Mkit

Products & Services

THE COMPANY

Mkit was founded in 2008 in Buenos Aires, Argentina. We provide defensive and offensive security solutions, on-demand incident detection and response services, personalized strategy planning and execution, and high-end hands-on technical training.

After only 5 years after being founded, Mkit became a Top-5 ITSec company in Argentina, protecting companies and government agencies with their security strategy planning.

In 2015, Mkit consolidated its presence in Latin America and Europe (providing solutions to the regions from its offices in Argentina, Brazil, and Spain), and in 2017 it began its business expansion strategy into North America, incorporating new branches in Canada and the United States.

We hold a strong ethic behavior in our work. That is our commitment and what makes us preserve the trust from our clients, providers and friends.

The solutions we offer come with an added value related to human conduct and behavior, regardless of the understanding of how current technology works and changes constantly.

Our Team

Mkit was created based on the experience of a group of renowned security professionals, who during the development of their careers decided to team up to supply the significant consulting needs in the local market.

Our staff has dozens of years of experience in the ITSec field, having presented their research in conferences in Latin America, North America and Europe.

Back home, they actively assist government agencies and nonprofit organizations. They are also professors at universities, and frequently offer free seminars about computer security to the general public.

Each one of our specialists holds a unique set of skills in their area of expertise, and the combined group is constantly gaining significant knowledge and experience on each possible subject in the field, achieving a uniform and synergetic growth towards the entire team.

Our Values

- Trajectory: Our delivery quality has gained us the trust of our peers.
- Experience: Each of us has over 20 years walking the field.
- Quality: No detail is overlooked. No doubt is left uncleared.
- Flexibility: Every client is a universe. To each their own strategy.
- Transparency: We don’t hide our tricks from you. Step into our kitchen.
- Innovation: We never stop learning. For you, and for us.

SERVICES

VATE

Red Team Operations

A Red Team has the objective of evaluating the effectiveness of a security program. This is accomplished by the emulation of techniques and behaviours of a potential attacker, in the most realistic way possible.

Red Team Operations represents the assembly and execution of a strategic plan, involving the infiltration to the physical and computer infrastructure of the target organization, and to obtain and exfiltrate an object, piece of data or specific asset, in order to verify the effectiveness of the organization's preventive, detective, recuperative and resilience capacities.

You should hire a Red Team if you need to identify vulnerabilities in your infrastructure and systems, and test your security controls.

A Red Team allows a fresh set of eyes to take a look at your overall status.

Network Penetration Testing

General perimeter visibility

Service exposure

General patching status

Overall network protection level

Private structure disclosure

Denial of Service

Application Penetration Testing

Bypass of input field controls

Strength of the authentication process

Security in communications

Reverse engineering

Exploit development

App ecosystem testing

Difference between Red Team Operations and Penetration Testing, and the confusion in terminologies:

Red Team Operations involves the execution of different offensive tasks, including different areas (computer, physical, human) at the same time, presenting a single specific objective planned. Once the objective is reached, the operation concludes and the project finalizes.

Penetration Testing represents the massive and general search for vulnerabilities, with the final objective of identifying and verifying as many of them as possible, to test them and report them, thus establishing the general security level of the environment, application or specific group being analyzed.

A Red Team Operations execution generally **includes** the execution of Penetration Testing tasks, although it may not be limited to it.

Human Penetration Testing

Client-side attacks
Personalized spear phishing attacks
Exposure and online reputation
Masquerading & replay attacks
Simulation planning
Data leak

Physical Penetration Testing

Frequency and wave analysis
Access control bypass
Vulnerable transit points
Denial of Service
Alarm system testing
Hardware evaluation

Blue Team Operations

A Blue Team consists of a security group that strategically defends the organization against real attackers, or even Red Teams.

A Blue Team periodically analyses the effectiveness of the security policies and measurements taken by the organization, to ensure that all potential risks and threats are being revised, identified and mitigated.

The execution of Blue Team projects is done through Managed Security Services inside a macro project, with a bigger focus that covers both offensive and defensive techniques, inside a long term execution plan.

