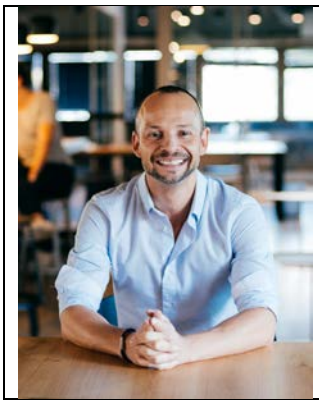

Gregor Schlosser
Auslandsbeauftragter und Technologiescout für die LEG Thüringen in Israel

Sharbat House, 9. Stock
4 Kaufmann Street, Tel Aviv

Email: gs@ahkisrael.co.il
Tel: +972-6-680 6800

Der Auslandsbeauftragte in Israel fungiert als Technologiescout für die Branchen Optik, Life Sciences und IKT, darunter Cybersecurity und Big Data. Er beobachtet die vielfältige und hochentwickelte Startup-Szene Israels und bringt interessierte thüringische Unternehmen mit israelischen Startups zusammen. So profitieren die deutschen Firmen von der enormen Innovationskraft der Startups, inbesondere in den genannten Bereichen.

Außerdem unterstützt der Auslandsbeauftragte thüringische Unternehmen dabei

- Geschäftspartner in Israel zu finden,
- Kontakte zu wirtschaftspolitischen Entscheidungsträgern, Verbänden und Institutionen auszubauen und zu pflegen,
- Sondierungsgespräche und Verhandlungen vorzubereiten,
- Informationen zu beschaffen,
- vor Ort Unternehmensbesuche, Messeauftritte oder sonstige Termine durchzuführen.

Egal ob Sie von Thüringen aus oder vor Ort in Israel Kontakte knüpfen wollen, der Technologiescout findet für Sie den passenden Partner.

Cybersecurity-Lösungen aus Israel für thüringische KMU

In Zeiten allumfassender Digitalisierung steigt die Anfälligkeit für Cyber-Angriffe immens. Ende 2016 erlitt YAHOO durch eine drei Jahre alte Sicherheitslücke den bisher weltweit verheerendsten Hackerangriff, in dem mehr als eine Milliarde Nutzerdaten entwendet wurden. 2015 führte ein Hackerangriff in der Ukraine zu einem Stromausfall und im Februar 2016 wurden in Bangladesch bei einem Hackerangriff auf die Federal Reserve Bank in New York 80 Millionen US-Dollar entwendet. Und wenn selbst das IT-Netz des Deutschen Bundestages nicht vor Cyberangriffen sicher ist, wie soll dann ein mittelgroßes oder kleines Unternehmen aus Thüringen seine Daten schützen oder Zahlungen sicher abwickeln? Und die Gefahr ist real: 2.267 Fälle von Computerkriminalität wurden in Thüringen 2014 erfasst, ein Drittel mehr als in 2010. Die Dunkelziffer liegt deutlich höher. Eine der Hauptgefahrenquellen für Büronetze und Datenbanken (z.B. von Kundeninformationen) geht dabei von Schadsoftware aus, die durch mobile Endgeräte, Wechseldatenträger und externe Hardware übertragen wird. Auch menschliches Fehlverhalten, digitale Sabotage oder der Einbruch über Fernwartungszugänge stellen Unternehmen zunehmend vor große Herausforderungen beim Schutz der eigenen IT-Infrakstruktur.

Wie diese Herausforderungen für KMU gemeistert werden können, zeigt sich bei einem Blick nach Israel. Das kleine Land am Meer ist ein Riese bei der Abwehr von Cyberangriffen und anderen Gefahren für IT-Infrastruktur. Dies spiegelt sich unter anderem in der hohen Zahl der Neugründungen im Bereich Cybersecurity – waren Anfang 2015 noch 187 Firmen auf den Bereich der Cybersecurity spezialisiert, wurden Ende 2016 bereits 365 Firmen gezählt. Der Trend bildet sich auch in den steigenden Investitionen in Cybersecurity in Israel ab: mit Investitionen in Höhe von 582 Millionen US-Dollar im Jahr 2016 durch Venture Capital Fonds (ein Plus von neun Prozent zum Vorjahr) liegt Israel weltweit auf Rang zwei direkt hinter den USA. Und das Interesse an Cybersecurity Firmen scheint weiter zu steigen. So erwarten Vorhersagen bis 2021 einen Marktwert im Bereich Cybersecurity von 202,36 Milliarden US-Dollar. Experten gehen davon aus, dass der maximale Marktwert pro Jahr um 20 Milliarden US-Dollar zulegen wird.

