Positive Technologies

Leading cybersecurity innovations to help you resist cyber threats of today

About Positive Technologies

22 years
In security R&D

3 000+
Employees

280M
USD revenue in 2023

3 000+
Customers worldwide

20+
Cybersecurity products

Protected
2018 FIFA World Cup
2014 Sochi Olympic Games
2018 and 2021 President Elections

Expertise is PT main asset

350+ Experts in PT ESC

Biggest Expert Security Center
in Eastern Europe

Hall of Fame

Experts recognized by
market leaders

PT SWARM

Security research team
(99% success rate)

Uncovered APT groups

ChamelGang
Calypso
Space Pirates
TaskMasters

300+

security audits of corporate systems performed annually

250+

zero-day vulnerabilities discovered every year (70% high or critical level)

Customers

International Companies

SAMSUNG
Terna
Hanwha
Posteitaliane
ABBYY
UniCredit Bank
ATB
du
Raiffeisen BANK
SK telecom
التجاري وفا بنك Attijariwafa bank
Auchan

Critical Industry Level Coverage in Russian Federation

4/4 largest telecom providers
8/10 largest gas & oil companies
8/10 largest banks
3/5 largest transport and logistics companies
1/1 nuclear industry company

Government Level

- Ministry of Digital Development
- Ministry of Interior
- Tax Authority
- Ministry of Healthcare
- Ministry of Transport
- Ministry of Energy
- Information security regulators

Government SOC Deployments

GovCERT

FinCERT
Central Bank of Russia

HealhCERT
Ministry of Healthcare

TransportCERT
Ministry of Transport

Corporate SOC Deployments

GAZPROM
ROSNEFT
LUKOIL
ROSATOM

Awareness projects

phd Positive Hack Days

Annual international cybersecurity forum on practical cybersecurity

500 000+
offline participants

120 000+
online participants

STANDOFF

The **largest Cyber Battle** in the world (Replicated the infrastructure of 12 industries)

STANDOFF

Unparalleled interactive Standoff model country demonstrating the consequences of malicious hacker actions

A 30-hour cyberbattle for control over digital infrastructure of a mock city. Conditions for attackers and defenders are as realistic as possible

Top-notch researchers test how well the virtual State F's infrastructure is protected

20+ teams of hackers from around the world compete

Diversified product portfolio

AI-enabled CS autopilot

MaxPatrol O2
SOC autopilot

MaxPatrol Carbon
Infrastructure security assessment and attack chain prediction

Cyber resilience platform

Standoff 365
Cyber range for cyber exercises

Bounty platform
Online platform

Services

- **Services** (Offense & Defense)
- **Consulting** (SOC, DevSecOps)
- **Education programs**
- **Technical and Expert Support**

Infrastructure Security

MaxPatrol SIEM
Security information and event management

MaxPatrol VM
Vulnerabilities management

PT Knockin
E-mail security assessment tool

PT Feeds **PT TAP**
Threat Intelligence (TI Feeds and TI Platform)

PT NGFW **PT AF PRO**
Perimeter protection (WAF and NGFW)

PT Sandbox
Malware protection

PT NAD
IT-Network NTA

PT ISIM
OT-Network NTA

MaxPatrol EDR
Endpoint protection

Application Security

Container Security

PT BlackBox
DAST

PT Application Inspector
SAST/IAST/SCA

https://global.ptsecurity.com/products (Products overview)
https://help.ptsecurity.com/projects (Products technical documentation)

Global recognition of Positive Technologies

Gartner

- Web application firewall Magic Quadrant *(link)*
- Application Security Magic Quadrant *(link)*
- Operational Technology Security recommended vendor *(in line with companies such as Boeing, GE, IBM, Schneider Electric, Siemens) (link)*

IDC

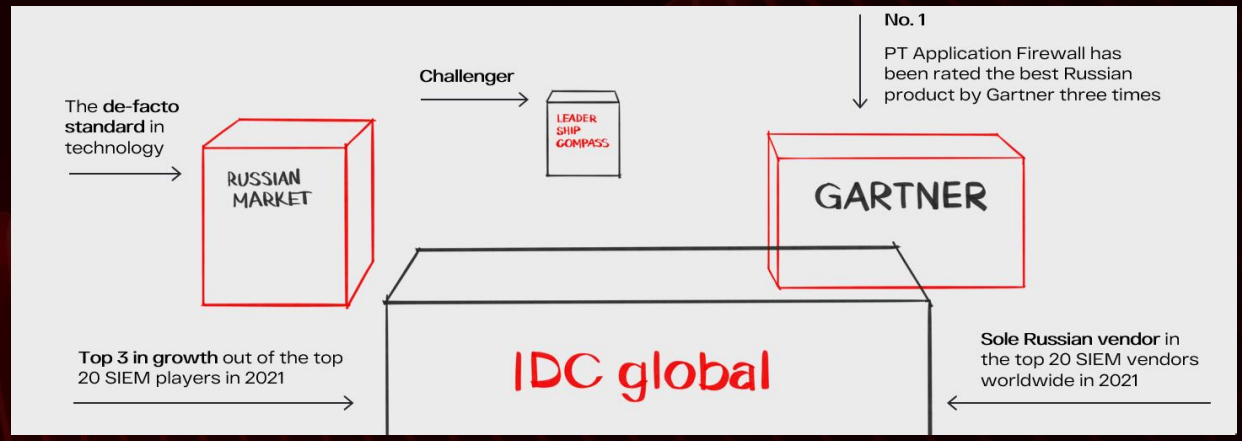
Positive Technologies – the fastest-growing company in Vulnerability Management area *(Worldwide Security and Vulnerability Management Forecast for 2013—2017)*

GSMA

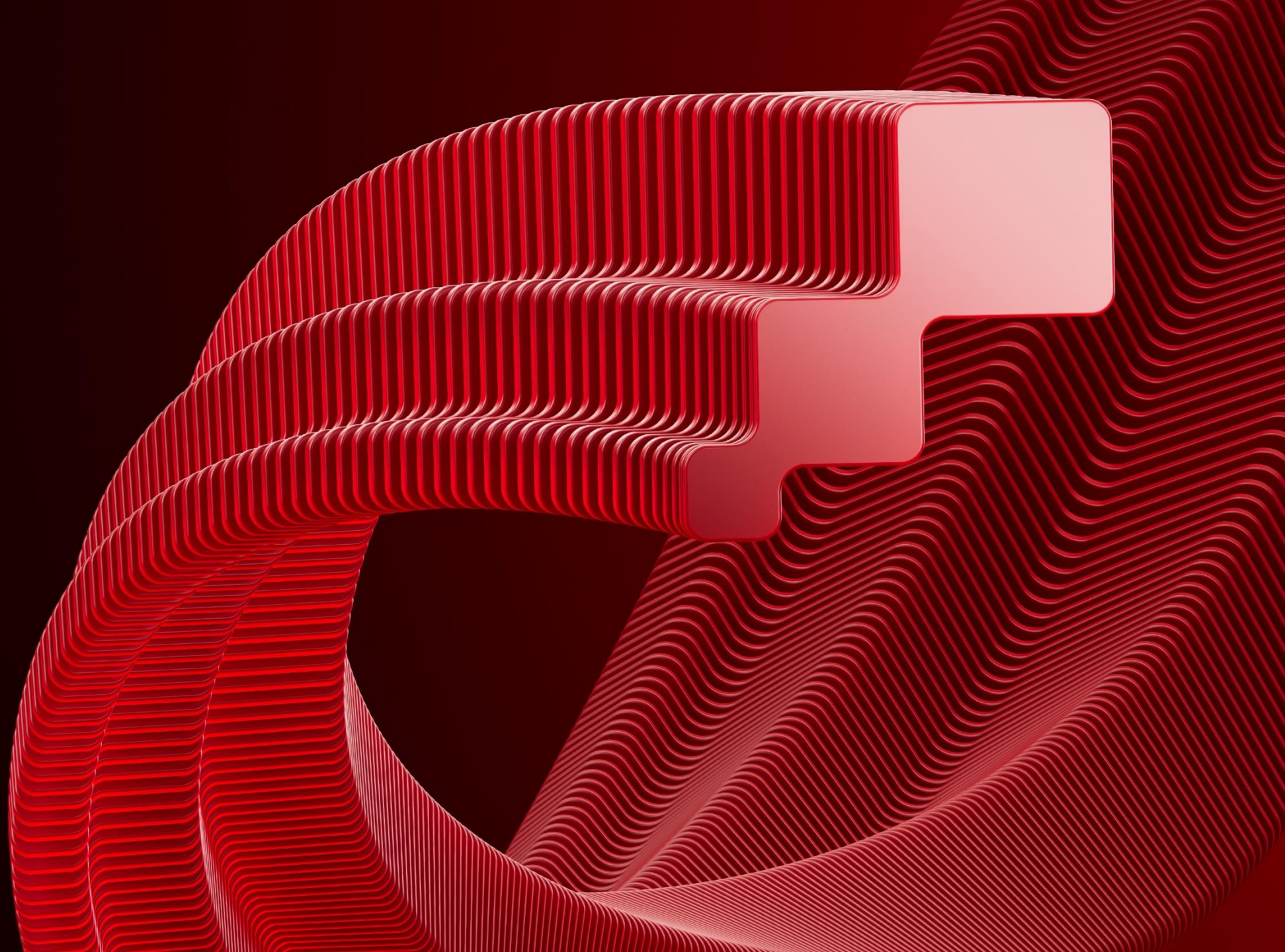
GSM Association *(1000+ telecom operators)* recommends **PT** network security solution and hardening standards

phd Positive Hack Days

The organizer of the **largest cybersecurity forum** in Europe and the **largest cyber battle** in the world



Product Portfolio



MaxPatrol SIEM

MaxPatrol SIEM Detects

- Advanced Active Directory attacks
- Activity per MITRE ATT&CK
- Database attacks
- Non-compliance with internal policies and rules
- Attacks on Linux systems
- Signs of use of hacking tools
- Ransomware activity
- Suspicious network activity, including employees working from home
- User behavior anomalies
- Changes in system configurations
- Unauthorized access to company resources

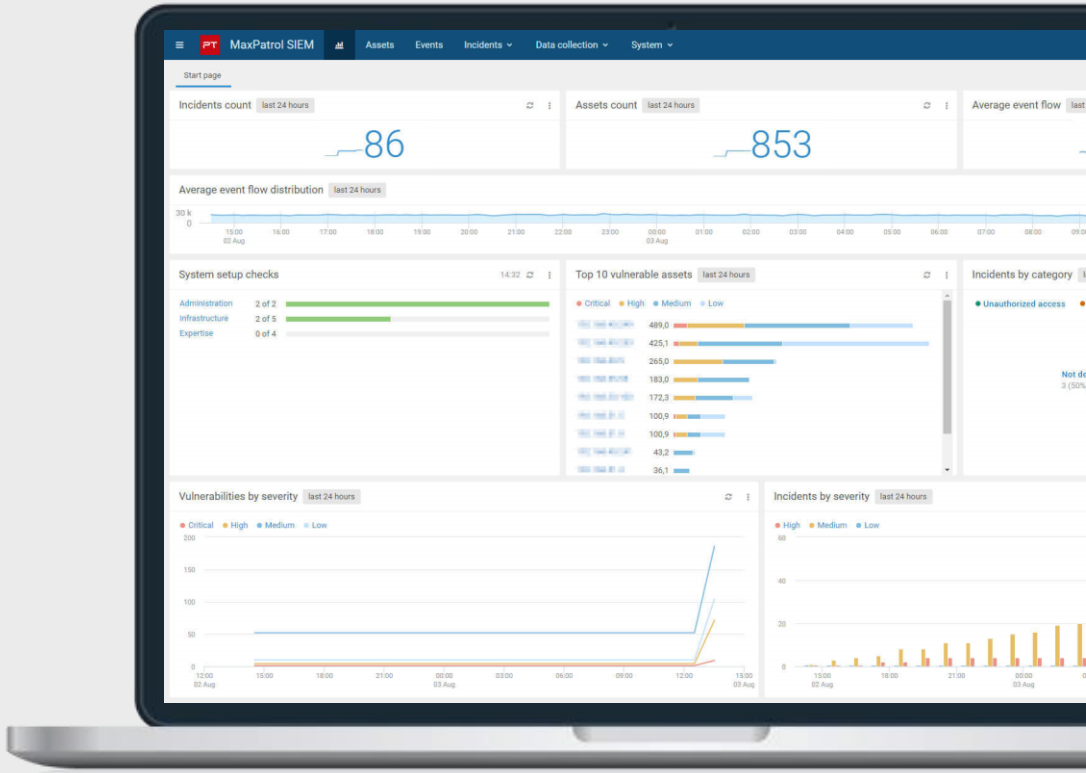
Key differentiators - MaxPatrol SIEM

Detects incidents with a unique approach that keeps IT infrastructure transparent and leverages deep expertise to discover threats.

Receives data from **300+** systems, scans the network in white and black box modes; automatically creates network topology showing the geography of the entire IT infrastructure and updates it once the new asset emerged in the system.

600+ correlation rules (out of the box included in Knowledge base) which can be also customized.
At least once a month, MaxPatrol SIEM is updated with expertise packs containing new correlation rules, indicators of compromise and playbooks.

