Control your Attack Surface

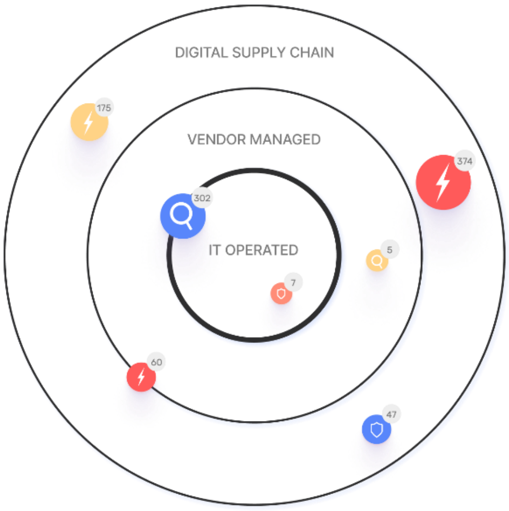
LS INTERNATIONAL SA

It's a Swiss-based Company with an international vision and a complete offering on different technological areas: networking, network security, cyber security, performance monitoring, homeland security and collaboration. The mission is to support customers in digital transformation and offering assessment, design, implementation and support services for technologically advanced IT solutions

IONIX

is an Israeli Company that operates in the world of Cyber Security. Developed a SAAS solution for managing cyber risks of organizations' supply chains. Headquartered in Tel Aviv, it helps businesses around the world minimize attack risks and vulnerability exposures through advanced Attack Surface Management (ASM) features.

Contact us:
for more info and to organize a **FREE DEMO** **tailor-made** for your Company.



With the introduction of the nLPD (01/09/2023), companies have to pay increasingly more attention to their IT security level.
In addition to Vulnerability Assessment and Penetration Test services, it becomes essential to have tools and services that allow you to better know and understand your attack surface and prevent any critical exposures.
IONIX is among our main technology partners for the management of our Customers' Digital Supply Chain.

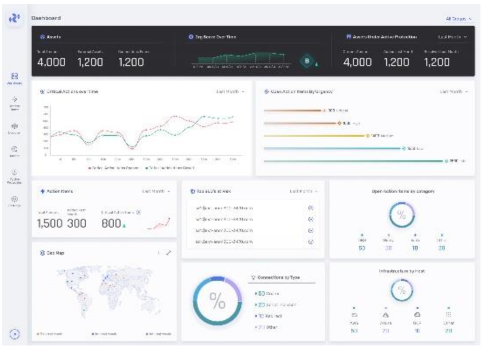
With the ASM (Attack Surface Management) solution we help organizations to take control of their real attack surface, before any vulnerabilities due to third parties interconnected with customers can be exploited by cyber criminals.

The solution is completely AAS, therefore it can be activated very quickly, it offers a very intuitive, easy and complete platform with an extremely deep analysis.

For this reason IONIX won the **CyberSecurity Excellence Award 2023** and the **Globee® Award 2024 – Attack Surface Management Category.**

Using patented "Connective Intelligence" technology, IONIX offers a complete solution that includes the following features.

- **Discovery** – complete visibility not only on all its assets exposed to the outside, but also on the Digital Supply Chain which represent potential attack vectors.
- **Assesment** - multi-level risk assessment classified into 13 categories (e.g. DNS, web application, PKI) – performed both for each asset and at the organization level (overall risk score).
- **Prioritation** - prioritization based on the importance of the asset to the business, ease of exploiting vulnerabilities and threat intelligence.
- **Remediation** - implementation of automatic Active Protection functions to neutralize entire categories of threats (IP, domain, cloud storage).



LS INTERNATIONAL SA | C.so San Gottardo 23 | 6830 CHIASSO
info@lsinternational.ch | +41 (0) 91 682 9019 | https://lsinternational.ch