ThreatSee

Digital twin of your IT infrastructure for penetration testing

INTRODUCTION

New vulnerabilities

22316

(2019)

23210

(2018)

https://www.securitylab.ru/news/505210.php

INTRODUCTION

High or Critical Risk

20%

67 days

The average time for applying a patch to a known vulnerability.

https://www.edgescan.com/wp-content/uploads/2018/05/edgescan-stats-report-2018.pdf

INTRODUCTION

+30%

Number of new vulnerabilities in automated technological process control systems

+17%

critical and high-risk vulnerabilities (in 2018 compared 2017)

https://www.ptsecurity.com/en-us/research/analytics/ics-vulnerabilities-2019/

INTRODUCTION

From 6 months to 2 years

The time that vendors eliminate vulnerabilities in automated technological process control systems components.

https://www.ptsecurity.com/en-us/research/analytics/ics-vulnerabilities-2019/

INTRODUCTION

SO WHAT?!

PROBLEMS

Business Owners, CIO, CISO, etc wants:

to know (or already knows) about the vulnerabilities of the IT and OT infrastructure,

but don’t understand what the consequences may be from their presence;

PROBLEMS

Business Owners, CIO, CISO, etc wants:

to make penetration testing to gain knowledge about the state of cybersecurity,

but afraid to make it in a working infrastructure.

PROBLEMS

Business Owners, CIO, CISO, etc wants:

to know about the possibilities of attackers to inflict damage in environments where penetration testing cannot be carried out (for example, automated technological process control systems, operating medical equipment, etc ...)

PROBLEMS

Penetration testing

is an excellent way to understand the degree of vulnerability of existing IT and OT infrastructure and the abilities of hackers to damage the infrastructure in its current state.

But it’s not always possible to conduct penetration testing…

PROBLEMS

Penetration testing

is an excellent way to understand the degree of vulnerability of existing IT and OT infrastructure and the abilities of hackers to damage the infrastructure in its current state.

But the result depends on the qualifications of the pentesters

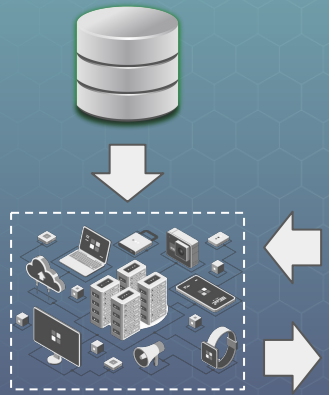
SOLUTION

ThreatSee

is the system that creates a "digital twin" of IT and OT infrastructure and demonstrates the ability of an attacker to inflict damage by exploiting existing vulnerabilities.

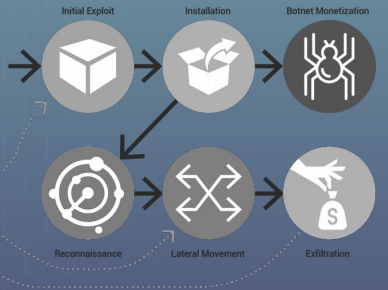
HOW IT WORKS

Collecting information about infrastructure



Digital twin creation

TreatSee



Report

COMPETITORS

Penetration Testers

Vulnerability Scanners

Infrastructure Duplicators

COMPETITIVE ADVANTAGE

Penetration Testing

Real penetration testing is needed.

Sometimes it can be dangerous or impossible!

ThreatSee

No real penetration testing needed.

Safe and informative!

COMPETITIVE ADVANTAGE

Vulnerability scanners

Not understand the “kill chain”