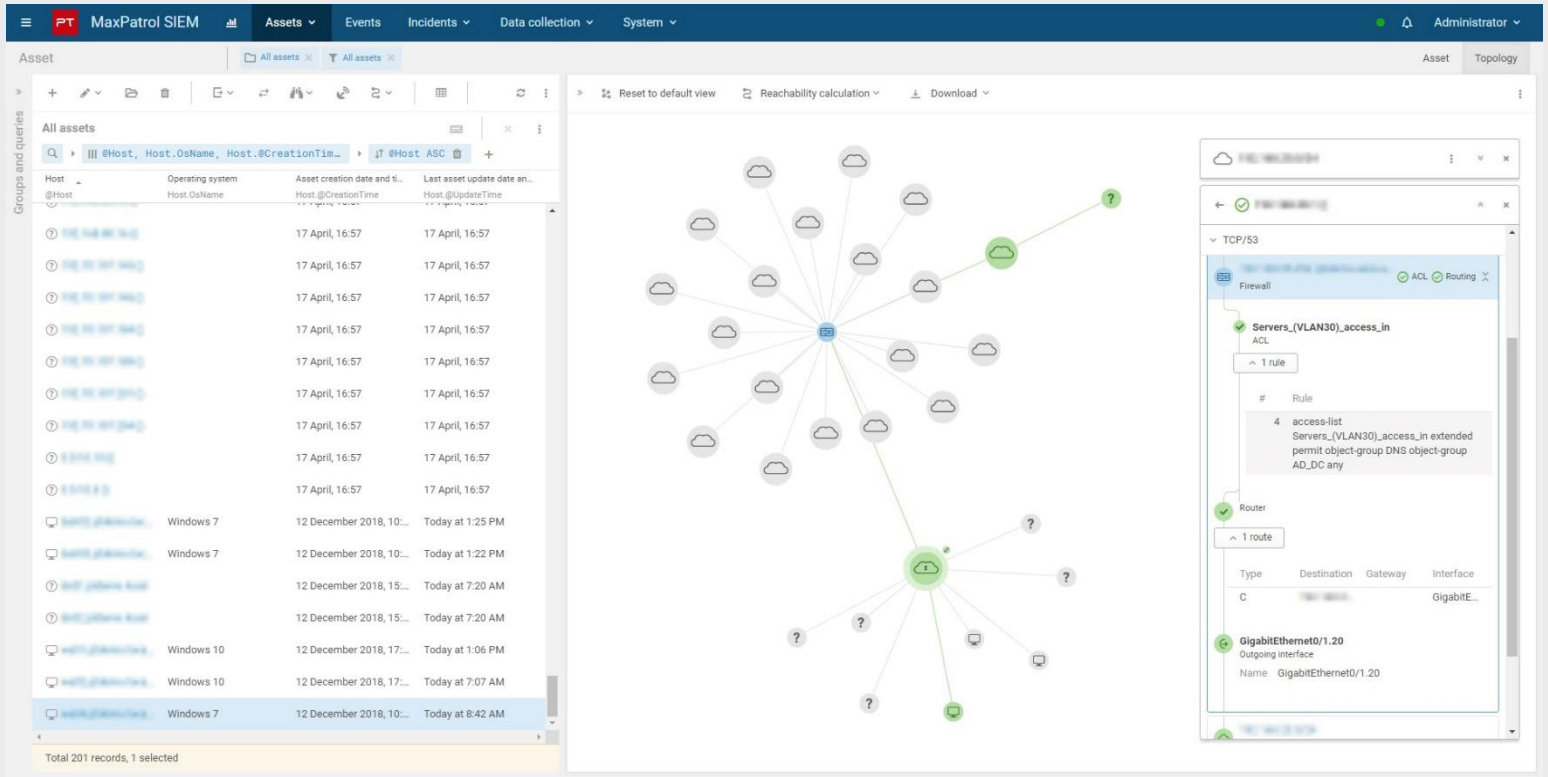
MaxPatrol SIEM users can add exception to the white list for threat detection rules in a couple of clicks, which will quickly **eliminate repetitive false positives**.



SIEM’s Network Topology Maps

Network topology shows the geography of the entire IT infrastructure. Automatically updated.

Visualization helps to better understand infrastructure, check ports on assets, evaluate feasibility of attacks, and investigate incidents.



MaxPatrol VM

MaxPatrol VM

Find all assets on the network;

Prioritize what assets are important

Get latest information on assets and vulnerabilities;

Set scan policies

Control what is happening on important assets;

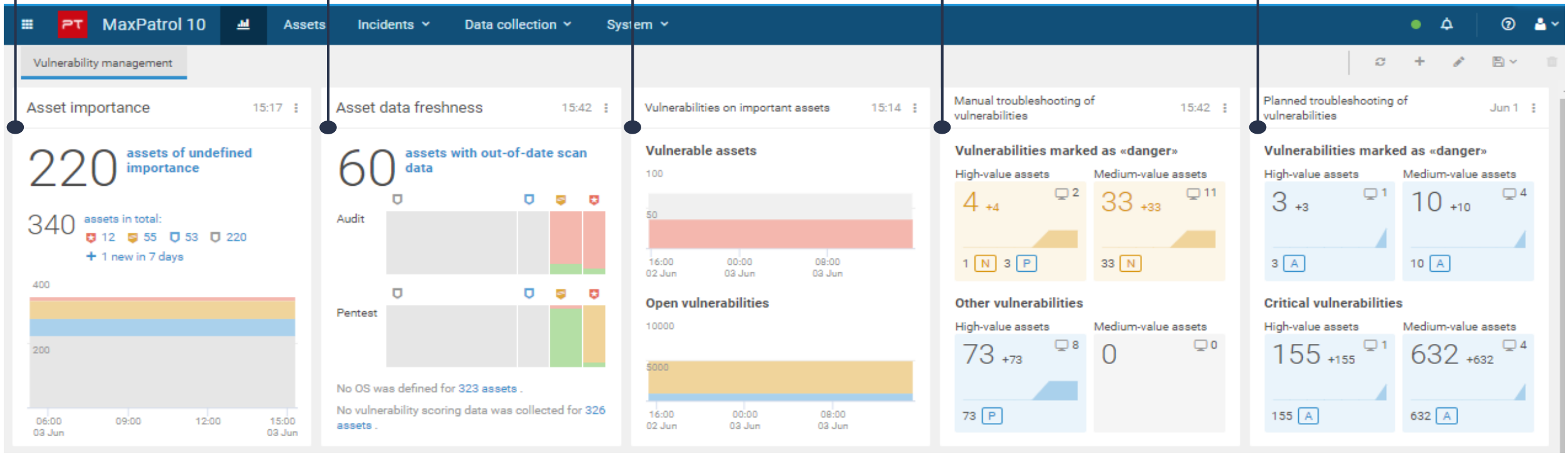
Track new assets

Regular vulnerabilities fixed by IT (in SLA);

Infosec officer monitors dangerous ones…

…as well as SLA compliance;

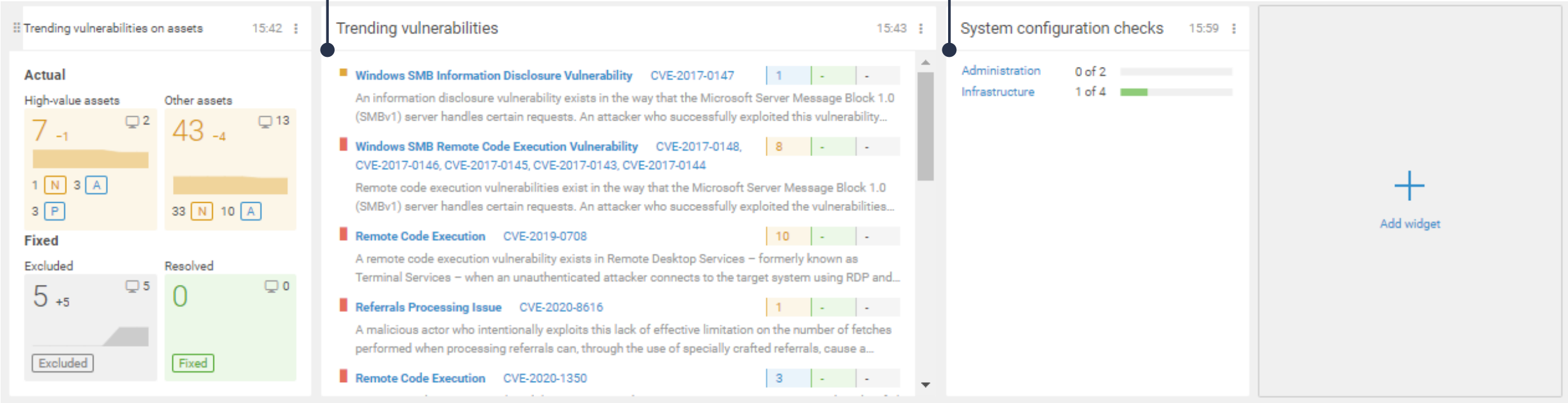
Control timely elimination of vulnerabilities



Top-trending vulnerabilities

Get information from PT experts about **top-trending vulnerabilities** that hackers and penetration testers are using worldwide

Monitor VM implementation status



How we see a truly effective vulnerability management

VM process

Scheduled vulnerability patch management

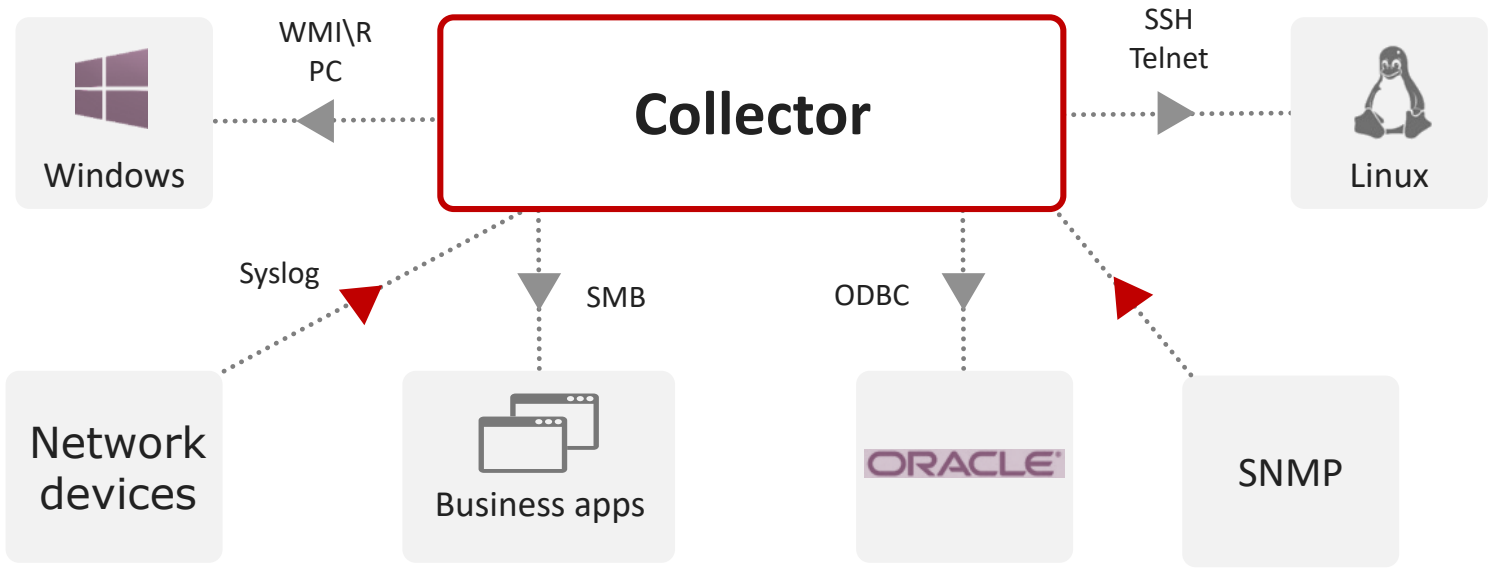
- IT department have the scheduled and negotiated patch-management process with Service Level Agreement (SLA)
- Security department control how IT department ensure the SLA for patch-management process

Addresses high-risk or trend vulnerabilities

- Trend vulnerabilities, modern or popular vulnerabilities with exploits and located in important assets
- IT and Security department have additional SLA for trend vulnerabilities

How MaxPatrol VM collects data

- Receives data via transport as active, and passively
- Scans the network in white and black box modes;
- Receives data with +300 systems
- Can receive data even from Customers unique systems



MP VM advantages

Collects >3k host parameters

500+ PT experts team
finds unique vulnerabilities and verifies public ones. This reduces the number of false positives

Passive vulnerabilities reassessment

Trending vulnerabilities are synchronized **within 12 hours**

Universal policies
that are understood by IT engineers, security experts and management

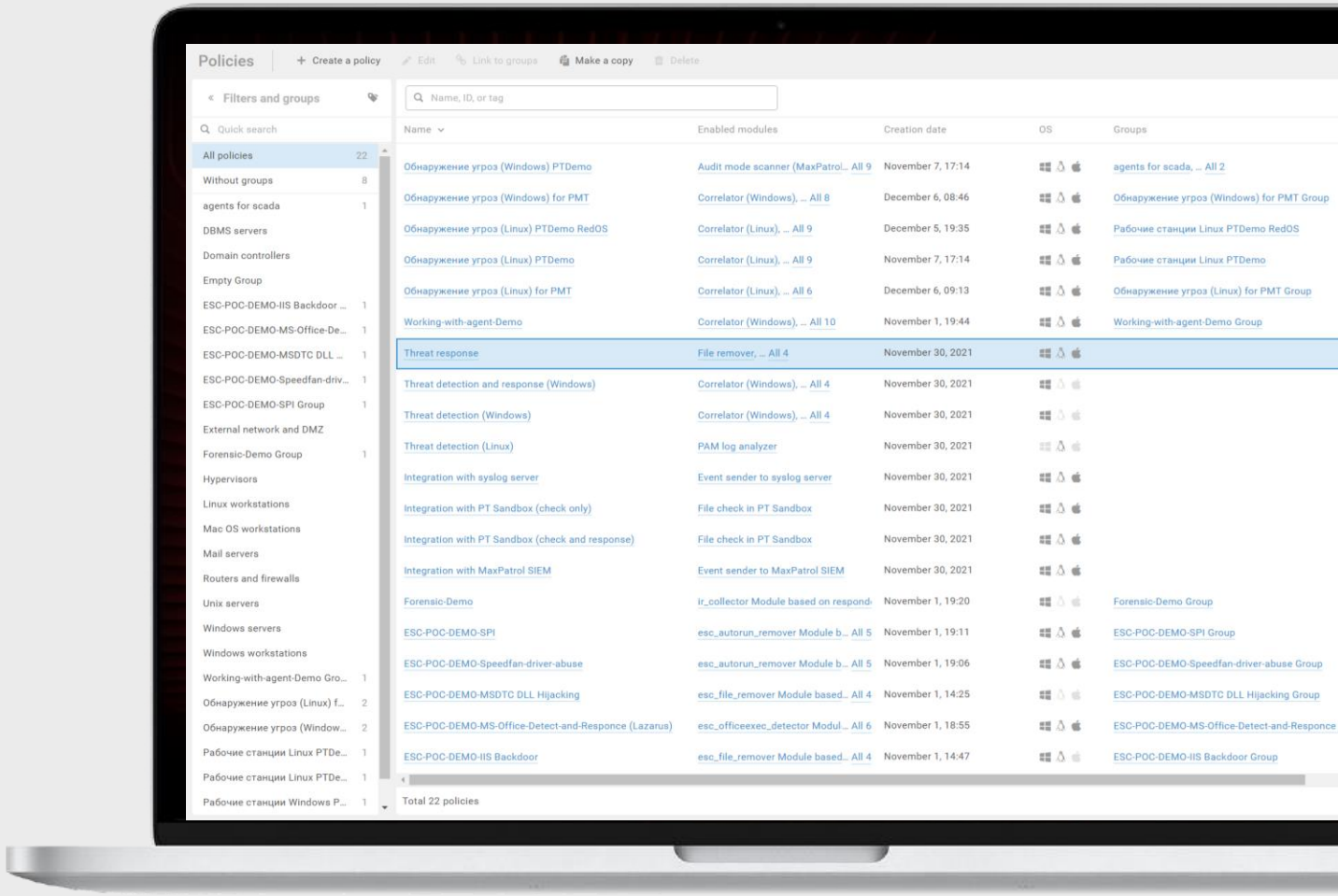
Truly on-premises: does not transmit information outside the perimeter

MaxPatrol EDR

PT EDR

Endpoint detection and response solution used to detect cyberthreats and respond to them

- Collects and analyzes data from multiple systems, detects hackers in the network, and automatically responds to attacks.
- Based on the technologies of the Positive Technologies product ecosystem, it uses unique expert knowledge about threats to identify attacks.