Treibende Kraft hinter den Neugründungen im Bereich Cybersecurity ist in Israel die Armee (Israel Defense Forces – IDF) bzw. die Übertragung militärischer Anwendungen auf den zivilen Bereich. Israel sieht sich tagtäglich zahlreicher Cyber-Angriffe auf kritische Infrastruktur und Unternehmen ausgesetzt. In den Eliteeinheiten für Nachrichtentechnik der Armee (z.B. „8200“) werden daher High-End-Lösungen zu deren Abwehr entwickelt. Die jungen Rekrutinnen und Rekruten, die an diesen

Techniken ausgebildet werden, arbeiten nach Beendigung des obligatorischen Wehrdiensts unmittelbar an zivilen Anwendungen für ihr gewonnenes Wissen und tun sich als Gründer hervor. Diverse Unternehmen und Acceleratoren (z.B. Team8) sind direkt oder indirekt auf die Einheit „8200“ zurückzuführen.

Im Jahr 2016 haben neue Themenfelder an Bedeutung gewonnen, darunter der Bereich der Drohnensicherheit, der Cyber-Versicherungen, Gefährdungsanalysen sowie Risikomanagement und die Sicherheit im (industriellen) Internet der Dinge. Und im Bereich der Cybersecurity für vernetzte Fahrzeuge gewinnt Israel für immer mehr Autobauer an Bedeutung. Fast alle namhaften Hersteller unterhalten mittlerweile Forschungs- und Entwicklungszentren zwischen Mittelmeer und Jordan. Zuletzt gesellte sich Daimler im April 2017 hinzu.

Thüringische Unternehmen finden in Israel Cybersecurity-Lösungen für alle Bereiche. Im Bereich des E-Commerce werden diese außerdem durch diverse Secure Payment-Anbieter aus der vielfältigen FinTech-Szene Israels ergänzt.

Der Technologiescout für Thüringen an der Deutsch-Israelischen Industrie- und Handelskammer vermittelt Ihnen gern den passenden Partner für Ihre Bedürfnisse. Die nachfolgende Übersicht über wichtige Unternehmen, Inkubatoren und Investoren im Bereich der Cybersecurity in Israel soll dabei als erster Anhaltspunkt dienen.

Auflistung der wichtigsten Acceleratoren, Inkubatoren und Investoren:

Acceleratoren

8200 EISP - Ein Accelerator für Absolventen der Militäreinheit 8200 (Nachrichtentechnik, Cyber).
Link: http://www.eisp.org.il/en/home
Upwest Labs - Unterstützt israelische Startups beim Start im Silicon Valley.
Link: http://upwestlabs.com/
Microsoft – betreiben ihren eigenen Accelerator in Herzliya bei Tel Aviv.
Link: https://www.microsoftaccelerator.com/locations/telaviv
Team8 - VC und Accelerator, der von ehemaligen führenden IDF Cybersecurity-Persönlichkeiten geführt wird. Link: http://www.team8.vc/

Inkubatoren

Die folgenden Einrichtungen sind von der Israeli Innovation Authority lizensierte Inkubatoren im Bereich Cybersecurity:

JVP Cyber Labs - Spezialisiert auf Cybersecurity Startups mit Sitz in Beer Sheva.
Link: http://www.jvpvc.com/cyberlabs
Incubit - Inkubator von Elbit Systems, Israels wichtigstem zivilen Unternehmen für Sicherheitstechnologie. Link: http://incubitventures.com/

Investoren und Venture Capital Fonds (VCs)

Viele der Inkubatoren treten auch als Investoren auf. Zusätzlich zu den oben aufgelisteten sind wichtig:

YL Ventures - Venture Capital Fonds (VC) von Yoav Leitersdorf. Er investiert in early-stage Cybersecurity Startups. Link: https://www.ylventures.com/
Jerusalem Venture Capital (JVP) – VC mit thematisch breitem Portfolio, darunter viele Cyber-security Startups. Link: http://www.jvpvc.com/
Glilot Capital – VC mit Fokus auf Cybersecurity-Lösungen. Link: http://glilotcapital.com/

Wichtige Persönlichkeiten und Investoren

Shlomo Kremer - Top Investor, Palo Alto Networks, Cato Networks
Gil Shwed - Checkpoint
Miki Bodai - Aorato, Trusteer, Imperva
Nadav Tzafrir - Ehemaliger Kommandeur der wichtigen Cybersecurity-Einheit 8200 der israelischen Armee, Team8-Gründer
Yuval Elovici - Direktor der Deutsche Telekom Innovation Laboratories an der Ben-Gurion-Universität des Negev (BGU), Leiter des BGU Cybersecurity Research Centers. Seine Schwerpunkte: Cybersecurity (für Smartphone-Sicherheit, Malware-Erkennung, APT-Erkennung, Absichern von IoT, etc.), Big Data Security Analytics (Nutzeranalysen, forensische Analyse, fortschrittliche Maschinen zur Erkennung von Cyber-Angriffen, Insidererkennung, etc.).

Wichtige Zentren

Tel Aviv und Herzliya

Tel Aviv ist der Nabel der Startup-Szene Israels und hier findet man auch die größte Konzentration von Cybersecurity-Firmen in Israel.

Beer Sheva

Beer Sheva liegt im Süden des Landes in der Wüste Negev und wird von der Regierung als „Hauptstadt des Südens“, akademisches Zentrum und Cybercity gefördert. Hier ansässig ist die Ben-Gurion-Universität mit einem starken Fokus auf Cybersecurity. Außerdem verlegt die israelische Regierung derzeit verschiedene Einheiten des Militärs in die Stadt, darunter die Eliteeinheit zu Cyber Security „8200“. Außerdem im Aufbau befindet sich der Nation Cyber Tech Park, ein Gewerbepark mit Fokus auf Cybersecurity, in dem bereits Unternehmen wie die Deutsche Telekom, Lockheed Martin, IBM und 20 weitere Cybersecurity-Firmen angesiedelt sind.

Jerusalem

In Jerusalem befindet sich das SIT – ein Research Center der Hebrew University Jerusalem und des Fraunhofer Instituts zum Thema Informationssicherheit.

Firmenprofile

Die nachfolgenden Unternehmen bieten für thüringische Unternehmen relevante Produkte und Services an.

Fokus Cybersecurity im Allgemeinen

CyberBit

https://www.cyberbit.net

Kontakt:

Tel: +49-89-215416-22 (Deutschland)
Oder
Tel: +972.(0)9.779.9800 (Israel)

info@cyberbit.net

Cyberbit betreut **Unternehmen** und **kritische Infrastrukturen** um sie vor fortgeschrittenen Cyberthreats abzuschirmen. Die im Militär erprobten Cybersecurity-Lösungen des Unternehmens erkennen, analysieren und reagieren auf die fortschrittlichsten und komplexesten Bedrohungen. Cyberbit beschäftigt ein vielfältiges Team aus dem öffentlichen und privaten Sektor, einschließlich PhDs, Hacker, ehemalige CISOs und SOC-Manager sowie erfahrene Veteranen der Intelligenz- und Militärgemeinschaft des israelischen Militärs. Mit Niederlassungen in Texas und Israel ist Cyberbit eine Tochtergesellschaft von Elbit Systems Ltd. (NASDAQ: ESLT) und hat über 500 Mitarbeiter in den USA, Europa und Asien. Zu Cyberbits Spezialgebieten zählen Endpoint Protection, SCADA Security, Security Operations Center, Sicherheitstraining und Simulation sowie kritische Infrastruktursicherheit.

Sitz: Ra'anana, Israel sowie München, Austin, Singapur und London.

Cyberbit hat ein Büro in Deutschland:
Mies-van-der-Rohe-Str. 8; 80807 München

CyberArk

https://www.cyberark.com/

Kontakt:

Tel: +972-3-918 0000
info@cyberark.com

CyberArk entwickelt Technologien, um **Unternehmen gegen Cyber-Angriffe von Insidern** zu schützen und zu verhindern, dass Angriffe irreparable Schäden hinterlassen. Die Sicherheitslösungen von CyberArk entsprechen der Einhaltung von Compliance- und Auditanforderungen, während die Unternehmen so ihre Vermögenswerte schützen können.