ThreatSee

Artificial Intelligence show, what attackers can do and how they will do it

COMPETITIVE ADVANTAGE

Infrastructure duplicate

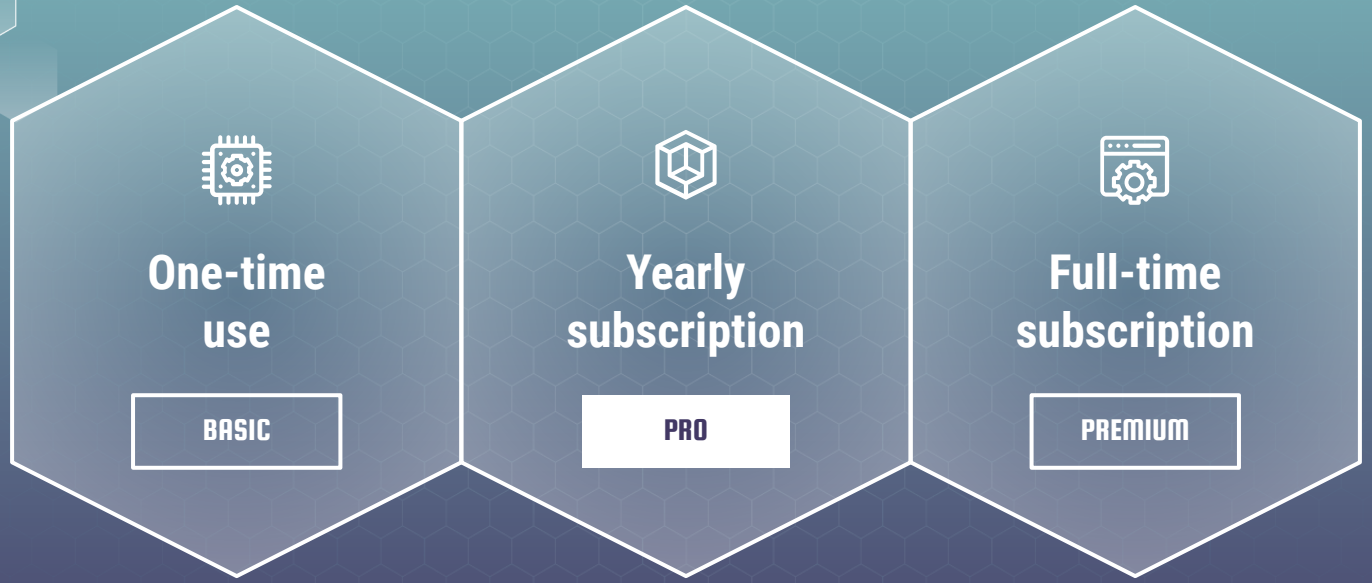
Very expensive

ThreatSee

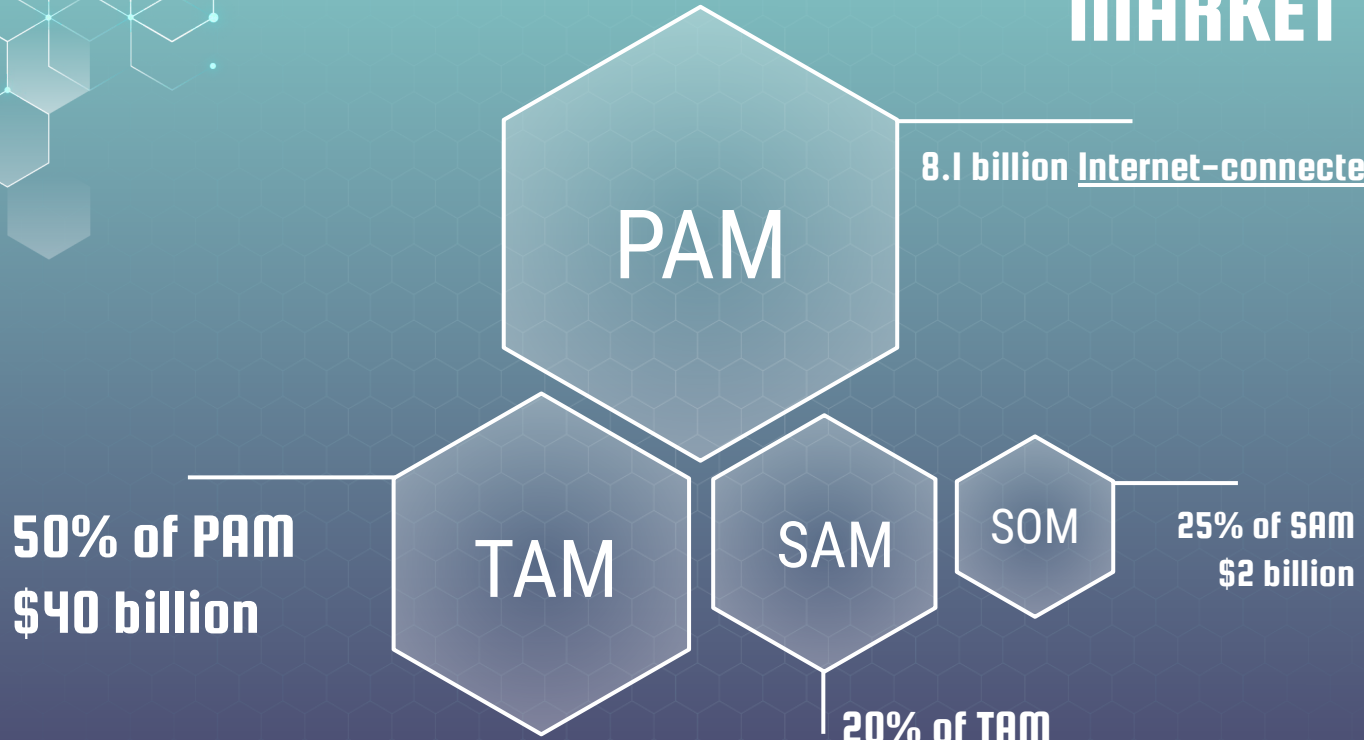
Low cost

PRODUCT OVERVIEW

PLANS


One-time use
BASIC
Yearly subscription
PRO
Full-time subscription
PREMIUM

MARKET SIZE



8.1 billion Internet-connected devices (2015)
$10 per host

50% of PAM
$40 billion

25% of SAM
$2 billion

20% of TAM
$8 billion

TARGET

Size

75% Enterprise

25% SMB

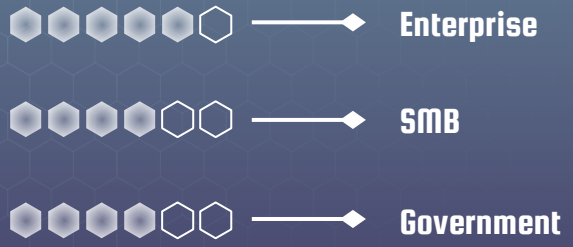
500

Average number of hosts

5000,00

Average payment per customer

Interest



SWOT ANALYSIS

STRENGTHS

- Competencies
- Global market
- The growth the number of computer equipment
- Accompanying cybersecurity services