Max Patrol EDR: Detection

- Provisioning of extended audit tools
- Combination od detection mechanisms:
- Static analysis (5000+ rules)
- Behavioral analysis (600+ rules)
- Reputational analysis
- Step-by-step chained actions triggered by any EDR alert
- Forensics collection (MVP)
- Honeypots on request (MVP)
- Additional checks in external tools

Covers most popular MITRE ATT&CK techniques:

- Top-50 for Windows
- Top-20 for Linux

Fine and granular policies tuning

- Detection rate – workload balance
- Filter your events to lower your SIEM workload if needed

Max Patrol EDR: Response

- Full and partial host isolation
- Process termination
- File removal
- External shell
- YARA scans (with user rules as well)
- Autorun clean-up
- DNS sinkholing
- IP Blocking

SOC automation:

- Flexible autoresponse policies
- Autonomous agents

Remote Workstations control

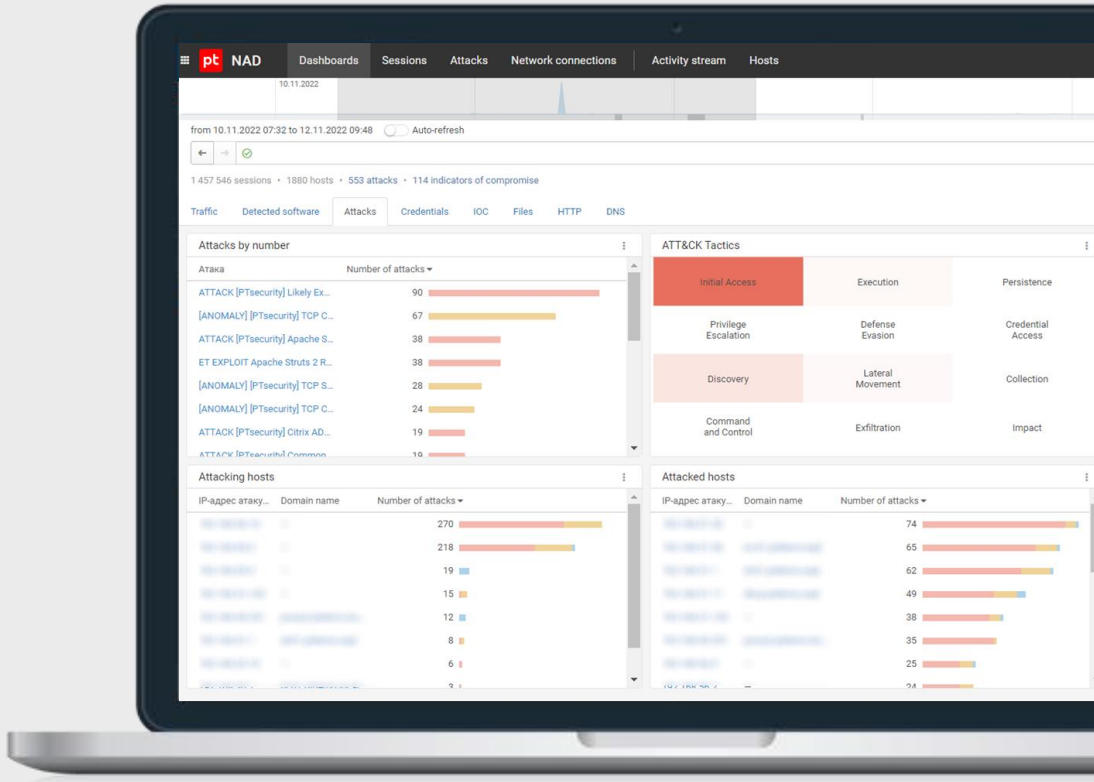
- Visibility (Events, Vulnerabilities) on Out-of-Domain and Out-of-Domain nodes

PT Network Attack Discovery (PT NAD)

PT Network Attack Discovery (PT NAD)

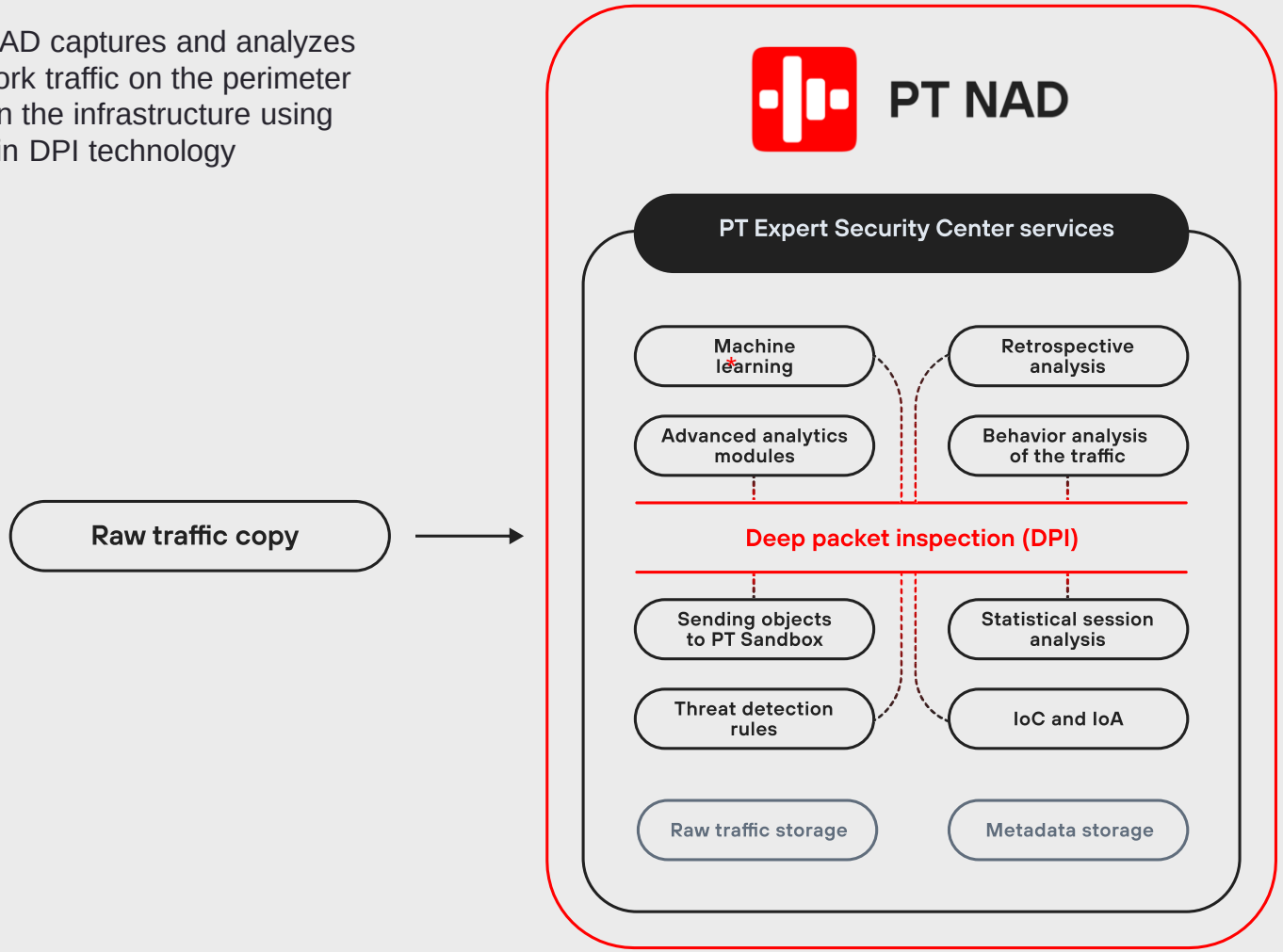
System for deep NTA used to detect attacks on the perimeter and inside the network

- PT NAD detects **over 180 MITTRE ATT&CK**
- Has **over 8000 IoAs** and 52 advanced threat detection modules
- **AI/ML detection modules**
- Detects suspicious **activity even in encrypted traffic** (Abnormalities detection)
- Stores metadata and raw traffic to provide the **full attack context** and make it easier to reconstruct the kill chain
- Detects flaws in information systems' configuration and **non-compliance with information security policy** that can lead to attacks
- Keeps attacks private. All **data is stored on client infrastructure**, never leaving the corporate perimeter

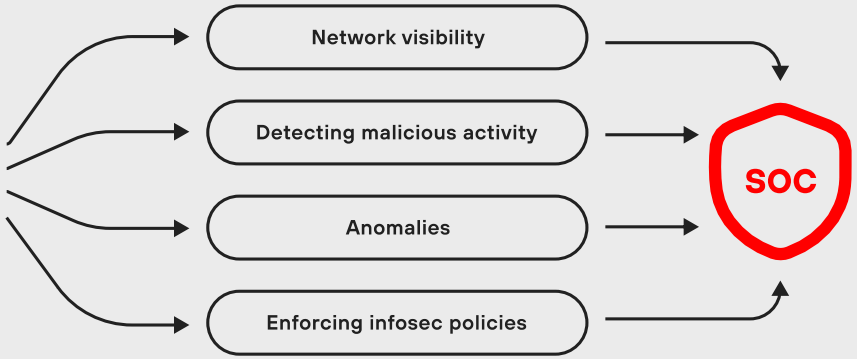


PT Network Attack Discovery

PT NAD captures and analyzes network traffic on the perimeter and in the infrastructure using built-in DPI technology

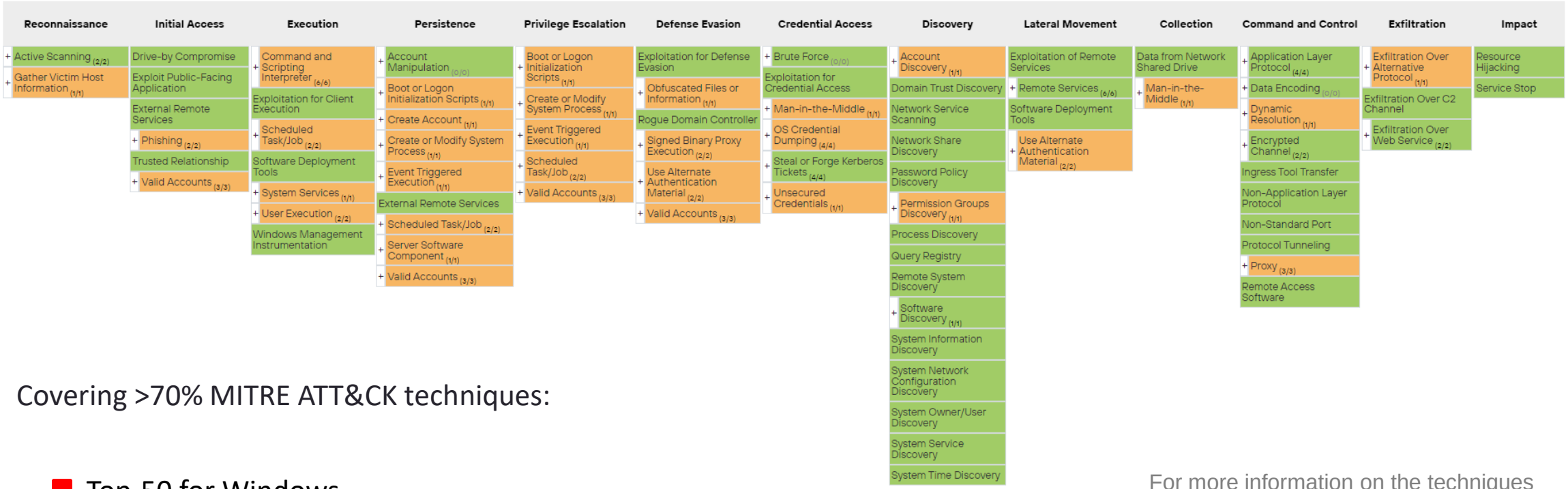


By analyzing a copy of the network traffic using statistical and behavioral modules, PT NAD detects hacker activity **at the earliest stages of network penetration**, as well as when an attacker is attempting to gain a foothold in the network and escalate the attack



MITRE ATT&CK techniques

PT NAD detects >180 adversary techniques



Covering >70% MITRE ATT&CK techniques:

- Top-50 for Windows
- Top-20 for Linux

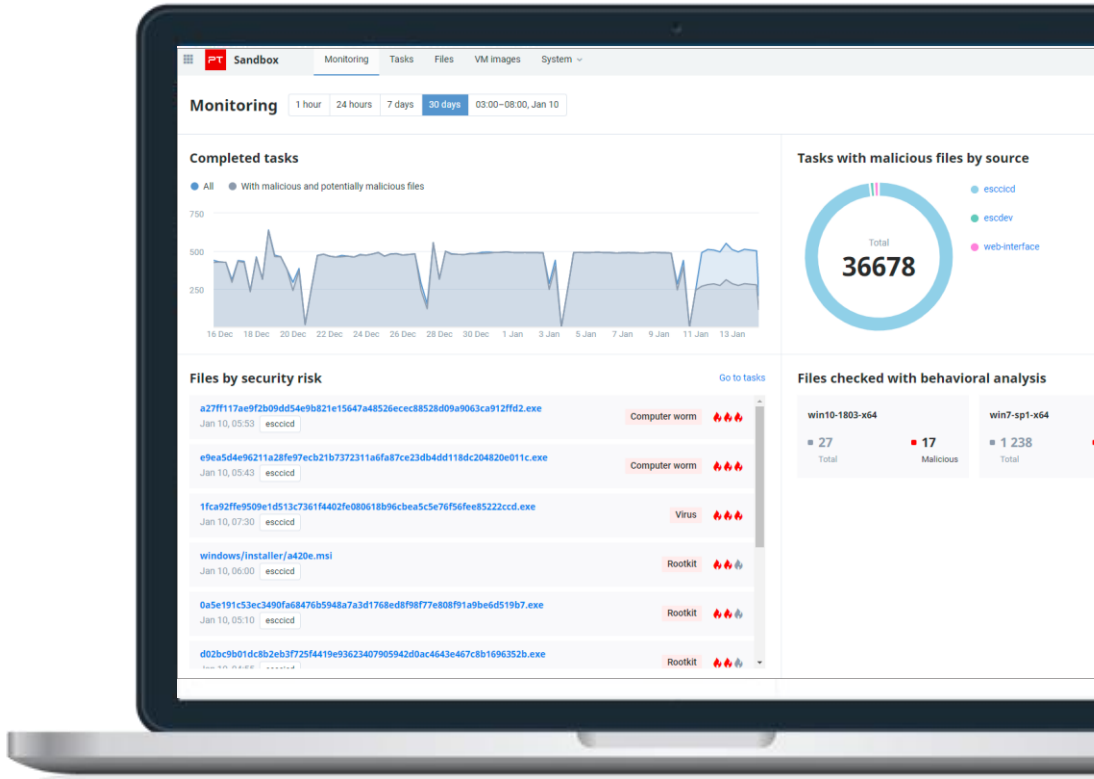
For more information on the techniques covered by PT NAD, visit https://mitre.ptsecurity.com/en-US/techniques/product/pt-nad

PT Sandbox

PT Sandbox

Risk-oriented sandbox with customizable virtual environments

- Protects against targeted and mass attacks, modern malware, and zero-day threats.
- Allows the detection of threats in email, file storages, user web traffic, internal corporate traffic, corporate document management systems, and manual file check portals.
- Analysis of 8500 object behavior traits using machine learning.