Sitz: Petach Tikva, Israel und Deutschland, USA, Spanien, Singapur, Australien und Frankreich sowie Italien und die Niederlande.

Illusive Networks

http://illusivenetworks.com/

Kontakt:

info@illusivenetworks.com

Illusive Networks bieten mit ihrem Produkt “Deceptions Everywhere” eine Cyberdefense-Lösung, die APTs und gezielte Angriffe neutralisiert, indem sie dem Angreifer scheinbar relevante, jedoch gefälschte Informationen vortäuscht. Die Technologie von Illusive ermöglicht es Unternehmen Sicherheitsschwachpunkte sichtbar zu machen, Angriffer in die Irre zu führen und Angriffe in Echtzeit zu unterbinden. Auch hochentwickelte Ransomware kann aufgespürt und geblockt werden, bevor Schaden angerichtet wird.

Sitz: Tel Aviv und New York

Fokus E-Commerce und Ad-Tec-Security

Protected Media

http://www.protected.media/

Kontakt:
Frau Lianne Trantz (Marketing)
+972 50 272 7929
Oder +972 206 337 8363

Protected Media wurde 2014 gegründet und ist spezialsiert auf **Betrugsschutz im Bereich der Werbung.** Das Unternehmen bietet eine Cyber-Security-Lösung für die Bekämpfung von online Werbebetrug durch die Installation verschiedener Schutzschilde für unterschiedlichste Anzeigenarten an. Das Angebot gilt sowohl für Display- als auch für Handy- und Video-Werbung und sichert die Sichtbarkeit durch „echte“ Menschen. Das Unternehmen nutzt einen Lösungsansatz für eine Vielzahl an Bedrohungen wie beispielsweise nicht personengebundene Nutzer, Anzeigensichtbarkeit und Markenschutz.

Sitz: Tel Aviv

Namogoo

https://www.namogoo.com/

Kontakt:

info@namogoo.com

Gegründet im Jahr 2014 bietet die Firma eine Software an, die das unfreiwillige Öffnen neuer Browserfenster beim Besuch einer Website verhindert. Die Server des Unternehmens scannen Homepages und schaffen ein **Hinderniss für „male ware“**, die zum **Öffnen unerlaubter Zusatzprogramme (Widges)** führen könnten, die vom Website-Manager nicht intendiert sind.

Spezialgebiete von namgoo sind Cybersecurity, eCommerce, Intelligence, Big Data Analytics, Fraud, Client-Side Injections, Machine Learning, Deep Behavioral Analytics und Client-Side Malware.

Sitz: Ra‘anana, Israel und Singapur, San Francisco und London

Cabara Software

Das Unternehmen verhindert **online Wilderei (e-poaching)** - den unbefugten Zutritt auf Websites, das unerlaubte Einfügen von Inhalten sowie das Stehlen von Daten im digitalen Verkehr durch Hacker. Damit hilft Cabara-Software beim Vorbeugen des Verlusts der Markenintegrität durch Anzeigen, die vor einem „Vandalismus“ auf der Webseite warnen. So können Verluste im Informationsverkehr, der enthaltenen Daten sowie des Umsatzes verhindert werden.

Spezialgebiete von Cabara sind Security, Brand protection, Ad Injection Removal, Affiliate Scam Detection und das Verhindern von ePoaching

Sitz: Tel Aviv

http://www.cabarasoftware.com/

Kontakt:

contact@cabarasoftware.com

Forter

Forter stellt eine neue Generation von Betrugsprävention bereit, um die Herausforderungen des modernen E-Commerce zu erfüllen. Forter bietet vollautomatisierte, **Echtzeit-Decision Betrugsprävention**. Durch ihr spezielles Prinzip wird eine 100% **Chargeback-Garantie** erzielt. Das System macht Regeln oder manuelle Bewertungen überflüssig, so dass Betrug reibungsfrei verhindert werden kann.

