# Data Sheet
## Zion


### Abstract

Oxyde Technologies' offensive-cybersecurity-as-a-service, Zion, empowers the client to be ahead of the hackers by obtaining the right overview of how all their current systems, tools, network & infrastructure play together, whilst drastically improving team efficiency and operations, similar to a Breach & Attack methodology.

Hackers do not stop once they break into the corporate perimeter. For such, Zion will validate every level of production security, including all the existing software of the client's regular work-flow.

Zion gives awareness and remediation strategies with a zero likelihood of false positives, through continuous and automatic pen-testing attacks, culminating in simple, yet precise remediation strategies, fully integrated into the client's existing work-flow.


### FEATURES

1. Agentless
2. Serverless
3. Completely automatic
4. Scalable-by-design
5. Fully proprietary, no dependencies
6. Easily integrated into any other system
7. Blockchain-based database security

### BENEFITS

1. Faster vulnerability-remediation cycle
2. Drastically increased team efficiency
3. Understandable by non-cyber experts
4. Seamless integration with the client
5. Zero likelihood of false positives
6. Model a hacker's mindset 24/7

### AUTOMATIC CONTINUOUS MONITORING & SURVEILLANCE

This allows our clients to be always at the vanguard of any new or unexpected development in their networks, Zion's AI engine never sleeps, 24/7. Upon receiving feedback of an attack at a later stage, Zion creates a comprehensive, yet very detailed and sought-after histogram, showing our client how their network has evolved over time, and how effective the past and present security measures are.
Zion is also able to incorporate the client's existing security data from other defensive mechanisms, in order to simplify the end-user's work and remediation-strategy, letting Zion deal with all the information overhead.

### AUTOMATIC BREACH & ATTACK PEN-TEST

During the first phase of exploitation, Zion follows industry-gold-standards of corporate attacks, according to the MITRE ATT&CK knowledge-base, alongside Oxyde's own Red Team expertise and vision.
Secondly, throughout the post-exploitation phase, the software is able to move laterally within the given perimeter of the client, just like the spread of an organic virus. Zion's proprietary deep reinforcement learning algorithms mean a non-biased and unprecedented adaptability, utterly important in this field, given that no network shall always be the same, whilst harnessing the power of adaptation and creativity from this AI model.

### REPORTING

At this stage, Zion gives the client all the information needed to better understand, and visualise their overall security, through either a dashboard or fed onto the client's existing ticketing / management system (Jira, GLPi…).
To do so, Zion will manage, assess and prioritise the vulnerabilities, according to a risk-based score, whereby massively offering the client a unique overview of their entire network.

## BLOCKCHAIN-BASED INFORMATION FLOW & DATABASE

Trust. Empowerment. Adaptability.
Oxyde Technologies' core values are a reflection of how the heart of Zion ticks. We are currently market leaders and pioneers in the space of blockchain-based information flow and database design.
Our in-house built blockchain-based database architecture allows our clients to be truly in control of their data. If the client desires, it will never be accessible to anyone else, not even us, given the nature of this new technology. This opens an entire new horizon of possibilities in sectors where data regulation is very tight, such as financial institutions or governments, instead of the highly insecure cloud-based approaches that they already employ.
Furthermore, this also implies that, from the eyes of a malicious entity, Oxyde Technologies' data is as secure as the most secure Cryptocurrencies out there. No other information security institutions offers the same level of protection.

## Business cases

Zion's offering will tackle directly the main technology pillars that the industry heavily relies upon, including, but not limited to the assessment of the client's network-based and cloud-based security posture, culminating it the management, assessment and remediation of their vulnerabilities to exponentially empower and accelerate the remediation cycle.

Zion will particularly shine in large corporative networks (the higher the entropy of their network, the more information Zion will present), the ever-growing IoT sector (specifically in hospitals, smart houses and autonomous-connected vehicles), as well as companies that have recently suffered a M&A, which ultimately culminates in a new and extra technical and political layer of complexity.

Moreover, given Oxyde Technologies' truly secure and distributed infrastructure, we are able to offer to our clients real-time protection from attacks that are happening around the globe to other similar institutions.

Finally, Zion will consequently empower the client, making sure the solution integrates fully with their existing work-flow. Its 24/7 breach & attack validation will make a precedent to the clients efficiency, giving them the power to finally be ahead of the hackers and attackers with zero false positives, whilst keeping their data secure like no other cyber-player.

## INTEGRATION

Given that Zion empowers the client, it is able to fully integrate with their already existing platforms and tools, and hence providing a high-level perspective or their security infrastructure including their tools. To do such, Zion has two types of integration: inbound and outbound integration through proprietary APIs.
For the former, Zion can weaponise and integrate the client's existing IoCs (from other threat intelligence software), apart from its own, to design a more educated pen-test approach.
On the other hand, outbound integration allows for findings prioritisation and acting upon them, whereby Zion will integrate with other platforms (if the client prefers it that way, instead of the built-in one) to visualise all relevant data and relay its strategies onto the client's vulnerabilities' ticketing platform.

## MODEL HACKER'S MENTALITY & BEHAVIOUR

„It is not same same knowing the path, as walking the path" - Morpheus to Neo in Matrix.
Zion uses the same, if not more advanced tools than a professional hacker, and it is fully automated. Armed with the attackers mentality and behaviour, any IT-department (even if they are not cyber specialised) can securely close the security gaps fast, that would otherwise go unnoticed until it may be too late.

## INDUSTRY-GOLD-STANDARDS & METHODOLOGY

Zion follows a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. Together with Oxyde Technologies' in-house knowledge-base, the client's company will be secure against present and future attacks.