PT Sandbox

Customizable protection for businesses

PT Sandbox allows a company to add specific software and its versions to virtual environments. It also uses deception technology: bait in the form of fake files and processes, and data that provokes malware to take action, and reveale its true nature.

Finds threats in files and traffic too

PT Sandbox checks files, analyzes traffic generated during file analysis, and detects malicious activity hidden by TLS encryption. This approach significantly improves the efficiency of attack detection, even in encrypted traffic.

Detects previously unnoticed attacks

Each time the knowledge base is updated, PT Sandbox automatically runs another check of previously analyzed files. This allows you to detect threats hidden in your infrastructure as quickly as possible.

Not just for the corporate segment: an industrial version of PT Sandbox

Industrial PT Sandbox detects threats targeting ICS components (SCADA) and allows you to customize the emulation environment and the employment of decoys to fit the specific network of an industrial enterprise.

PT ISIM

PT ISIM

Is a hardware application performs non-stop monitoring of ICS network security, helps to detect cyberattacks in their early stages, identifies negligent or malicious actions by staff, and promotes compliance with cybersecurity legislation and industry regulations.

Uninterrupted ICS operations

The monitoring architecture of PT ISIM is passive-only. Unlike other popular ICS security products, PT ISIM isolates ICS components from any possible interference.

Automatic ICS network inventory

PT ISIM continuously conducts inventory of the ICS network, monitors its integrity, and notifies of critical changes that may indicate a security concern requiring immediate response.

Pinpoint threat detection

Proprietary database of industrial system threat indicators (PT ISTI) provides insight into most important dangers. Combining this information with signature methods and behavioral analysis, PT ISIM possesses a full range of methods for detecting cyberattacks in earliest stages.

PT ISIM

OT network threat analysis

NTA with deep packet inspection for OT networks

OT network security monitoring

Automatically generates **incident chains** based on traffic analysis in the OT network

OT network visibility

Automatically identifies new hosts, builds connection and subnetwork topologies

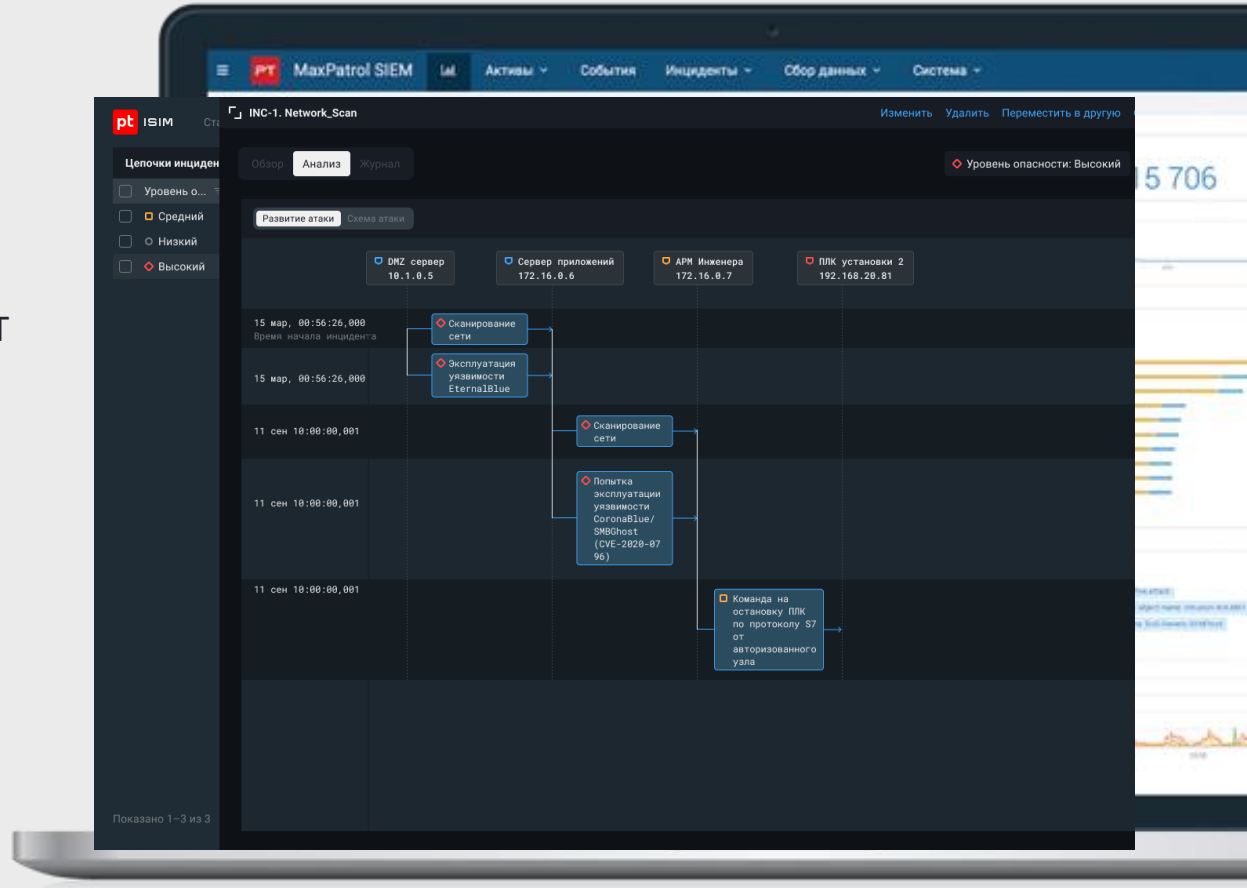
Technological expertise cases

Use of typical hacker techniques and tools

Malware activity in a network

Suspicious network activity

Suspicious actions aimed at violating a technological process



PT ISIM

123 network protocols

80 with open specs

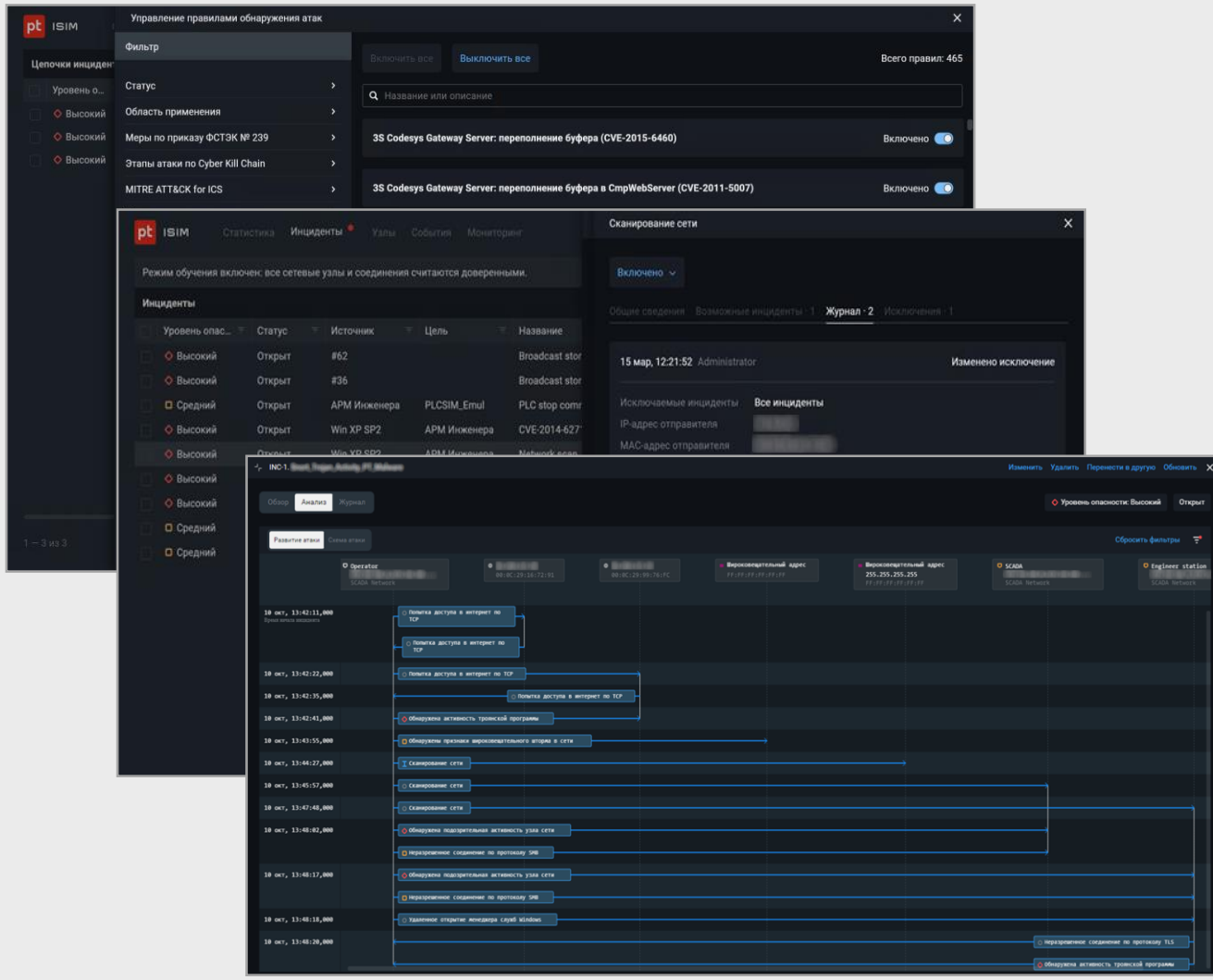
43 proprietary protocols

52 industrial protocols

72 common protocols

23 frame Ethernet-based protocols (non-IP)

100 IP-based protocols



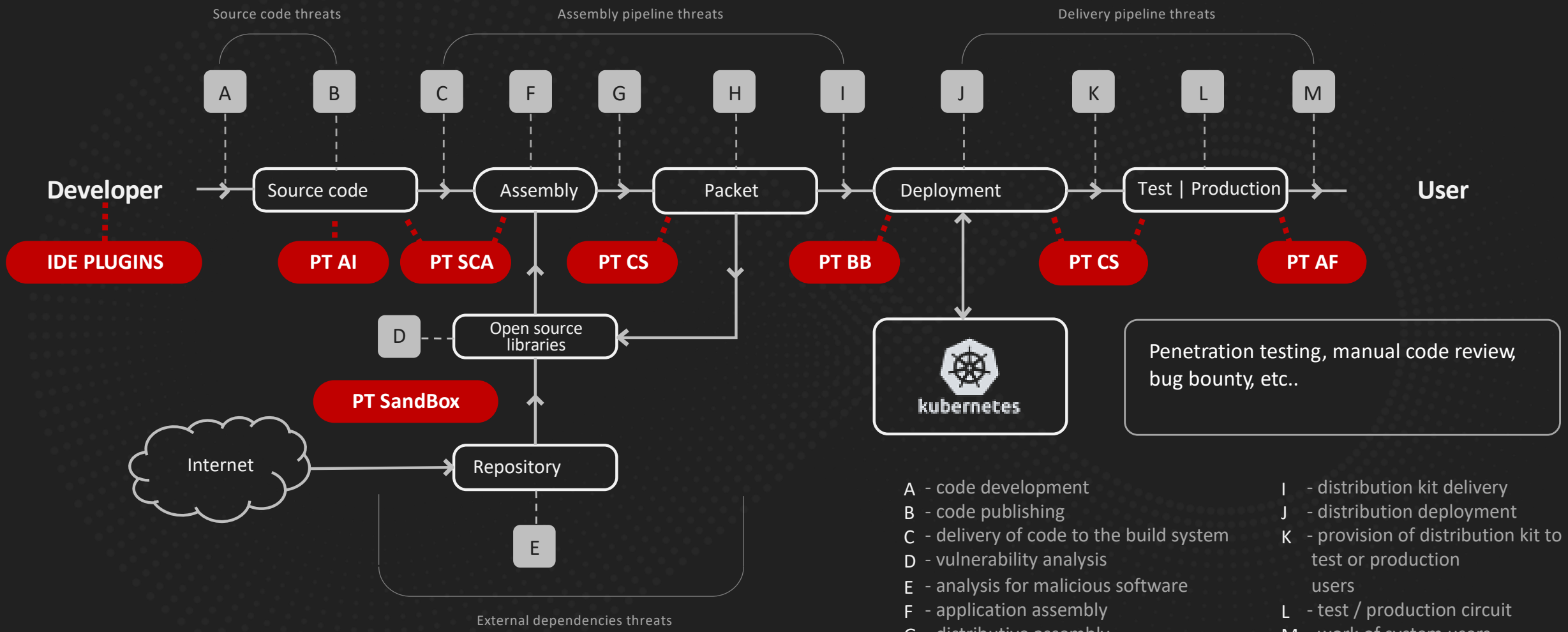
More than 6000 rules and threat indicators “out of the box” – and keeps growing!

ISIM is the sensor for OT. ISIM does not need a 3rd party NTA nor open source (i.e. Suricata).
It’s off-the-shelve product ready for use.

Application Security Suite

- PT Application Inspector
- PT BlackBox
- PT Container Security
- PT WAF

PT solutions for AppSec



Penetration testing, manual code review, bug bounty, etc..