Das Ergebnis ist eine Betrugsprävention, die für die Käufer unsichtbar ist und u.a. einen einfacheren Checkout sichert.

Hinter den Kulissen kombiniert Forters maschinelle Lerntechnologie fortschrittliche Cyber-Intelligenz mit Verhaltens- und Identitätsanalysen, um einen mehrschichtigen Betrugserkennungsmechanismus zu schaffen.

Sitz: Tel Aviv und San Francisco

https://www.forter.com

Kontakt:

1-800-537-0601
sales@forter.com

Riskified

Riskified ist eine All-in-One-Lösung für die **Betrugsvermeidung im eCommerce.** Riskified bietet einen 100%igen Rückvergütungsschutz auf jede Bestellung, die sie genehmigen.

Riskified ist der weltweit führende Anbieter von Betrugsprävention im eCommerce-Bereich, dem viele globale Marken vertrauen (Referenzen u.a. Paypal und Billguard). Riskified nutzt fortschrittliche eCommerce-Betrugserkennungsmethoden, um Händler vor Betrug zu schützen, indem sie nicht vorhandene Karten-Transaktionen (CNP) mit maschinellen Lernalgorithmen, Verhaltensanalysen und Geräte-Fingerprinting genau analysieren.

Spezialgebiete von Riskified sind u.a. Risk Enablement, Betrug, E-Commerce, Maschinelles Lernen, Chargeback-Garantie, E-Commerce-Betrugsverhinderung.

Sitz: Tel Aviv und New York

https://www.riskified.com

Kontakt:

support@riskified.com

Fokus Industrie

Fireglass

https://fire.glass

Kontakt:
+972-3-5188877

Fireglass bietet Firmen Netzwerk-Security Lösungen für Firmen durch **Webisolation** an. Dazu nutzen sie Cybersecurity-Ansätze, um die **Sicherheit des Unternehmensnetzwerks** zu verbessern **(Malware Prevention)**, ohne die Nutzererfahrung oder Produktivität zu beeinträchtigen. Die Threat-Isolation-Plattform eliminiert Webangriffe und schränkt alle potentiell schädlichen Inhalte auf eine sichere Ausführungsumgebung ein.

Fireglass-Lösungen können vor Ort eingesetzt oder als Cloud-Service genutzt werden. Die Threat-Isolation-Platform benötigt keine Endpunktinstallation und unterstützt alle Browser, Betriebssysteme und Geräte. Es ist für Organisationen aller Größen skalierbar und kann in wenigen Minuten aktiviert werden.

Sitz: Tel Aviv, New York, und London

Claroty (ehemals Team 82)

https://www.claroty.com

Kontakt:
+972-73-3318088
contact@claroty.com

Claroty ermöglicht Ingenieuren, Betreibern und Cybersecurity-Profis den Schutz und die Optimierung auch komplexester OT-Netzwerke mittels einer ganzheitlichen Cybersecurity-Plattform.

Sitz: Tel Aviv und New York

CyberX

https://cyberx-labs.com/en/home

Kontakt:
+1.657.229.2370
info@cyberx-labs.com

CyberX ist ein Anbieter industrieller Cybersicherheitslösungen. CyberX hat den Weg in die Sicherheit des industriellen Internets maßgeblich bereitet – durch die Bereitstellung von Erkennungsmethoden und tiefen Einblicken in die operativen Netzwerke. Unter Verwendung praxiserprobter Technologien und anerkannter Forschung bietet CyberX **umfassenden Schutz für Dutzende große Industrieanlagen** in den Bereichen Fertigung, Öl und Gas, Wasseraufbereitung und Energie auf der ganzen Welt.

CyberX bringt eine neue und leistungsfähige Sicherheitsstrategie in Industrieumgebungen. CyberX erkennt Cyberbedrohungen, Systemmanipulation und Betriebsstörungen in Echtzeit. Durch die aktive Bedrohungsintelligenz für die Industrie, umfangreiche Forschung und viele Installationen erkennt CyberX Zero-Day Schwachstellen in Industrieanlagen und gewährleistet beispiellosen Schutz für Operationen im Bereich „Industrial Internet of Things“ (IIoT).

Die Hompeage des Unternehmens ist auch auf Deutsch abrufbar.