Blue Teams work from the inside out. They have access to all the necessary documentation and systems, and actively participate in management meetings to contribute ideas relating to the security strategy.

Application Security

Source code review (SAST)

Protection at runtime (DAST)

SDLC Involvement (DevSecOps)

Application ecosystem analysis

Reverse engineering

Exploit development

Managed Security Services

Planning and execution of company-wide projects, through defensive and offensive techniques:

Vulnerability assessments
Penetration Testing
Forensic analysis
Advice on market solutions
Assistance in the decision making
Training and Awareness

Purple Team

The Purple Team exists to ensure and maximize the effectiveness level of both Red and Blue Teams. This is accomplished through the integration of defensive and control tactics by the Blue Team, with the threats and vulnerabilities found by the Red Team, within a unique instance that guarantees that the efforts of both teams are being leveraged at the maximum.

In an ideal situation, it is the Red Team that creates the challenges for the Blue Team to solve. In doing so, both teams together are able to improve the organization's security level, and enhance the skills of all the people involved in the project.

Through the implementation of a Purple Team solution, a strong synergy is accomplished, that delivers an added value to the end result.

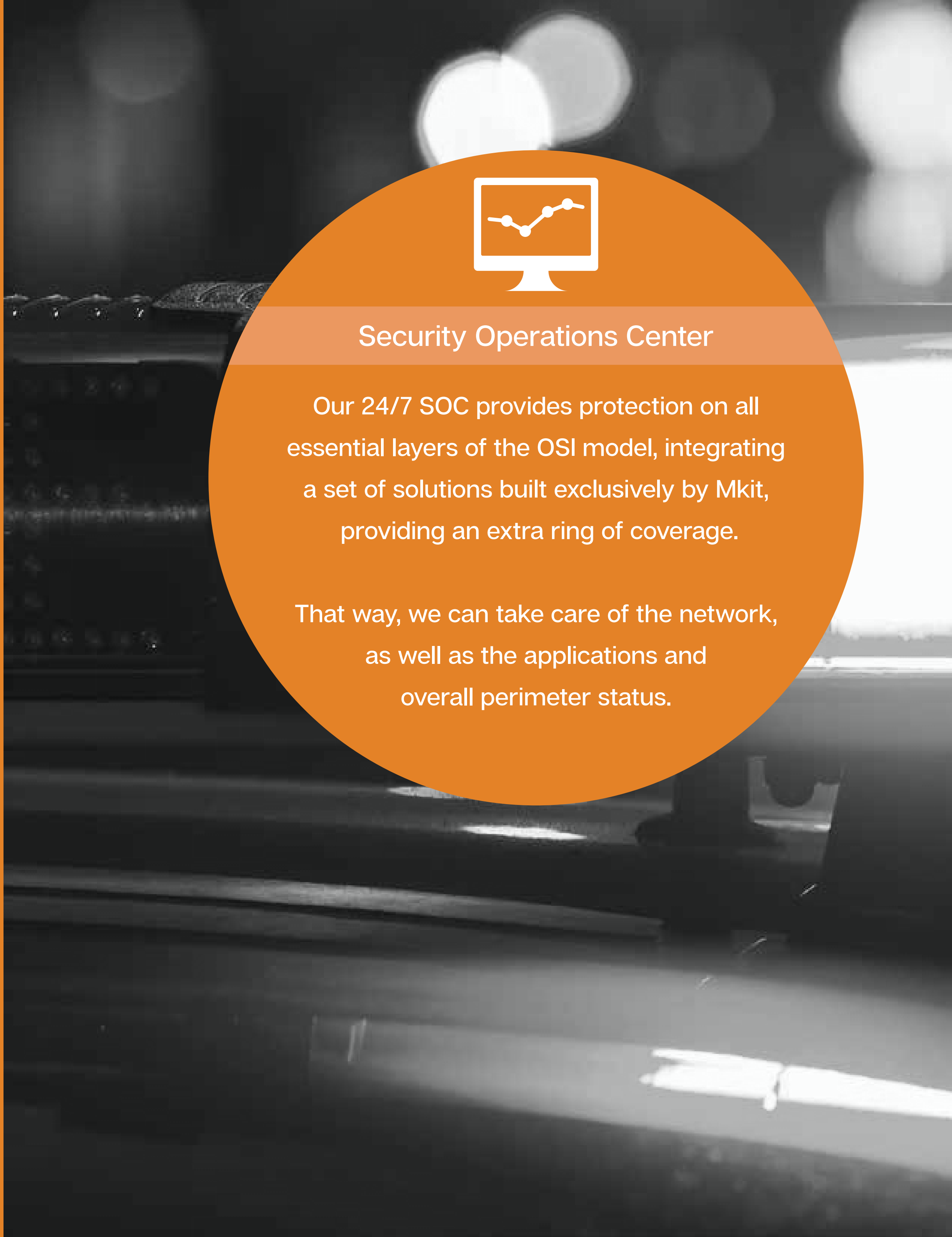
Sentinel Detection

Stay sharp. Protect your organization by keeping an eye on the activity surrounding it, both inside and outside the premises.

Right between defense and offense, lies observation. No security plan can be properly executed without including strong detection procedures.

The correct combination of monitoring solutions can prepare your organization for any type of attack, whether it is to prevent them from happening, or to ensure that your organization has the tools to face a potential incident and resolve it in the simplest and quickest way possible.

A solid surveillance strategy is crucial. Sometimes, the smallest risk can become the biggest threat, because of a failing monitoring solution. Gain control of the situation by staying ahead of the problem.



Security Operations Center

Our 24/7 SOC provides protection on all essential layers of the OSI model, integrating a set of solutions built exclusively by Mkit, providing an extra ring of coverage.

That way, we can take care of the network, as well as the applications and overall perimeter status.

CSIRT

Mkit currently runs one of the few private CSIRTs with global reach, joining professionals of diverse disciplines and developing computer incident response procedures, that mitigate their damage towards acceptable levels.

We hold alliances with several FIRST teams, building our Constituency towards both private and public entities.

Threat Intelligence

The Threat Intelligence service consists of a continuous analysis of the organization’s digital ecosystem in multiple scenarios for information exchange, allowing thus the anticipation of an incident that may negatively affect its reputation, and assisting in any potential investigation:

Detection of brand and logo usage in attacks

Vulnerability and incident databases

Public sources of information

Social networks

Search engines

PRODUCTS

DO OR DO NOT.
THERE IS NO TRY.
- YODA

Ctrl
Del
Alt

Network Threat Discovery

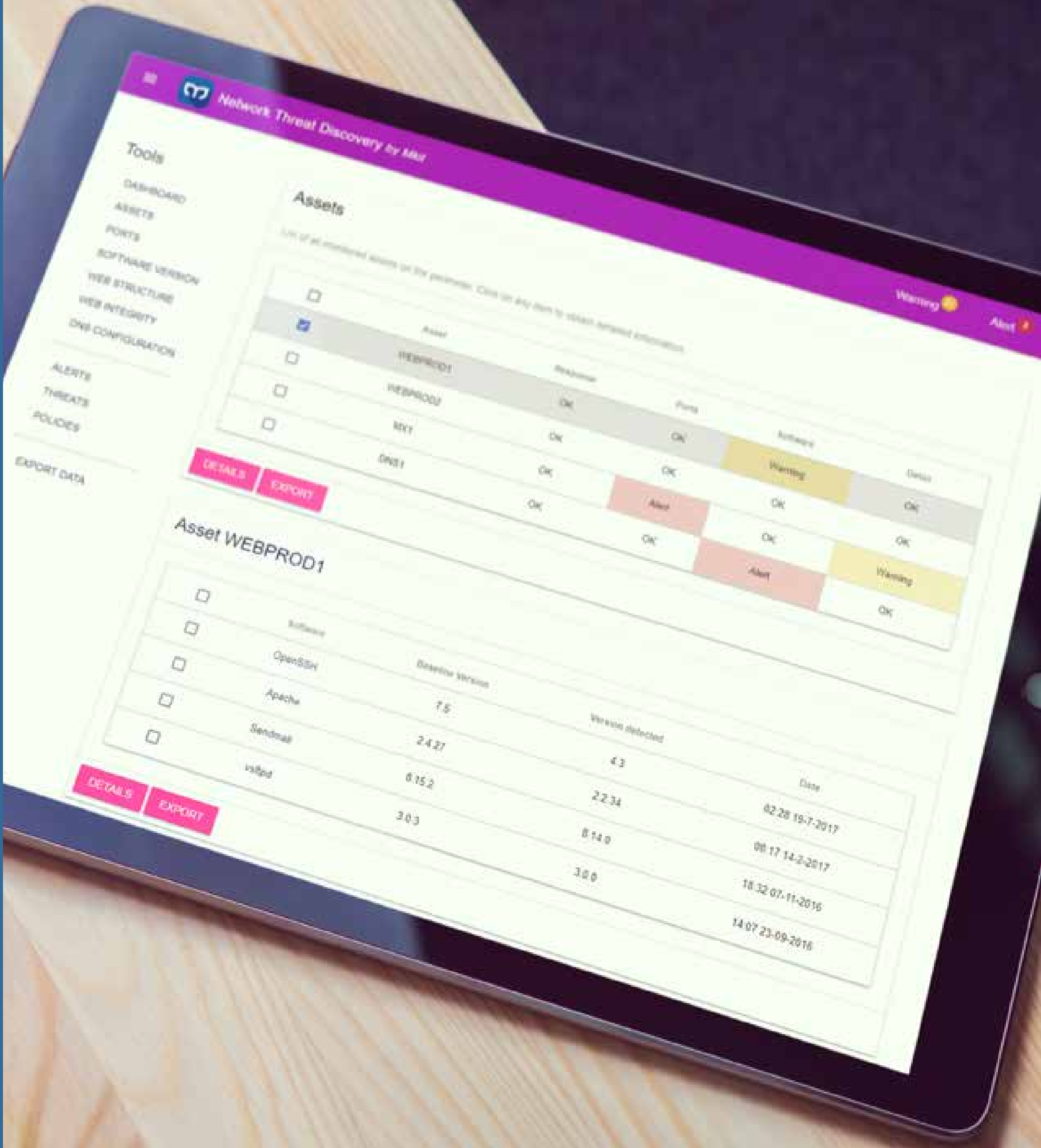
Be aware of what happens on your perimeter, all the time. Stop attacks from occurring, by noticing alterations on your network the second they take place.

Our Network Threat Discovery tool provides a 24/7 supervision of any changes in the network infrastructure, servers and Web applications the organization keeps publicly available on the Internet, in all the main essential layers of the OSI model, with the objective of early discovering a potential attack, or performance malfunction.

When a discrepancy is found, the tool will send out an alert in different ways (Email, SMS, phone call), according to its severity.

The tool can detect all major types of attacks:

Defacements	Injections
File uploads	Server hijacking
Domain takeover	Denial of Service