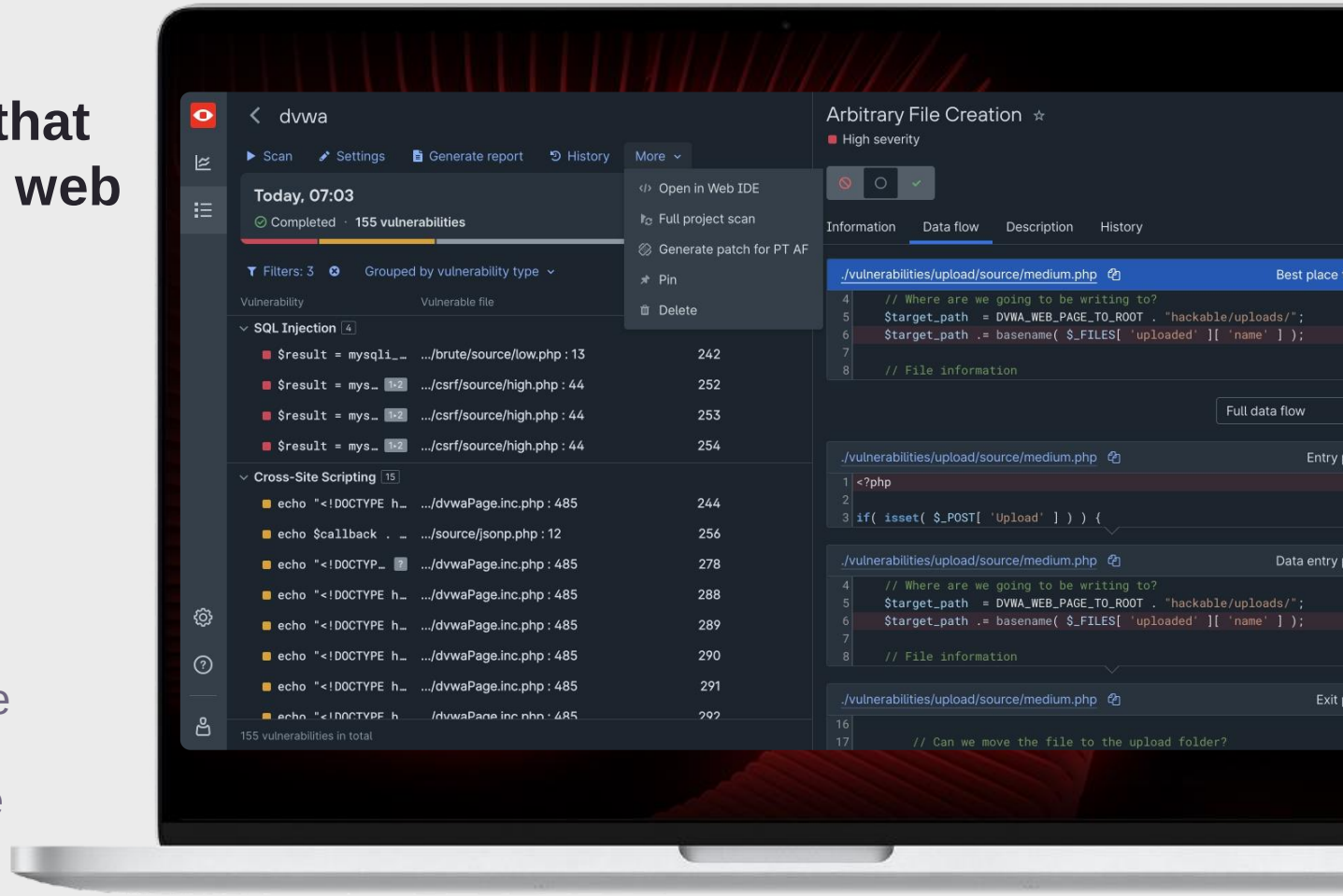
A - code development
B - code publishing
C - delivery of code to the build system
D - vulnerability analysis
E - analysis for malicious software
F - application assembly
G - distributive assembly
H - distribution kit
I - distribution kit delivery
J - distribution deployment
K - provision of distribution kit to test or production users
L - test / production circuit
M - work of system users

PT Application Inspector

PT Application Inspector

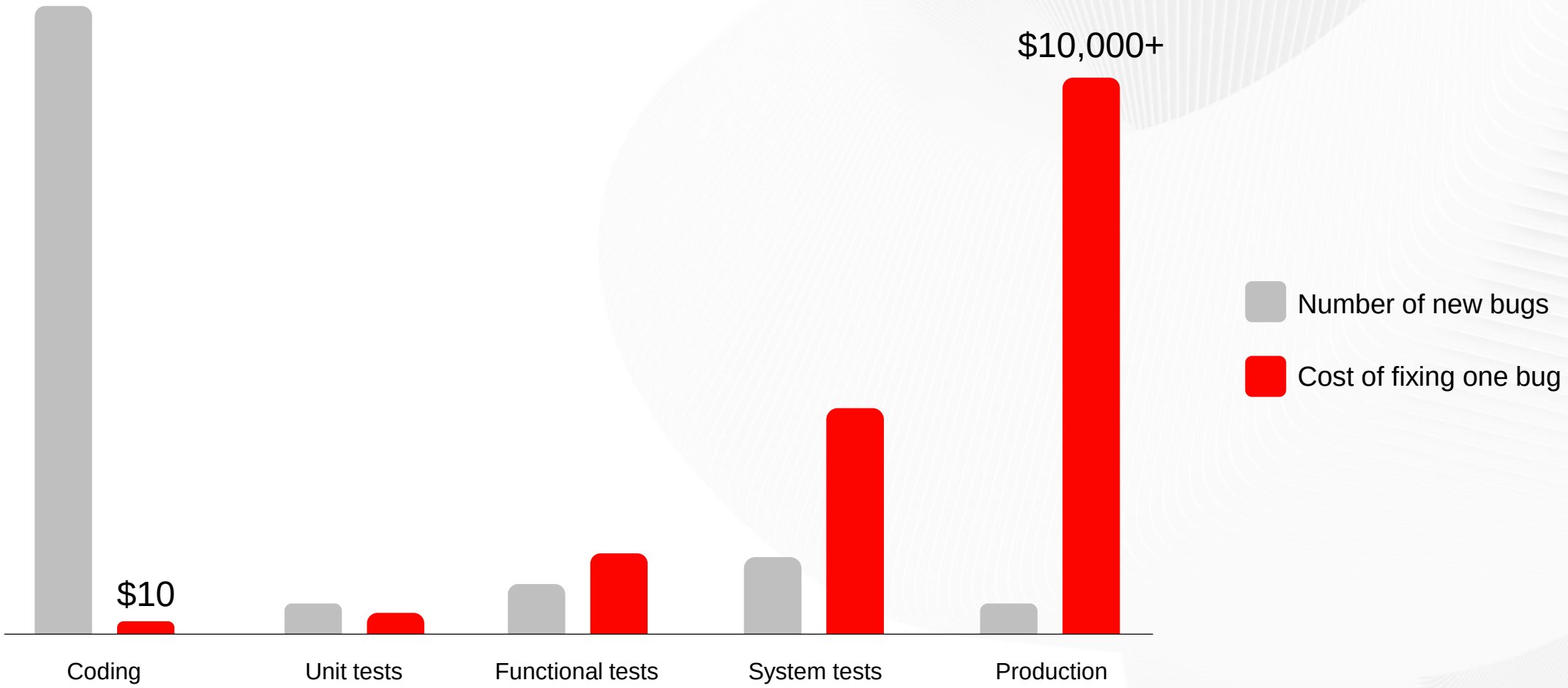
Comprehensive code analysis tool that detects vulnerabilities and errors in web applications

- Allows securing web applications throughout the entire lifecycle.
- Supports secure development processes.
- Reduces cost of remediation thanks to timely detection.
- In order to locate vulnerabilities in source code and in ready applications, PT AI uses a combination of static, dynamic, and interactive code-testing methods (**SAST, DAST, IAST**), and also analyzes side libraries (**SCA**).



The cost of a bug and why you need shift-left

Cost of fixing a defect at different stages of the application lifecycle



PT Application Inspector

Is the right choice for applications of any size and industry

PT Application Inspector is the only static application security testing (SAST) solution providing high-quality analysis and convenient tools to automatically confirm vulnerabilities — significantly speeding up the work with reports and simplifying teamwork between security specialists and developers

A unique combination of scanning methods, plus fingerprint and pattern matching — guarantees accurate results to defend applications everywhere from landing pages to corporate portals, online stores, banking apps, cloud services, Oil&Gas industry, gaming, media, e-government portals

Advantages of PT Application Inspector

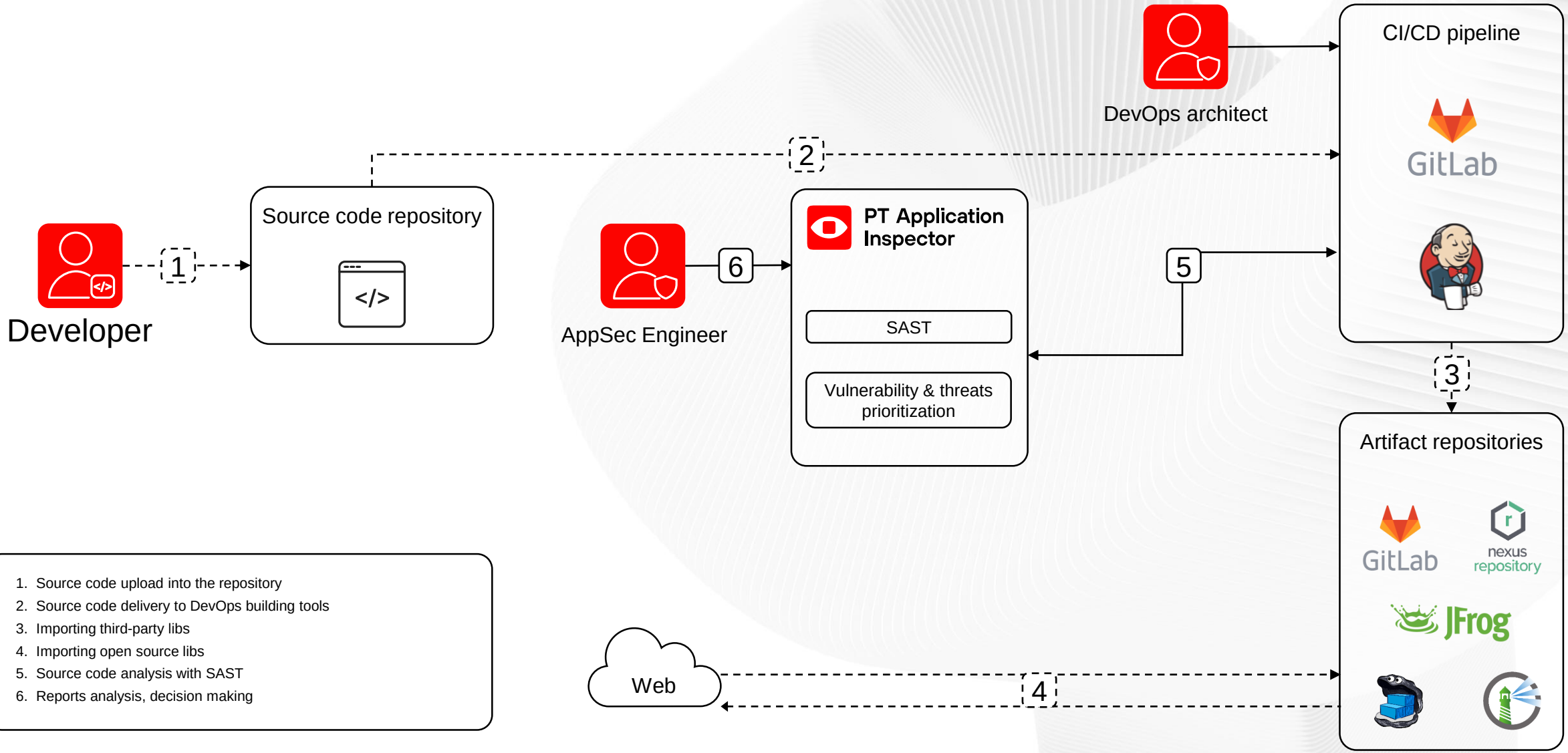
- Detect and confirm security vulnerabilities without a deep dive into source code or the development process
- Make sure that a vulnerability can be exploited before spending time to fix it. PT AI automatically generates safe test requests (exploits) to check it
- Easily collaborate with the development team creating tickets for them with one click

99%
of financial applications
may contain high-risk vulnerabilities

85%
of applications
contain vulnerabilities that enable attacks on users

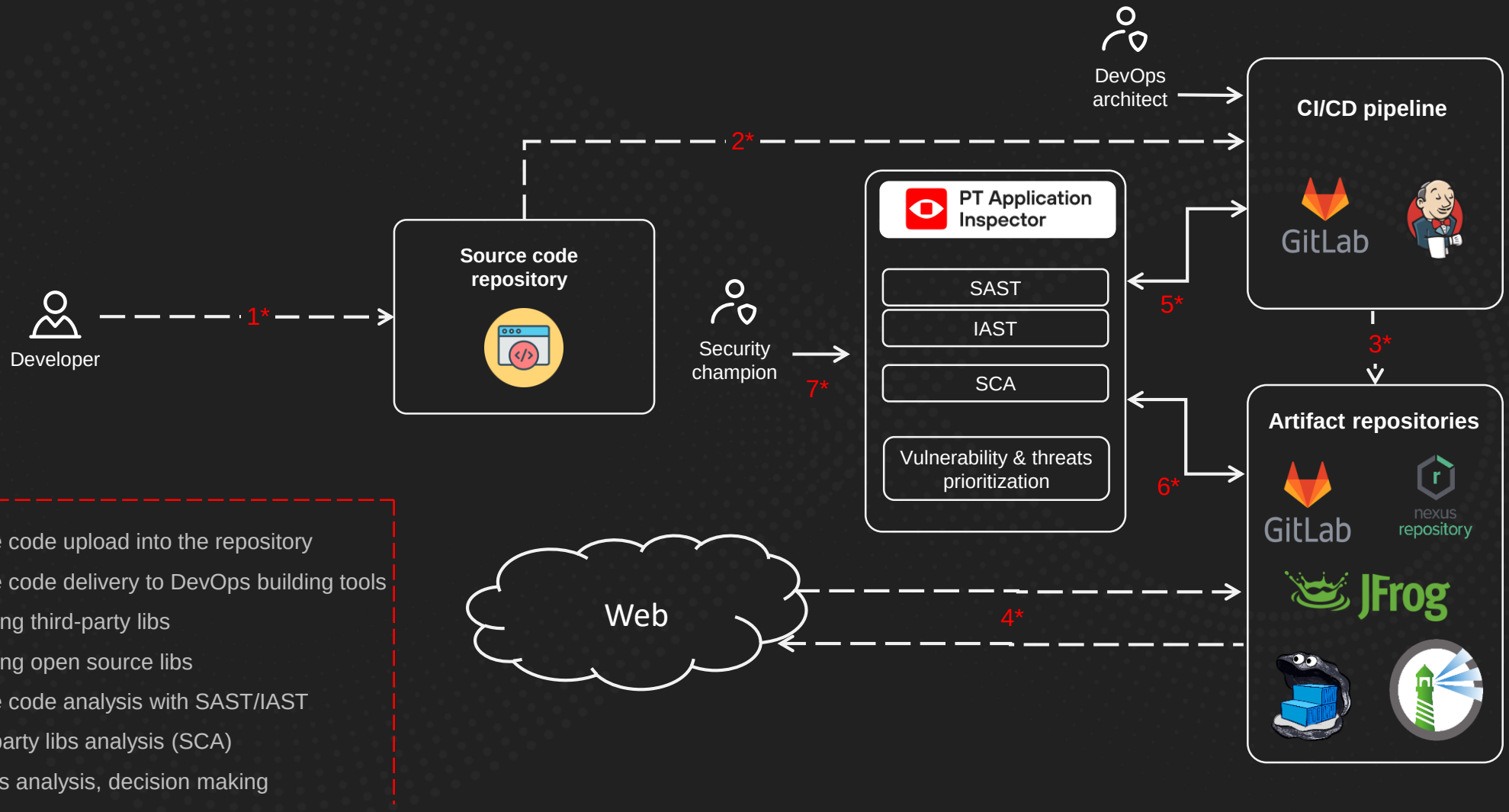
72%
of vulnerabilities
are due to errors in code

