

Continuous Security Monitoring Platform

Enumerate & deeply scan your infrastructure using 15 most trusted community-backed security tools

About us: Team leaders



Ethically hacking together since 2015



Vlad
CEO

MSc Information Security
(Royal Holloway University of London), 2014

Principle Consultant in Singapore,
Red team lead in Russia

Certificates: CREST and OSCP

Anatoly
CTO

Degree in computational mathematics and
cybernetics (MSU), 2011

Bugbounty hunter, participant and speaker of
invite-only HackerOne offline events

Winner of multiple CTF competitions
(ranked 15th in the world)



hackerone



Why 3950 companies were hacked in 2020¹?

- Company's infrastructure is changed daily
- Penetration test (manual security audits) are done only 1-2 per year
- It's not possible to analyse all changes for security impact
- Traditional scanners provide basic security coverage, hard to manage
- A lot of side-risks exist: Employee password leaks, source code leaks



[1] <https://www.varonis.com/blog/data-breach-statistics/>

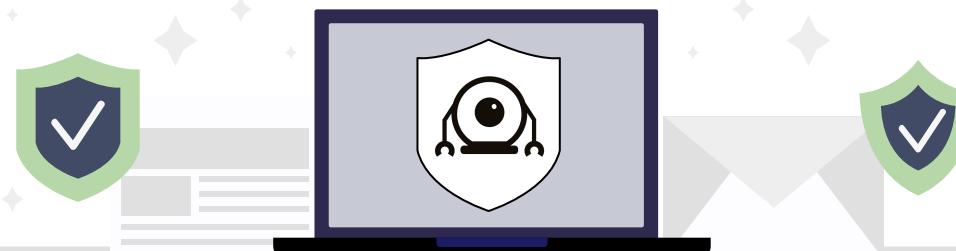
Solution: Platform that automates the work for InfoSec Departments

Comprehensive: Detects vulnerabilities **that are missed by scanners and by people**

24x7 monitoring: real-time vulnerability notifications

Signal Sources: a set of commercial and open source tools,
that are combined with proprietary algorithms

Extended support: we verify the monitoring results



Signal sources

15 top-rated scanners and growing

OSINT

Passive and active asset management

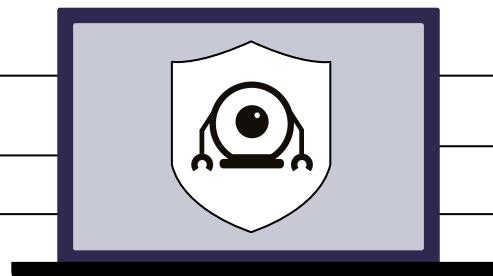


Port and service scanners



Web-scanners

Deepest coverage on the market



Email password leaks

The largest leak database:
15 billion records



Subdomain takeovers



Password bruteforce

Using self-crafted dictionaries

Demo: Real-time Vulnerability Feed

The screenshot displays the Scanfactory web application interface, specifically the 'Demo Project - scanfactory.io' page. The top navigation bar includes links for Dashboard, Alerts, and Projects. The main content area shows a summary for the demo project, indicating 6 URLs and 3 Domains, with a status of 100% and a green progress bar showing 21 finished out of 21 total.

The interface is divided into two sections: 'Scope:' containing the pattern *.scanfactory.io, and 'Out of scope:' which is currently empty. On the right side, there is a detailed 'List of alerts' table with the following data:

Alerts	Last Seen	Component	Severity
Cross-site scripting (reflected)	15 days ago	burp	Critical
External service interaction (DNS)	15 days ago	burp	Critical
Password bruteforce success: storage.scanfactory.io:21	14 days ago	patator	Critical
XML external entity injection	5 days ago	burp	Critical
Detailed Error Messages Revealed	15 days ago	burp	Medium
User enumeration on wordpress.scanfactory.io:80	15 days ago	wpscan	Medium

Demo: Real-time visibility of infrastructure

Overview



The rarest / newest

Host/ports	Updated
dev-test.google.com:80	2 min ago
admin.google.com:8443	5 min ago
admin.google.com:8242	10 min ago

See more ▾

Track new open ports

Hosts list

Hosts list					
Project		Name of hosts	Risk Score	Ports	Last update
Bu Google	Google	dev-test.google.com	Critical	80: https ✘ 3360: mysql 21: ftp 22: ssh 117: uucp-path 22: statsrv 131: cisco-tna 542: commerce	16:30 26.07.2021
		admin.google.com	Medium	80: https ✘ 3360: mysql 21: ftp 22: ssh 117: uucp-path 22: statsrv	16:30 26.07.2021
		142-24-19-22.google.com	Low	80: https ✘	16:30 26.07.2021
Sd Facebook	Facebook	www.facebook.com	Low	80: https ✘ 3360: mysql 21: ftp 22: ssh 117: uucp-path 22: statsrv 131: cisco-tna 542: commerce	16:30 26.07.2021
		www-dev.facebook.com	Low	80: https ✘ 3360: mysql 21: ftp 22: ssh 117: uucp-path 22: statsrv	16:30 26.07.2021
		staging.facebook.com	Low	80: https ✘	16:30 26.07.2021

Review historical changes



Search and filter your assets

How does it work?