WEAKNESSES

- Only one problem solution
- Not enough marketing experience
- Doesn't conduct phishing and Wifi-testing

OPPORTUNITIES

- Security GRC
- Patch Management
- Continuous Penetration Testing

THREATS

- Legal restrictions

PREDICTED GROWTH

Q4’2023
1000 clients - $5 000 000

Q1’2023
400 clients - $2 000 000

Q3’2022
100 clients - $500 000

Q1’2022
20 clients - $100 000

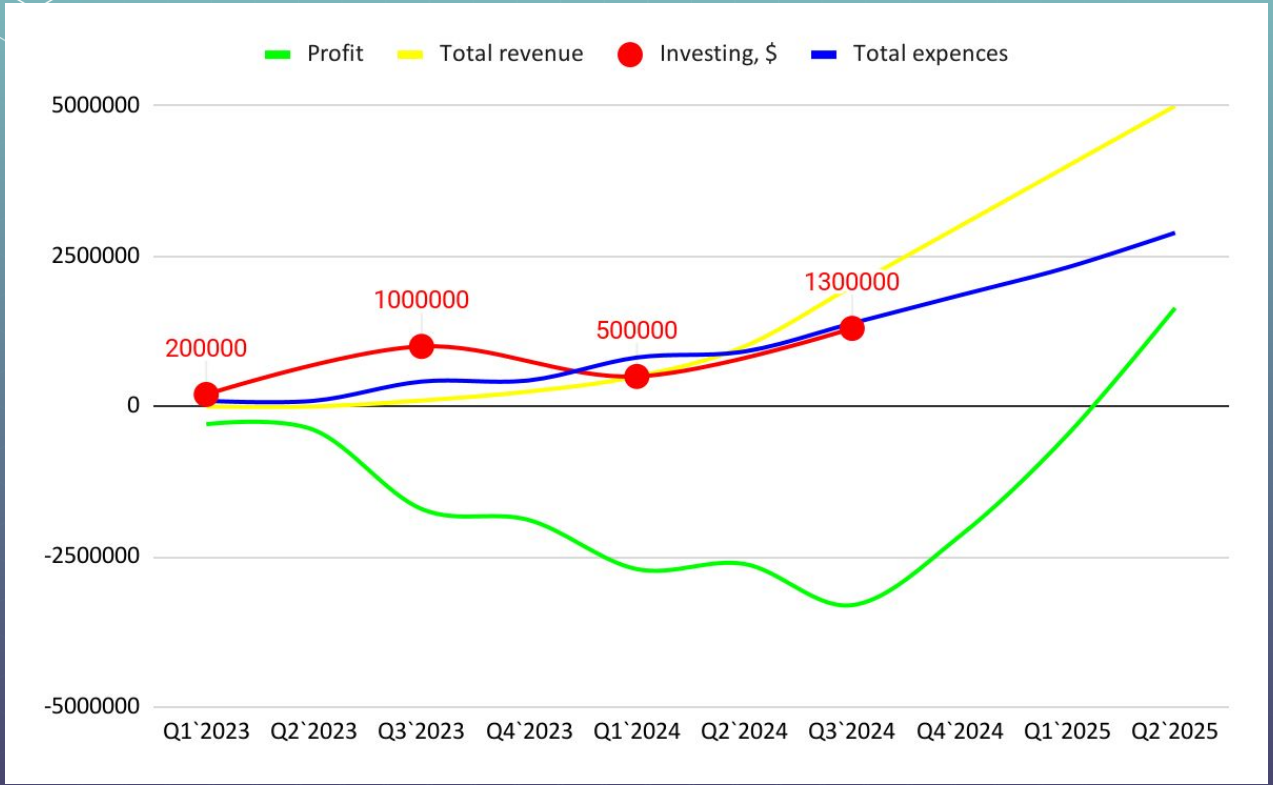
INVESTMENT

Before Q1`2021 (MVP): $ 200 000
Before Q1`2022 (First sales): $ 1000 000
Before Q3`2022 (Integrations): $ 500 000
Before Q1`2023 (Scaling): $ 1 300 000

Total: $ 3 000 000

After Q1`2023: Profitable

Graphs


Profit
Total revenue
Investing, $
Total expences
5000000
2500000
0
-2500000
-5000000
200000
1000000
500000
1300000
Q1`2023
Q2`2023
Q3`2023
Q4`2023
Q1`2024
Q2`2024
Q3`2024
Q4`2024
Q1`2025
Q2`2025

OUR TEAM

CONTACT

Does anyone have any questions?

contact@threatsee.com
+7 999 99 99
threatsee.com