PT Application Inspector (SAST@CI/CD)



1. Source code upload into the repository
2. Source code delivery to DevOps building tools
3. Importing third-party libs
4. Importing open source libs
5. Source code analysis with SAST
6. Reports analysis, decision making

PT Application Inspector (SAST)

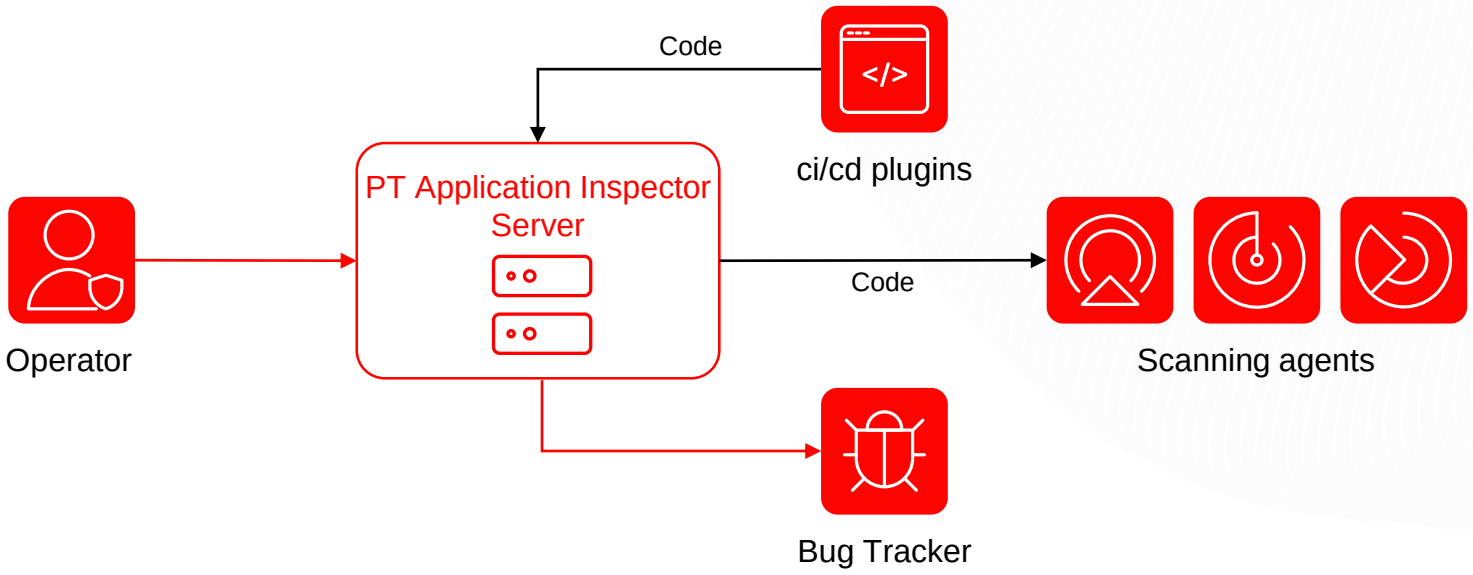


1* - Source code upload into the repository
2* - Source code delivery to DevOps building tools
3* - Importing third-party libs
4* - Importing open source libs
5* - Source code analysis with SAST/IAST
6* - Third-party libs analysis (SCA)
7* - Reports analysis, decision making

Supported languages and integrations

PT Application Inspector is effectively integrated into development processes. It supports integration with Jenkins, TeamCity, GitLab CI, and Azure, with a role-based access control model and ready-made plugins for connecting to application build and delivery systems, bug trackers, and development environments (IDE)

Integration into Security development lifecycle



Supported languages

Java, PHP, C#, Visual Basic .NET, JavaScript, TypeScript, Python, Kotlin, Go, C/C++, Objective-C, Swift, SQL (T-SQL, PL/SQL, MySQL), Ruby, Scala

Deployment: Linux + Docker containers + SSO (SAML, OpenID Connect, LDAP)

CI/CD integration: Jenkins, TeamCity, GitLab CI (CLI), Azure

IDE integration: JetBrains, Visual Studio Code

Bug tracker integration: Jira

API: REST API (Swagger)

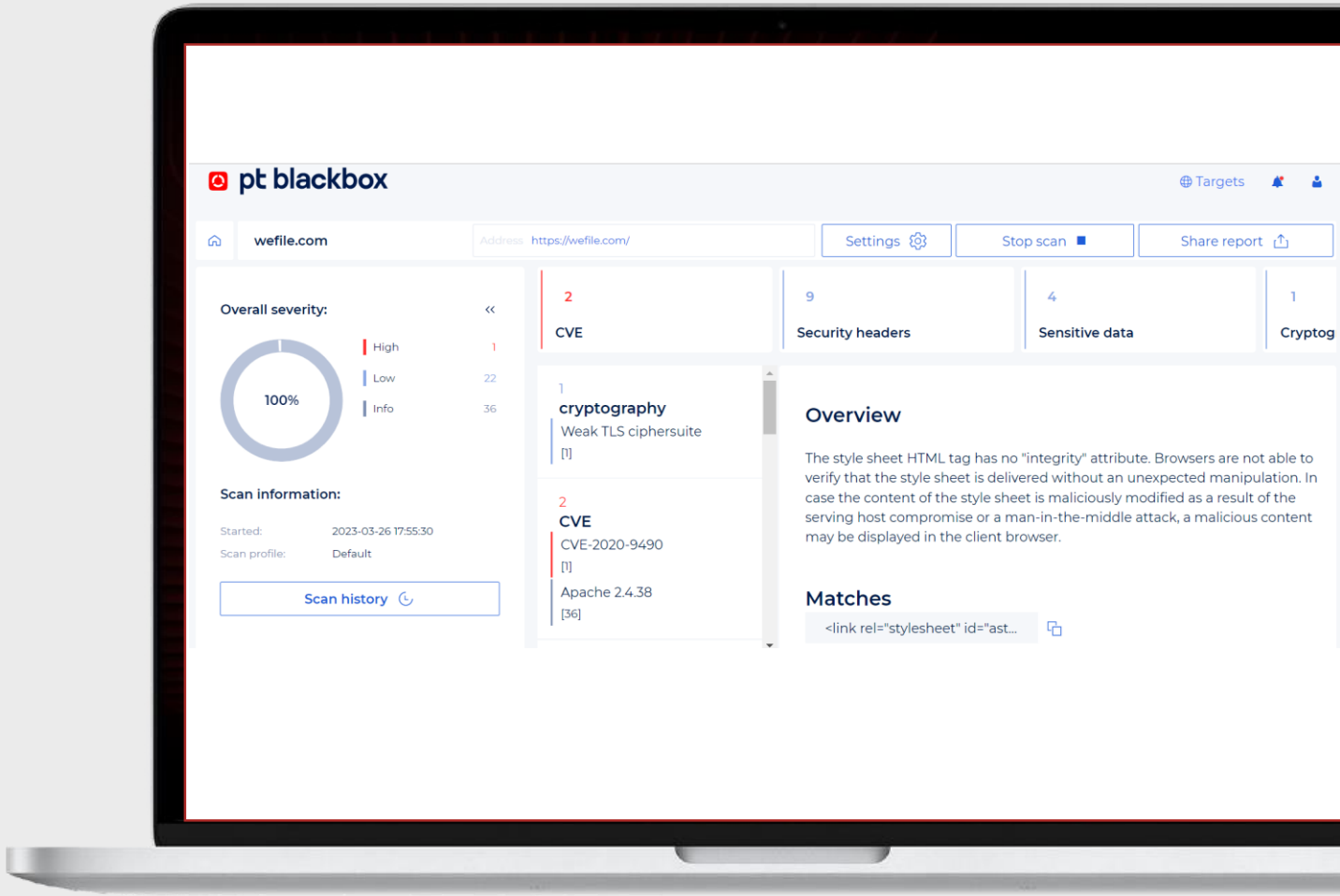
PT Black Box

PT BlackBox

Black-box security scanner for web applications. It makes the job of security researchers easier and provides useful information to help fix vulnerabilities

Can be integrated into the development and release cycle for efficient vulnerability detection and remediation.

- Works based on black-box principle
- Suggests how to fix problems
- Simplifies the work of developers



PT BlackBox

An easy-to-use dynamic application security testing tool that allows you to find and eliminate vulnerabilities at the software testing and delivery stages

Web applications are a popular destination for attackers. Such attacks can result in the spread of malware, redirection of users to malicious sites, or data theft through social engineering

To detect vulnerabilities, PT BlackBox simulates the behavior of an attacker who has no knowledge of the application's inner workings

Advantages of PT BlackBox

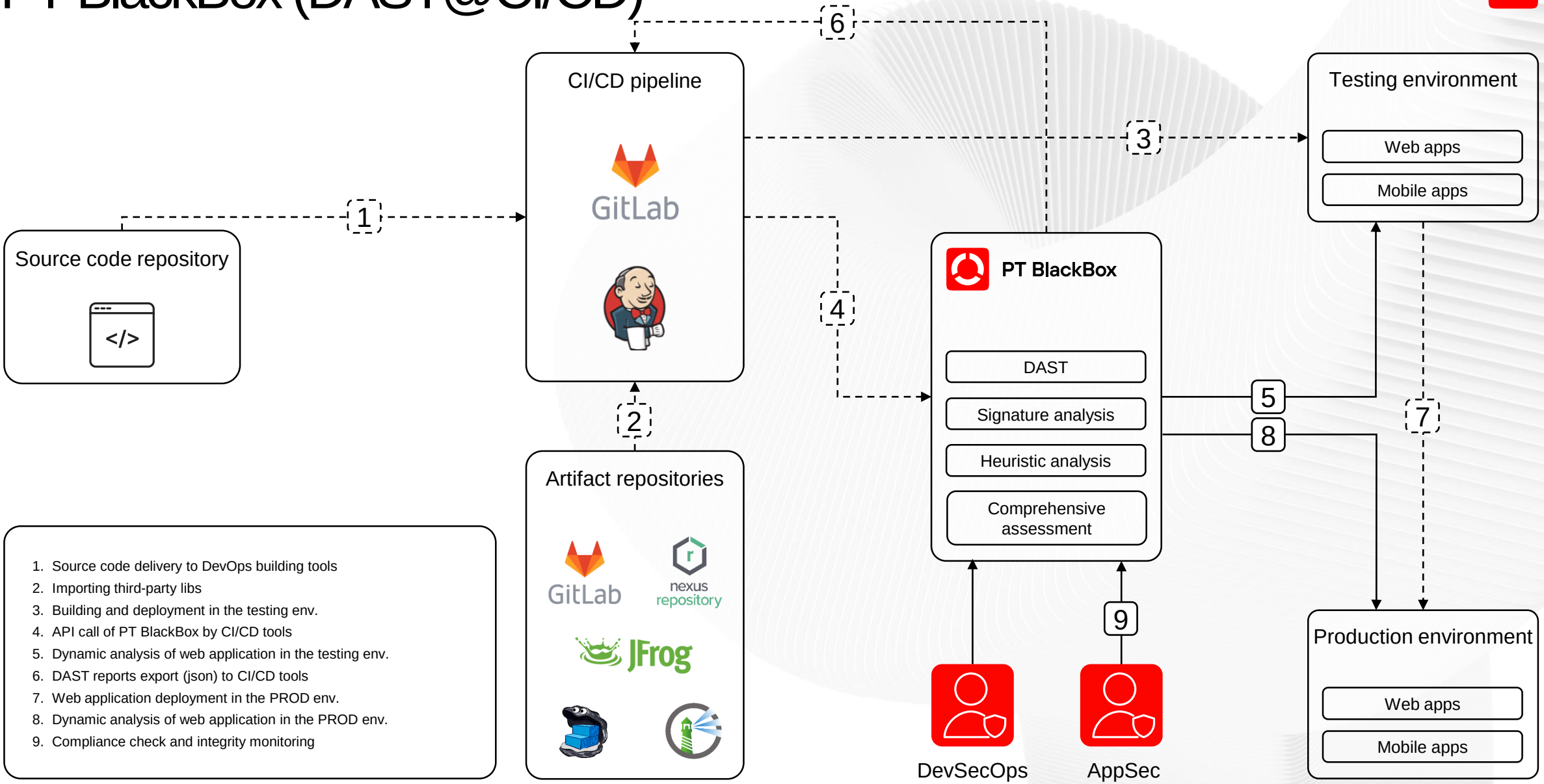
- Lowers resource consumption by recognizing and skipping duplicate pages
- Uncovers hidden threats using a combination of signature and heuristic analysis. Continuously updates
- Can be integrated into the development and release cycle for efficient vulnerability detection and remediation
- Users can customize analysis parameters by fine-tuning scanning and authorization settings
- Scan API for vulnerabilities

98%
of applications
contain vulnerabilities

91%
of applications
allow hackers to steal sensitive data

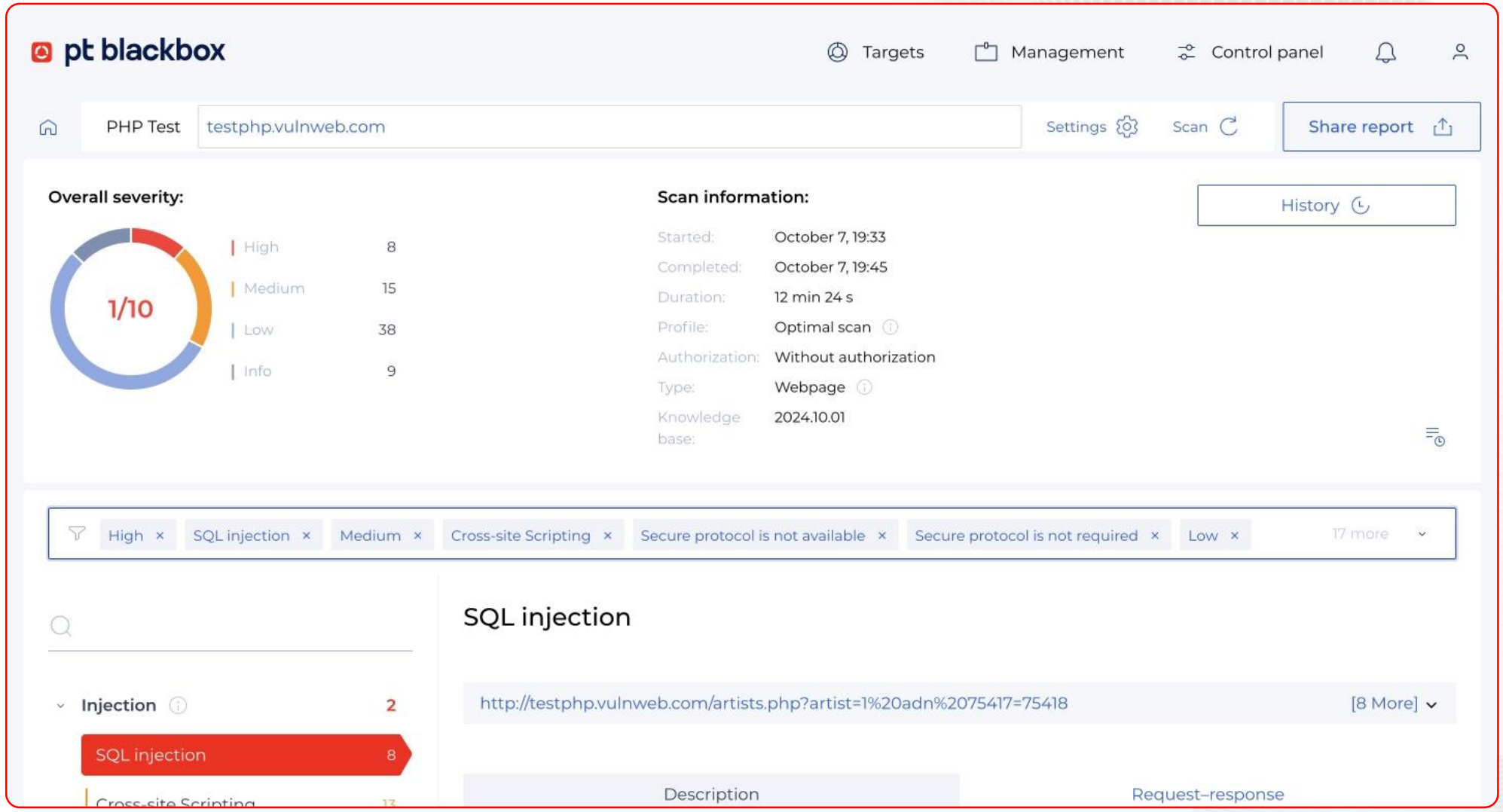
84%
of applications
enable hackers to gain access to web resources