01

Setup

Provide a list of domains and IP addresses or just the name of the company



02

Scanning 24x7

The platform crawls and analyzes sites, applications and services



03

Notifications

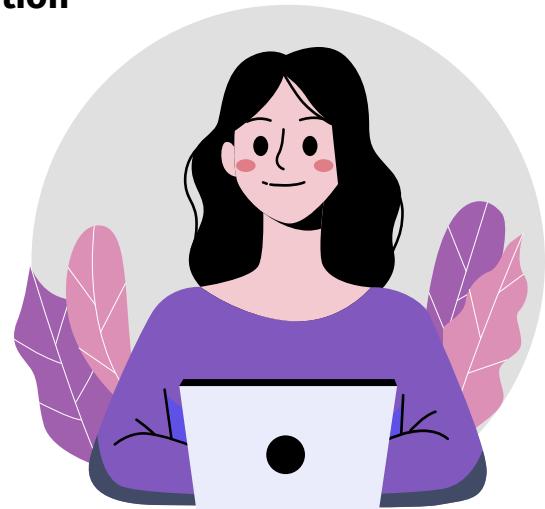
Results are available in the web panel, or integrate us with SOC/SIEM

Setup: variety of options

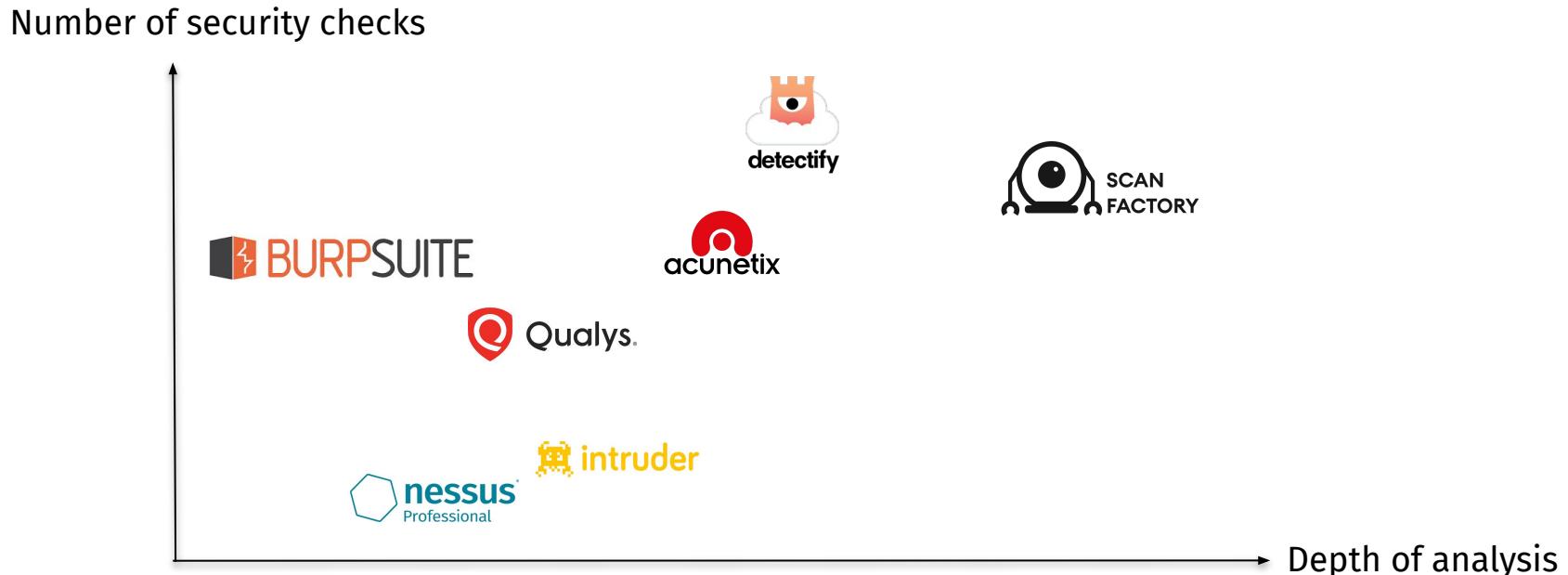
1. **Cloud SaaS:** We host the platform
2. **On-prem:** You host the platform
3. On-demand scans, results in PDF report
4. On-demand scans, results in PDF report **with manual verification**

As a result, this will

Automate the work of your
infosec department and provide
deepest security coverage



Competitor analysis



We are constantly adding new scanners to the platform

Platform found critical vulnerabilities in world's top companies

US

Uber

PayPal

yahoo!

amazon

shopify

Adobe

VALVE

GitHub

algolia

IBM

verizon[✓]

Scaleway

salesforce

APAC

DBS

ING



UOB
大華銀行

Agency for
Science, Technology
and Research
SINGAPORE

sivantos
the hearing company

Free trial: 1 week

Say hello:

vlad@scanfactory.io



Ask me anything:

+7 (915) 000-12-34  

Vlad