Sitz: Herzliya, Israel und Framingham, USA

Waterfall Security Solutions Ltd

http://www.waterfall-security.com

Kontakt:
ran@waterfall-security.com
France: +(33) 1 46 14 87 28

Die Technologie von Waterfall Security stellt eine **Alternative zu Firewalls** dar. Die innovativen, patentierten Unidirectional Security Gateway-Lösungen ermöglichen eine sichere und zuverlässige IT / OT-Integration, Datenfreigabe, Cloud-Services und alle erforderlichen Verbindungen für industrielle Steuerungssysteme und kritische Infrastrukturen. Die Produkte von Waterfall Security reduzieren die Kosten und die Komplexität der regulatorischen Einhaltung von NERC CIP, NRC, NIST, CFATS, ANSSI und anderen drastisch.

Die Produkte von Waterfall ermöglichen Drittanbietern, HQs, Ingenieuren, Auftragnehmern und Anbietern, Cloud-Services und anderen Unternehmen, Zugang zu Betriebsinformationen zu erhalten und gleichzeitig die industriellen Steuerungssysteme sicher zu halten.

In Kraftwerken, Atomkraftwerken, an Offshore-Plattformen, Raffinerien, Produktionsanlagen und Versorgungsunternehmen weltweit findet Waterfall bereits Anwendung.

Sitz: Rosh HaAyin, Israel und Nordamerika sowie Frankreich

Firmitas Cyber Solutions Ltd

http://www.firmitas-cs.com

Kontakt:
success@firmitas-cs.com

Firmitas Cyber Solutions ist ein Technologieunternehmen, **das Cybersecurity-lösungen für Mission-Critical Connected Systems** anbietet.

Die Cyberdefense-Lösungen des Unternehmens verbessern die Effizienz und verringern Risiken, sichern die Kommunikation und schützen vor zahlreichen Cyber-Attacken. Firmitas-Lösungen eignen sich für den Einsatz im Industrie-, Finanz- und Transportbereich sowie anderen Sektoren und können sowohl auf bestehende als auch auf neue Systeme angewendet werden.

Sitz: Kfar Saba, Israel

Nextnine

https://nextnine.com/

Kontakt:
+972 3 767 3000
oder +972 3 649 7810

Nextnine ist ein führender Anbieter **von Top-Down-OT-Sicherheitsmanagementlösungen für komplexe ICS-Umgebungen** mit mehreren Anbietern. Das ICS Shield von Nextnine ist eine bewährte Lösung für den Schutz von Multi-Site-Remote-Field-Assets aus einem einzigen Sicherheits- und Operations-Center. Mit dem Einsatz von ICS Shield automatisieren Industrieunternehmen die Implementierung und Durchsetzung von Richtlinien, die die Sicherheitskontrolle und interne Compliance verbessern und gleichzeitig OT- und IT-Ressourcen sparen.

Nextnine-Lösungen wurden von Systemintegratoren (SIs), Managed Security Service Providern (MSSPs) und den größten Automatisierungsanbietern bei Tausenden von Industrieanlagen weltweit eingesetzt. Im Bereich der Öl- und Gasindustrie, der Versorgungs-, Chemie-, Bergbau- und Fertigungsindustrie bietet Nextnine Sichtbarkeit, Zuverlässigkeit und Compliance für angeschlossene industrielle Betriebe.

Sitz: Petah Tikva, Israel und New York

Indegy

http://www.indegy.com

Kontakt:
+972 (3) 550-1783

Indegy bietet Situationsbewusstsein und **Echtzeit-Sicherheit für industrielle Steuerungsnetze**. Die Indegy Plattform ermöglicht ICS-Ingenieuren und Sicherheitspersonal ICS-Netzwerke zu sichern, anhand der Abbildung aller aktiven Controller im Netzwerk, deren Konfiguration, der Protokollierung aller Aktivitäten und des Austauschs sowie der Möglichkeit in-depth alle Aktivitäten zu verfolgen. Durch die Echtzeit-Beobachtung und ein hohes Situationsbewusstsein sowie effektives Change Management können nicht-autorisierte Aktivitäten verhindert werden.