PT BlackBox (DAST@CI/CD)



1. Source code delivery to DevOps building tools
2. Importing third-party libs
3. Building and deployment in the testing env.
4. API call of PT BlackBox by CI/CD tools
5. Dynamic analysis of web application in the testing env.
6. DAST reports export (json) to CI/CD tools
7. Web application deployment in the PROD env.
8. Dynamic analysis of web application in the PROD env.
9. Compliance check and integrity monitoring

Detect and exploit vulnerabilities



PT Container Security

PT Container Security

A high-tech, innovative solution for comprehensive protection of hybrid cloud infrastructures. It supports secure development of software systems that use containerized environment

PT Container Security involves the protection of containers, their infrastructure, and the applications that run in these containers during the build, deployment, and execution phases.
PT Container Security must comply with the organization's policies and processes

90% of IT specialists have encountered at least one security incident related to containers or Kubernetes clusters

81% of organizations have implemented containerization in some form

67% of companies delay the implementation of cloud technologies such as Kubernetes and microservices due to security concerns

Advantages of PT Container Security

A proprietary vulnerability database

maintained by Positive Technologies experts. The database allows you to accurately detect vulnerabilities in Oracle, Red Hat, Ubuntu, Cent OS, SUSE linux, as well as vulnerabilities listed in the NVD database

An expert knowledge base on configuration security

(Kubernetes, Docker, Helm, OpenShift, Podman) that meets the requirements of national and international information security standards, including CIS Benchmarks

A unified risk management approach

for container infrastructures, which involves using specialized risk assessment tools for container/cluster images and configurations, as well as cloud security posture management (CSPM) tools

Practical implementation of the security as code approach, which helps enforce container security policies. In particular, instructions in general-purpose programming languages can be created using WebAssembly

PT Container Security policies can be flexibly configured to include various types of checks such as: Admission controlling, Runtime security, Image and configuration checks

Key PT Container Security features

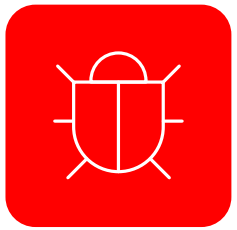


Image vulnerability management

- Image scans in CI
- Image registry scans
- Proprietary vulnerability database
- Monitoring the use of trusted images

Runtime container security

- Monitoring of container activity
- Anomaly detection
- Visualization of interactions
- Blocking of unwanted operations

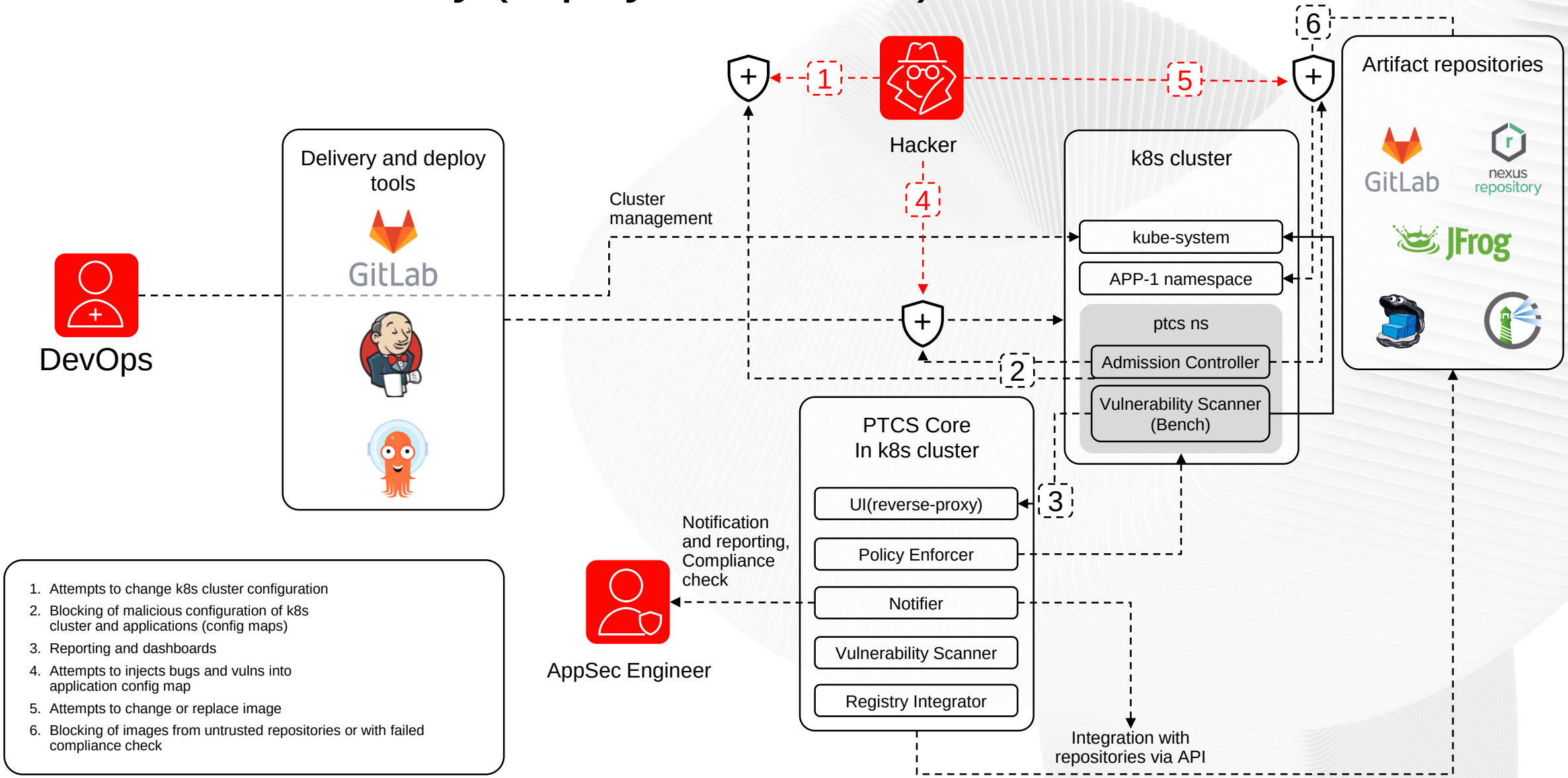
Cluster security

- Protecting clusters from unauthorized configuration changes
- Role-based access control (RBAC)
- Monitoring network policies
- Admission control
- Cluster and node benchmarking

DevSecOps integration

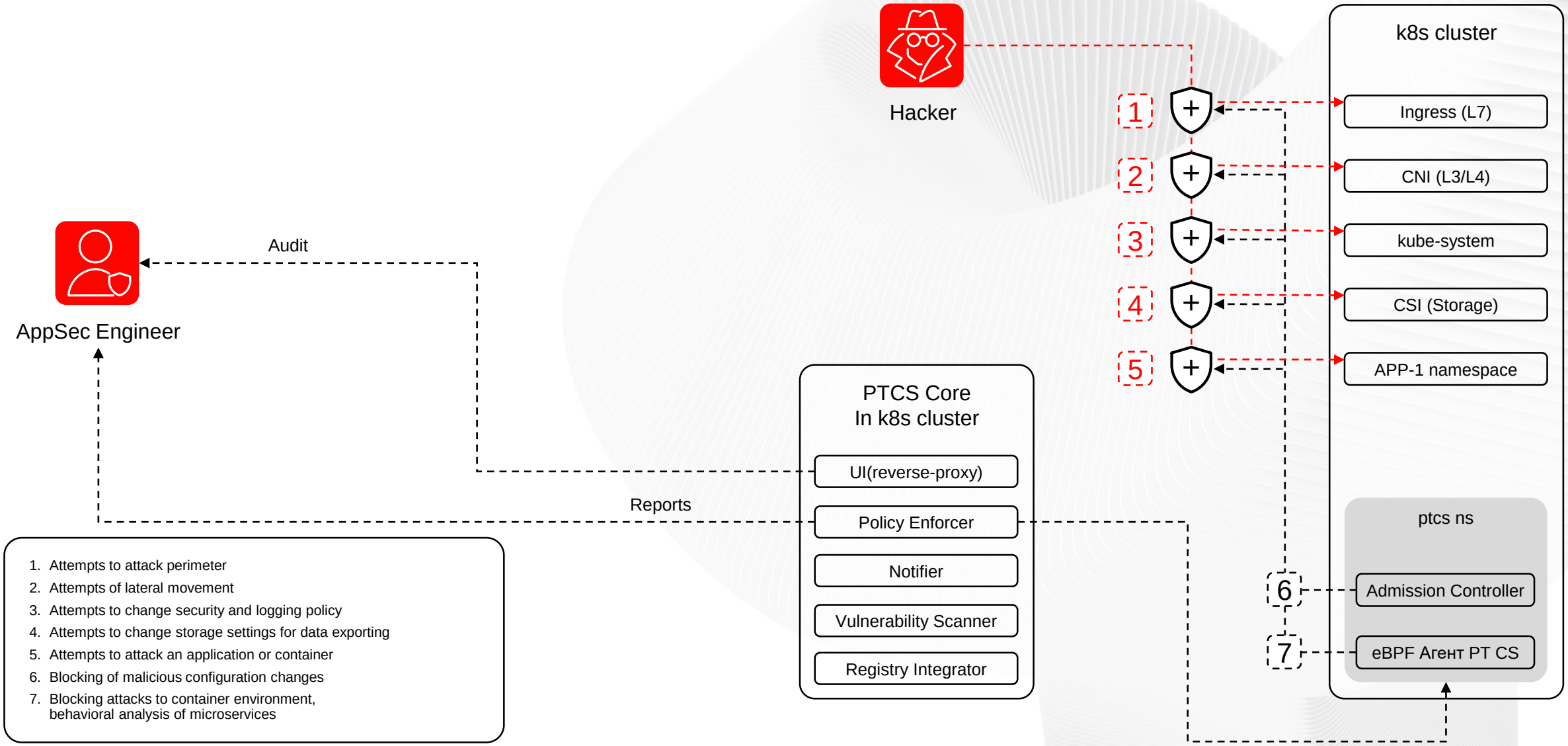
- Integration with Application Inspector SAST/DAST
- Integration with information security monitoring tools
- Integration with collaborative development tools

PT Container Security (deployment control)



1. Attempts to change k8s cluster configuration
2. Blocking of malicious configuration of k8s cluster and applications (config maps)
3. Reporting and dashboards
4. Attempts to injects bugs and vulns into application config map
5. Attempts to change or replace image
6. Blocking of images from untrusted repositories or with failed compliance check

PT Container Security (runtime)

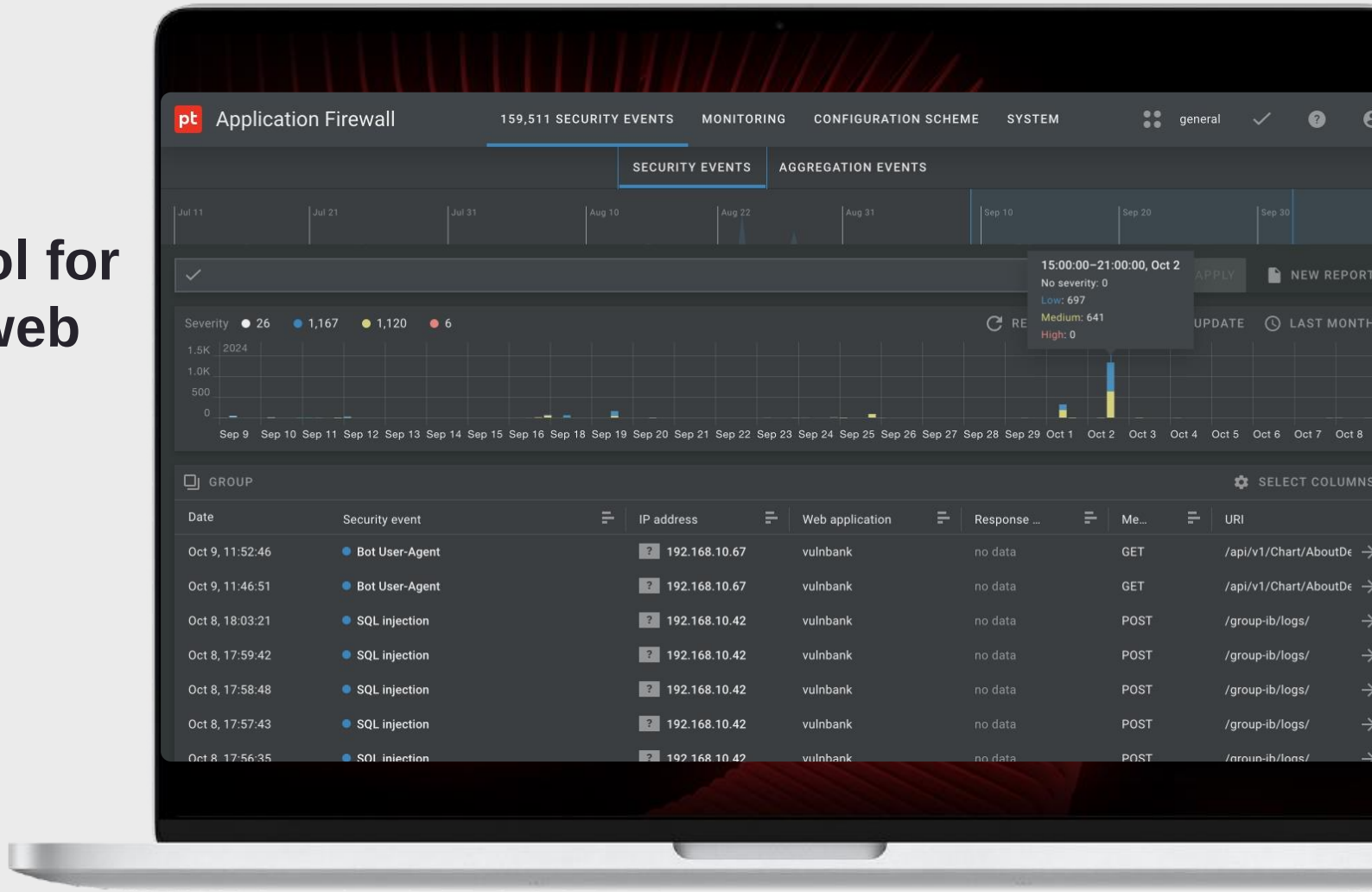


PT Web Application Firewall

PT Web Application Firewall

A flexible and precise tool for total protection against web attacks

Can be integrated into the development and release cycle for efficient vulnerability detection and remediation.



