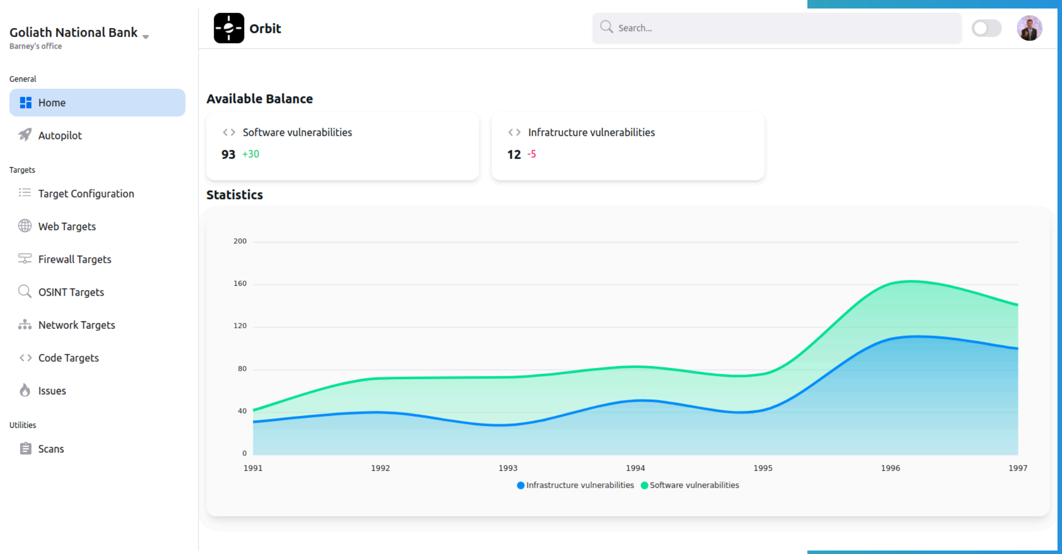
orbit

getorb.it

Orbit Cybersecurity Cloud Data Sheet



Next-gen Cybersecurity -

Find IT vulnerabilities before hackers will

Orbit scans on-premise and cloud IT infrastructure for cybersecurity attack vectors, offers actionable intelligence and measures for fixing them before they are exploited.

Key Use Cases

- Continuously scan your IT infrastructure (on-premise and cloud) for cybersecurity vulnerabilities
- Monitor SaaS applications for exposed files, endpoints or configuration errors
- Become alerted when stolen user credentials, configurations and user data appear on the Internet
- Manage cybersecurity issues centrally, enrich them with bleeding-edge information to gain insights, or to fix issues
- Enhance your own cybersecurity teams providing them fully automated vulnerability discovery, allowing them to conduct custom analyses

Features

Autonomous Discovery of IT Resources

Complex and dynamically changing IT infrastructures make it challenging to keep track of deployed servers, virtual machines,

Cyber Security is a Business Risk

As digital information technology is narrowly connected into day-to-day and strategic operations, cyberthreads have become not only a technology, but a business risk [1]. Cyberattacks are becoming more numerous, sophisticated, and more organized. With more services running in the cloud, Internet of Things connected to enterprise networks, and work from everywhere environments, more attack surface is exposed.

88% of company boards consider cybersecurity as a business risk [2].

containers and SaaS applications, let alone installing cybersecurity monitoring. Point Orbit to your environment and it will autonomously discover exposed systems and start monitoring them.

Reduce Noise, Enhance Signal

Orbit adaptively chooses the adequate tool to scan every of your attack surfaces. This reduces false-positives and brings more specific, relevant issues to light. Doubles and repeated data points are automatically squashed into one, enriched with contextual information and knowledge on how to fix vulnerabilities.

Integrated Issue Management

Traditionally, issues raised from a cybersecurity audit are collected in paper reports where they may be lost from track. Validation that the fixes have been applied correcly is missing. Orbit automatically opens issues from vulnerabilities, suggests a priorization, tracks the fixing process and rescans them for validation.

Human Quality, Machine Speed

Cybersecurity audits are still often performed by specialists, take several hours to days, are conducted infrequently and checks may be forgotten. In a World where hackers exploit vulnerabilities within hours - too quickly for the classical audit model. Orbit scans complete IT-infrastructures in the matter of minutes, up to several times a day, outpacing attackers.

Bleeding Edge Vulnerability Data

Orbit integrates several vulnerability databases and updates them continuosly. As soon as new vulnerabilities become available, Orbit is able to scan for them on your infrastructure, before others do.

Knowledge, not Information

Attacks, however clandestine, always leave traces. When examined individually, they may look insuspicious and stay under the radar. Similarly, Zero-day attacks are undocumented and render vulnerability databases useless. Orbit connects the dots and is able to detect advanced patterns from several sources to discover even those attacks.

Sources

[1]: Gartner, Inc: What Is Cybersecurity?, 2024

[2]: Gartner, Inc: Gartner 2023 Board of Directors Survey

[3]: Anderson, R.: Why information security is hard-an economic perspective

[4]: Schweizer Radio und Fernsehen: Verträge der Schweizer Luftwaffe im Darknet aufgetaucht

Level out the attack-defense asymmetry

For an attacker to find a vulnerability is easier than for the defender to secure a system. As the attacker can choose to exploit any vulnerability he finds, the defender does not know which vulnerability the attacker will chooses and has therefore to find any vulnerability present in the system guarantee security. This phenomenon is known as *attack-defense asymmetry*. Using already present, up-to-date vulnerability databases, information networks with other cybersecurity providers and automated scanning provides the muscle to level the playing ground in favor of the defender.

Outpace the Armaments Competition

With increasingly high-value targets and state state actors on the playing field, cybersecurity products need frequent updates and adaptation to maintain the same level of protection. Outdated IT systems quickly fall prey to attackers, interrupting day-to-day operations, stealing sensitive data, or exposing strategically important information.

The Federal Administration of Switzerland was hacked

3 times

within the last 6 months [4].