Sitz: Tel Aviv und New York

SCADAfence

https://www.scadafence.com/

Kontakt:

Beer Sheva Office
+972 73 260 1964
Email: info@scadafence.com

Tel-Aviv Office
Phone: +972-73-260-1964
Email: info@scadafence.com

SCADAfence bietet **Cyber-Security-Lösungen an, die die operative Kontinuität industrieller Netzwerke (ICS / SCADA) gewährleisten**. Ihre Kompetenz liegt in intelligenten Fertigungsbereichen, die **Industrial IoT / Industry 4.0** Technologien anwenden, wie Pharma, Chemie, Lebensmittel und Automotive.

Die passive Lösung von SCADAfence ist darauf ausgerichtet, operationelle Risiken wie **Ausfallzeiten, Prozessmanipulationen und Diebstahl** von sensiblen herstellergebundenen Informationen zu reduzieren. Das Unternehmen bietet eine umfassende Lösung, die eine kontinuierliche Echtzeitüberwachung der industriellen Umgebung sowie leichte Tools zur Automatisierung des Prozesses der Sicherheitsbewertung umfasst. Die Lösungen beinhalten die Erkennung von Cyber-Attacken und Forensik-Tools zur Verbesserung der Reaktionsfähigkeit.

SCADAfence sitzt im israelischen Cybersecurity Center of Excellence in Beer Sheva.

Nation-E

http://www.nation-e.com/

Kontakt:
+1 646 8512 623
contact@nation-e.com

Nation-E bietet **Cyber-Schutz für kritische Infrastrukturen und das industrielle Internet der Dinge (IIoT)** an. Im Fokus stehen innovative Sicherheitslösungen für Industrieanlagen, kritische Infrastrukturen und intelligente Netze.

Die Services und Produkte von Nation-E wurden entwickelt, um maximalen **Schutz für OT** zu bieten, wo die meisten Assets über serielle Schnittstellen verbunden sind. Die Plattform kombiniert **Cyber-Sicherheit, Risiko-management sowie Big-Data-Analytik** und ermöglicht die vollständige Kontrolle der bisher ungeschützten Infrastruktur.

Sitz: Herzliya, Israel, Silicon Valley und New York

Fokus Internet der Dinge

SecuriThings Ltd

http://securithings.com/

Kontakt:

+1 650 704 7916

SecuriThings bietet eine **IoT-Sicherheitsplattform**, die sich leicht mit allen Cloud-verbundenen Geräten und Systemen zum **Schutz vor unbefugtem Zugriff** integrieren lässt. Die SecuriThings-Lösung analysiert IoT-Aktivitäten in **Echtzeit** und bietet Herstellern und Dienstleistern eine ganzheitliche Sicht auf Bedrohungen, über Nutzer und Geräte. Die Plattform kombiniert Daten von Mensch und Gerät mit Threat-Intelligence-Berichten und anderen Sicherheitsdaten sowie mit Verhaltensanalysen, um Angriffe zu erkennen und zu mildern. **SecuriThings-Technologie hilft Smart Homes, Smart Buildings, Smart Cities und Industrial IoT zu sichern.**

Sitz: Tel Aviv

Dojo-Labs

http://www.dojo-labs.com/

Kontakt:
info@dojo-labs.com

Dojo-Labs bietet **Verbrauchersicherheits- und Datenschutzlösungen für IoT-Geräte in intelligenten Häusern**. Der Service wird über das Dojo-Labs-Gerät, das sog. Dojo und einen Cloud-basierten Service mit einem Consumer-Portal und mobilen Apps bereitgestellt. Dojo-Labs Service kann in jedem „smart-house“ genutzt werden.

Sitz: Herzliya, Israel und Palo Alto, USA

Fokus Vernetzte Fahrzeuge

Argus

https://argus-sec.com/

Kontakt:
iemea@argus-sec.com

Argus Cyber Security bietet umfangreiche Sicherheitslösungen für vernetzte Fahrzeuge. Die sofort einsatzbereiten Produkte schützen gegen bösartige Eindringlinge, die die Datensicherheit oder elektronische Kontroll-komponenten angreifen könnten. Argus hilft Fahrzeugherstellern, vernetzte Fahrzeuge anzubieten, ohne Kompromisse bei Datenschutz und Datensicherheit eingehen zu müssen.

Sitz: Tel Aviv