Keep IT Secure 24

Case Study Energy

The benefits of transforming the pentest project approach into a structured process

+79% Uncovered vulnerabilities

56% FASTER Time to solve a vulnerability

60% Reduction redundant interactions

+82% Risk reduction

Client profile

N° of employees: 1.000-5.000
Worldwide presence: Worldwide
N° of critical apps under testing: +100
N° of IPs under testing: +1.500

Technologies Tested

Internet Presence
Management Apps
Partners / Contracts / Apps
Control Stations
Business Apps
HR Apps
External Apis
Onsite Station Apps
Email, Dns, VPN

Potential savings if data was breach

If critical vulnerabilities reported over the period of 1 Year were exploited / generated an incident the estimated impact would be:

(over) > 20.000.000 Eur

The way that the company used to approach Pentesting

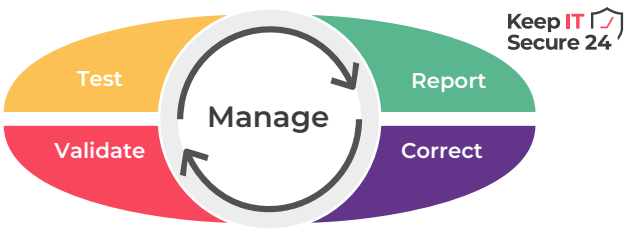
- Project based
- Hire an external company
- 1 Pentesting project per year focused on external network and infrastructure
- Reports were delivered in pdf and excel files
- Results were managed ad hoc through email or by using internal ticketing system

Problems

- Time wasted before and during the setup phase
- Challenging to manage the process:
  - Assign vulnerability (who, how, when)
  - Confirm that vulnerabilities were properly fixed
  - Enforce resolution
  - Manage all the communications about the project
- Absence of metrics
- Risk inherent to not Pentesting some releases
- Risk exposure to 0-days until the next cycle of testing
- Lack of knowledge from teams to solve vulnerabilities

Solution KEEP-IT-SECURE-24 (Persistent Pentesting in a managed services approach)

New approach to Pentesting



- Trust a specialized and recognized Team / Company with a well-structured process providing Persistent Pentesting through all the year
- Vulnerabilities are reported in a management platform that helps to manage all the process
- Vulnerabilities can be assigned directly to the responsible for fixing
- Teams interact with our expert consultants to ask for help during resolution process
- Integration with change management
- Custom reports about risk and efficiency

Benefits perceived by the client with the new approach

- Teams performance and motivation
- Less time wasted in communications (email, conf / phone calls)
- Improvement on the vulnerabilities resolution time
- Improved communication across all the process
- Risk reduction as all releases and changes were tested before going to production
- Less time wasted to set-up projects to test new releases
- Improve the security posture of the organisation since metrics help to define an adequate road map of actions to be taken. (eg: custom training, technologies used, suppliers)
- Effective communication with the board with customised metrics, graphics and reports

Provided by: devoteam Cyber Trust

Case Study Energy

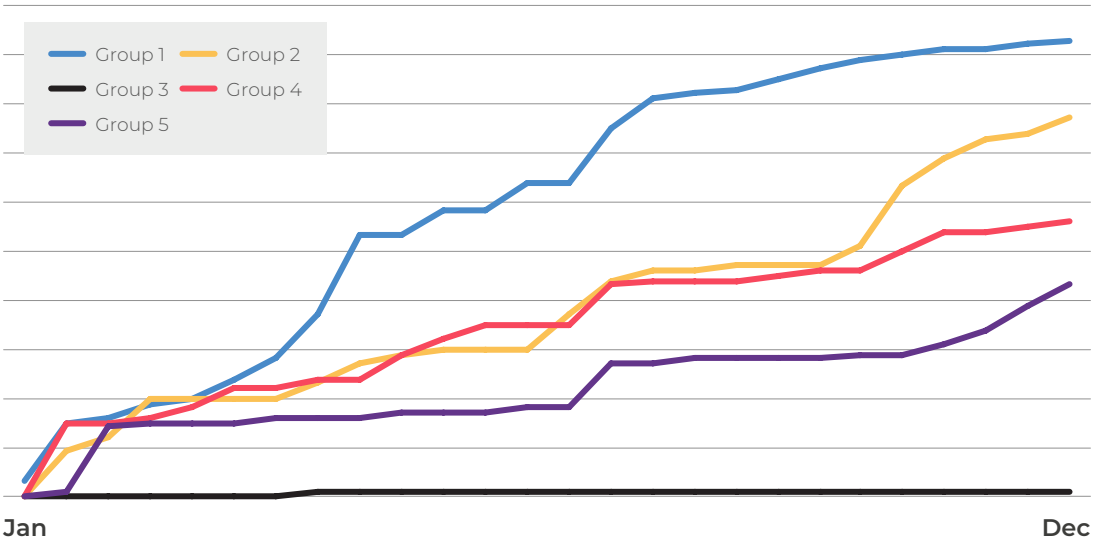
Keep IT Secure 24

In order to properly manage it is very important to be aware of metrics, KPIs and evolution. Below you can find some metrics that we provide to our clients:

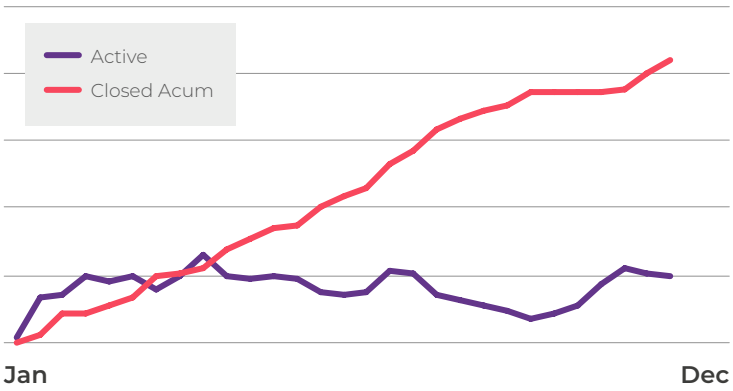
Vulnerabilities reported per Group of Asset

The Persistent Pentesting Model provides the continuous identification of vulnerabilities through the time, considering that tests are everytime more deep, and also considering new vulnerabilities, 0-Days and resulting from change management.

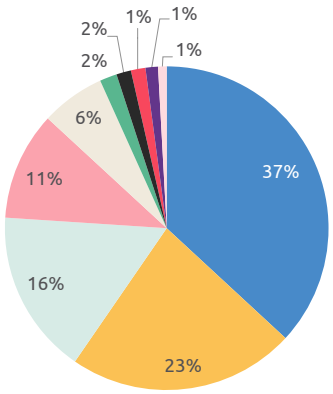
The solution also provides the feature of customizing reports according to client requirements.



Solved vs Active



Data from 2017 KITS-24 Study



- Sensitive Data Exposure
- Security Misconfiguration
- Broken Authentication and Session Management
- Cross Site Scripting (XSS)
- Information Leakage
- Insecure Data Storage
- SQL Injection
- Broken Access Control
- Insecure Direct Object References
- Business Logic

Contact us for a demo or for more detailed information www.keepitsecure24.com

Certifications & Accreditations

We are a certified company that is focused on protecting its clients' information, as well as on providing a world class service based on Industry Standards and best practices.

ISO 27001 (2012) **CREST (2014)** **ISO 9001 (2014)** **PNSC (2017)**

PCI (2020) **Bancontact (2021)** **ISO 27701 (2023)**

Provided by: devoteam Cyber Trust