediate on any endpoint without impacting business productivity.

Technology & Products

1) Secdo's Observer: Continuous thread-level endpoint data collection: Secdo captures and records in real time all events and behaviors on every host down to the thread level. 2) Secdo's Analyzer: automatic investigation and validation of any alert: Alerts from any source are automatically ingested into Secdo and analyzed, instantly revealing the complete context of the alert, including a visual timeline of the attack chain back to the root cause, damage assessment and more. 3) Secdo's Responder: Powerful, granular and surgical real-time response & remediation tools: Secdo provides a set of response tools that enable remote containment and remediation of actual threats on any host.

Secure-ly Ltd **www.secure-ly.com**

Data protection | encryption and recovery | Incident management - SIEM /SOC | Risk and Compliance (GRC)

Company at a Glance

Secure-ly, is focused on helping organizations to reduce the risk of service outage due to invalid or expired certificates. As well as to maintain continuous compliance with PKI security policies and best practices. We also provide PKI audit services and designing public key infrastructures.

Technology & Products

C-View is centralized agentless solution supporting all versions of Microsoft CAs. C-View scans networks and collects SSL certificates from any operating system. Enables enterprise to meet security policy compliance and best practices. C-View is using RBAC (Role Base Access Control) model Securely regularly releases new versions of C-View, reflecting a variety of enterprise-level needs and requirements, as well as new ideas and progress in the PKI industry. C-View installation and operation is very intuitive therefore easy to implement.C-view technology is based on Microsoft .NET, supporting all main browsers. Comprise of windows services and ASP.NET portal.

SIXGILL
Your Eyes in the Dark Web

Sixgill www.cybersixgill.com

Data protection | encryption and recovery | Intelligence | Incident management - SIEM /SOC | Forensic and Analytics

Company at a Glance

Sixgill is a cyber threat intelligence company that covertly and automatically analyzes Dark Web activity helping to detect and prevent cyber-attacks and sensitive data leaks before they occur. Utilizing advanced algorithms, Sixgill's cyber intelligence platform provides organizations with continuous monitoring, prioritized real time alerts and actionable intelligence.

Technology & Products

Sixgill's DARK-i is a cyber intelligence platform that analyzes Dark Web activity undetectably and autonomously. The platform has the ability to detect cyber attacks and sensitive data leaks originating from the Dark Web, and eliminate them before they occur. Our platform also provides clients with this information through prioritized real-time alerts. DARK-i creates profiles of Dark Web malicious actors mapping their hidden social networks and their behavior patterns, to analyze their activity. Through autonomous monitoring of closed, open, and hybrid dark web forums, we mine and analyze big data which allows us to identify potential criminals and terrorists with accuracy and depth.

This publication is for informational purposes only. While every effort has been made to ensure that the presented information is correct, The Israel Export & International Cooperation Institute assumes no responsibility for damages, financial or otherwise, caused by the information herein.

Production: IEICI Media & Communication Division.
Design: Ayala Eylath