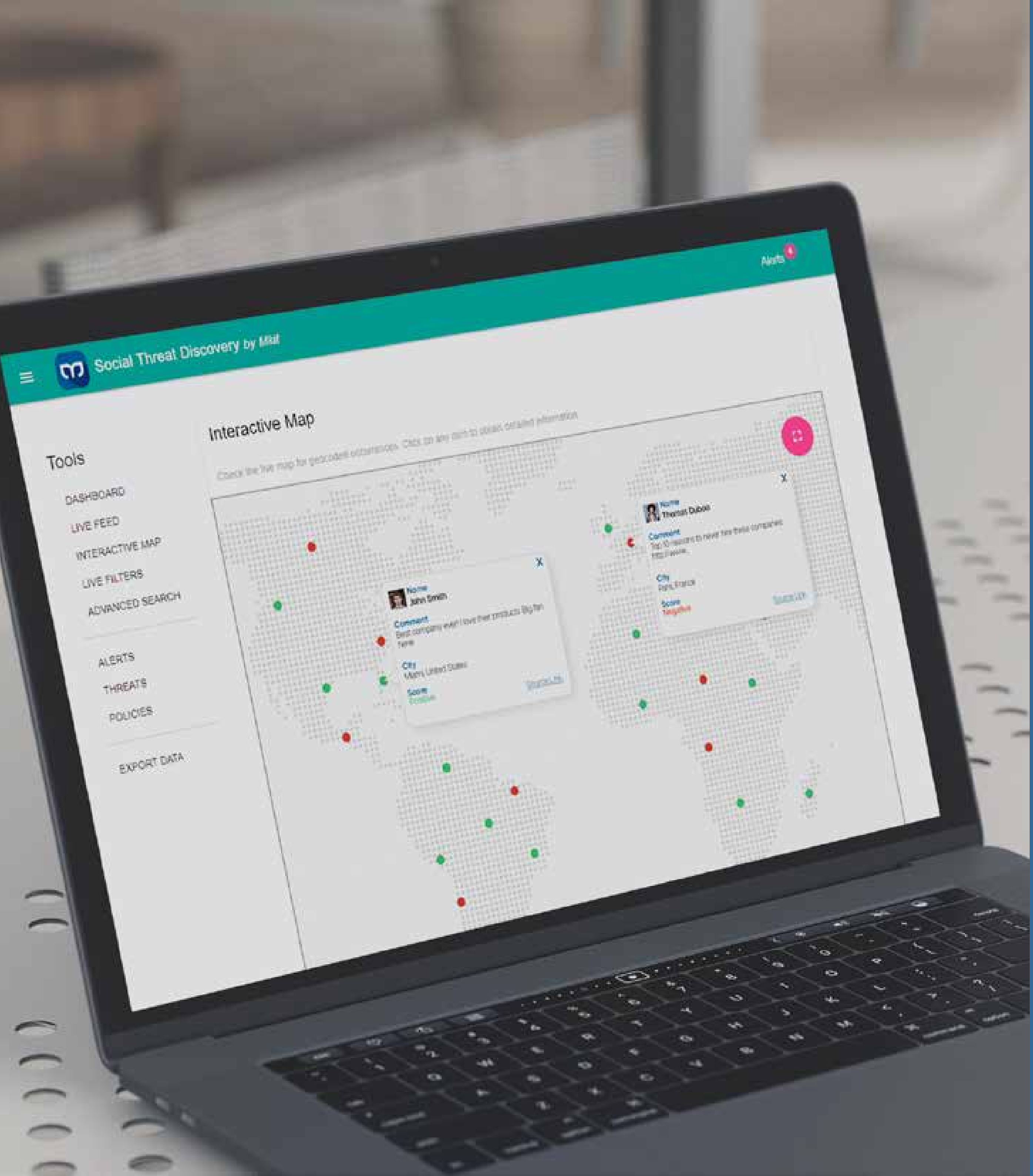
Assets

List of all monitored assets on the perimeter. Click on any item to obtain detailed information.

☐	Asset	Response	Ports	Software	Detail
☑	WEBPROD1	OK	OK	Warning	OK
☐	WEBPROD2	OK	OK	OK	OK
☐	MX1	OK	Alert	OK	Warning
☐	DNS1	OK	OK	Alert	OK

Asset WEBPROD1

☐	Software	Baseline Version	Version detected	Date
☐	OpenSSH	7.5	4.3	02:28 19-7-2017
☐	Apache	2.4.27	2.2.34	00:17 14-2-2017
☐	Sendmail	8.15.2	8.14.0	18:32 07-11-2016
☐	vsftpd	3.0.3	3.0.0	14:07 23-09-2016



Social Threat Discovery

Not all hazards come from network or application strikes. Social networks, search engines, and even the media can make or break your organization.

Our Social Threat Discovery tool consists of an advance search engine and social network monitoring system. It performs continuous scans for information in the public domain, looking for any kind of occurrence that may negatively affect the organization.

The tool integrates a syntactic analysis in realtime, to determine whether every captured message represents a comment with a positive or negative connotation.

You can visualize the results through a live interactive map that geocodes each publication. The framework includes live result filtering and an advanced historical search. It also notifies of any critical alert that should be addressed immediately.

Mkit | Security Solutions

Mkit® is a registered trademark of MKIT S.R.L., Buenos Aires, Argentina.