PT Application Firewall PRO

A flexible and precise tool for fully securing applications, APIs, users, and infrastructure against web attacks

Our web application firewall is an innovative protection system that detects and blocks attacks including the OWASP Top 10, WASC, layer 7 DDoS, and zero-day attacks with pinpoint accuracy

It ensures continuous security for applications, APIs, users, and infrastructure while supporting compliance with security standards including PCI DSS

100+
e-banking vulnerabilities
found every year

800+
vulnerabilities
found by us in web applications
every year

72%
of breaches
occur due to web vulnerabilities

$3,86
million is the average cost
of a single data breach

Advantages of PT Application Firewall PRO

PT AF PRO adapts to any web infrastructure and workload

Large companies deploy web applications across different network segments, branches, and subsidiaries. The microservice architecture of PT Application Firewall PRO allows security components to be placed directly in application segments

It requires minimal expenditure on deployment and support

If distributed deployment is required, instead of deploying a full-fledged solution on each site, you can integrate PT AF PRO into the existing Kubernetes-based container architecture or install lightweight modules on your existing nginx web servers

PT AF PRO safeguards against advanced attacks

PT Application Firewall PRO protects web applications and APIs from attacks listed in the OWASP Top 10, blocks malicious bot traffic using Google reCAPTCHA, and limits access to certain web application functions

Use cases

1

Proactive DDoS defense

Profiling with behavioral analysis improves application security - and even allows predicting how an attack will unfold

2

Automatic blocking of zero-day attacks

Multiple techniques, based on ML algorithms, combine to flag anomalies and automatically stop never-seen-before threats

3

Targeted protection

Built-in security scanners, plus PT Application Inspector integration, detect vulnerabilities in application source code and block attack attempts

4

Stopping attacks on users

Application users stay safe thanks to data masking, and granular access settings

5

Pinpoint protection from bot attacks

Modeling of user behavior makes it easy to identify bots and thwart automated attacks without slowing legitimate traffic

6

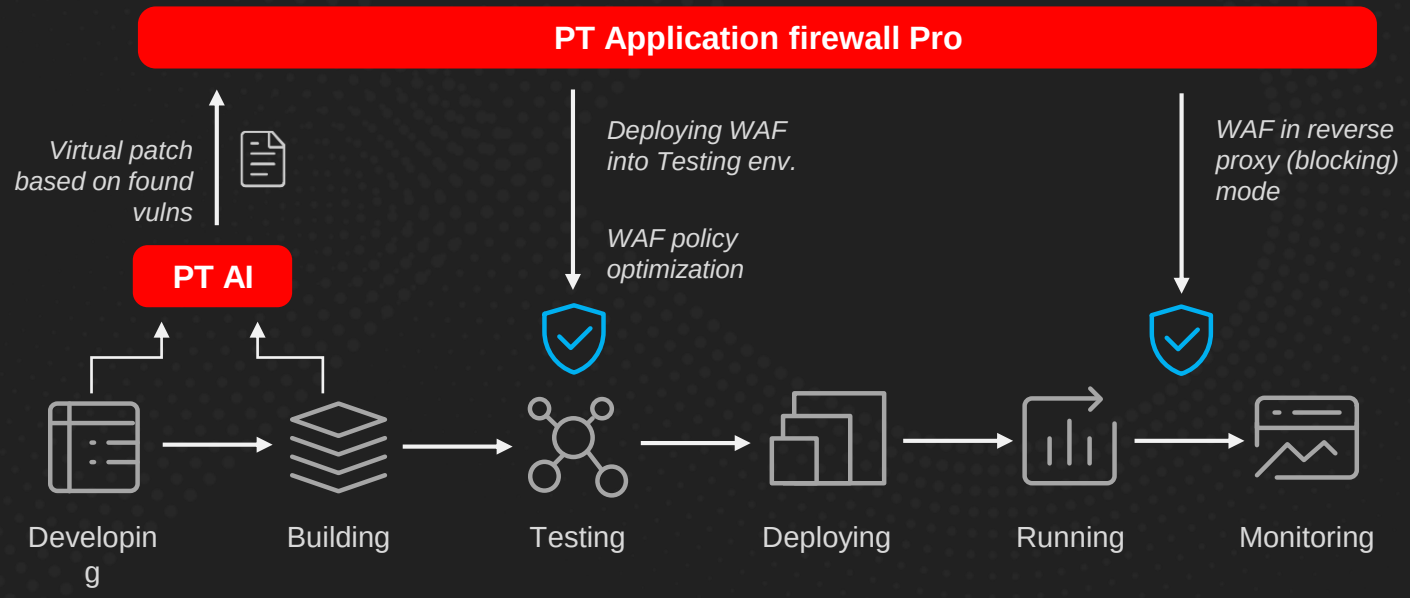
Full security for web and mobile APIs

Threats to web and mobile APIs are stopped by analysis of JSON and XML data

PT Application firewall

> Integration between PT Application inspector (SAST) and PT Application firewall (WAF) enables us to create WAF policies and virtual patches at early stages of Development

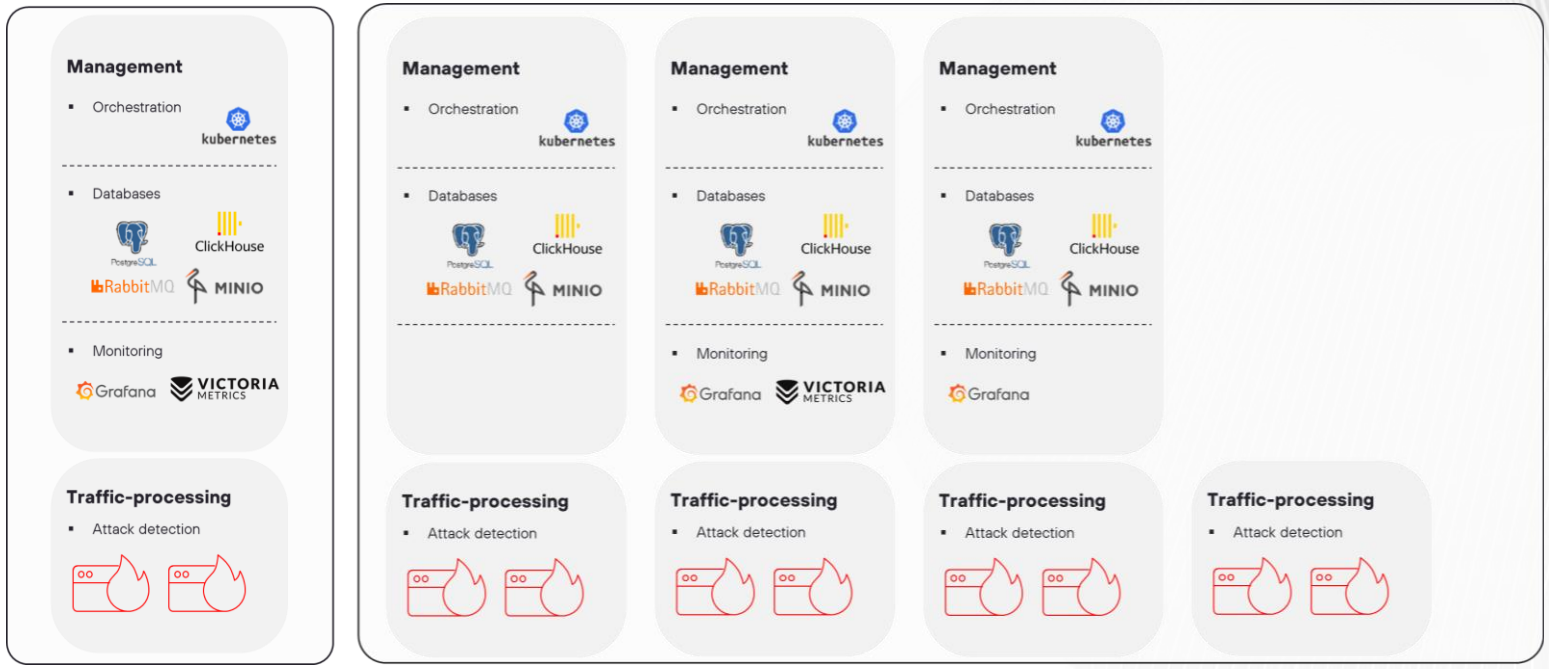
- DevOps-friendly solution
- Deploying applications with known vulnerabilities (decrease of time-to-market)
- No need of profiling and training WAF in PROD environment



Flexibility and scalability

STANDALONE

CLUSTER
ACTIVE—ACTIVE

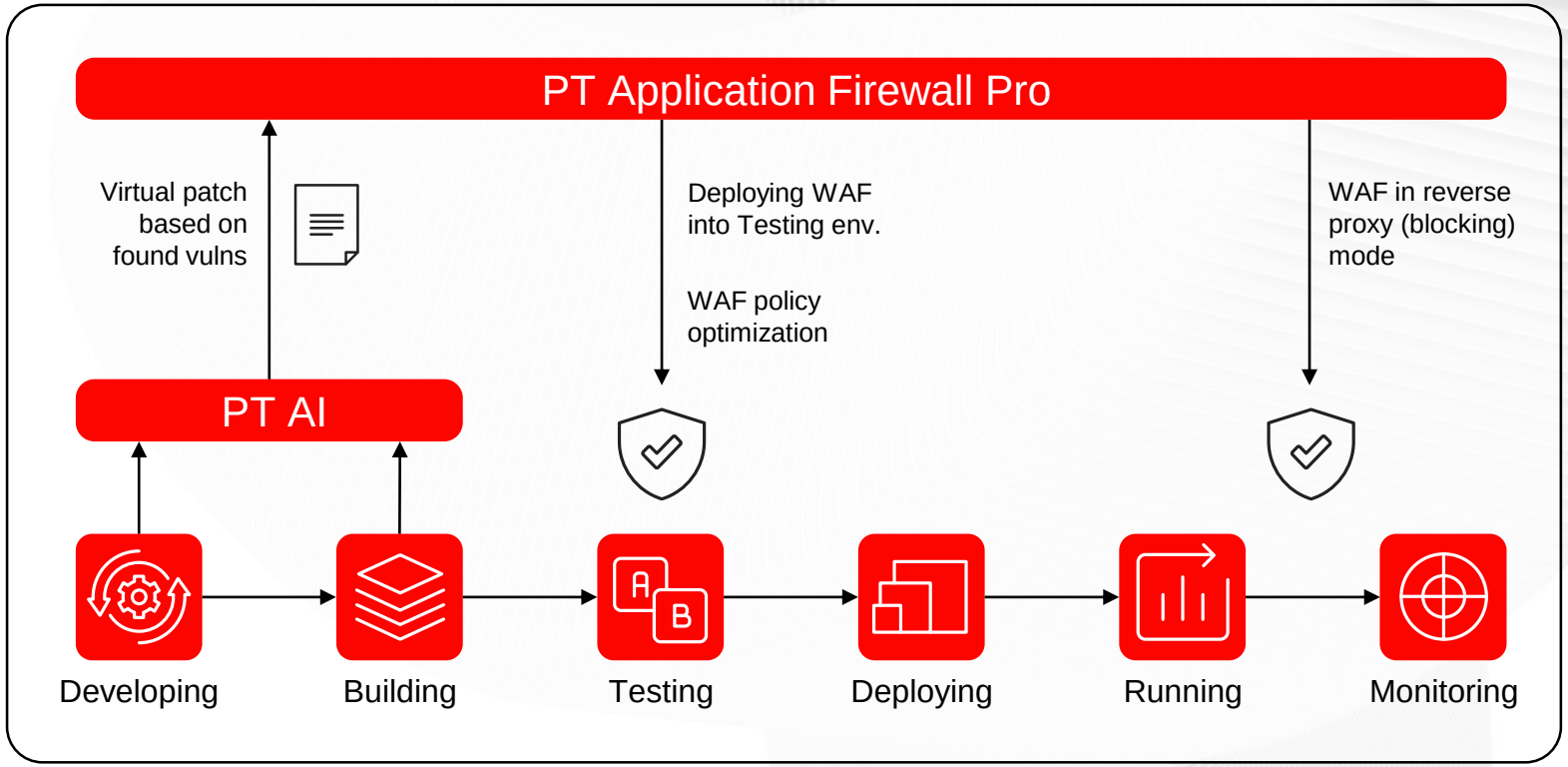


- Flexible deployment: software and hardware appliance, virtual appliance
- Ability to build scalable high-availability active-active configuration with no loss in efficiency and service interruption
- Multitenancy at the basis of the product architecture
- Ability to connect multiple locations using agents or additional traffic-processing servers

SAST integration

Integration between PT Application inspector (SAST) and PT Application Firewall PRO (WAF) enables us to create WAF policies and virtual patches at early stages of Development

- DevOps-friendly solution
- Deploying applications with known vulnerabilities (decrease of time-to-market)
- No need of profiling and training WAF in PROD environment



Services

Forensics services

Positive Technologies Expert Security Center specializes in performing incident response, investigation, and monitoring of corporate systems with PT products

We have 20 years of experience in security assessment, investigation of incidents and activities of major APT groups, and monitoring security at large companies

Manual malware analysis

Get recommendations on mitigation in case of being infected

Retrospective analysis

Detect traces of attack preparation and indicators of infrastructure compromise

Response and investigation

Quickly localize threats and restore operations

Deep security assessments

Penetration testing

Evaluates feasibility of a network breach and associated risks

Security assessment of wireless networks

Enables the boosting of the security of corporate Wi-Fi infrastructure

Online Banking Systems Security Assessment

Evaluates security measures applied to OLB systems

Staff awareness assessment

Helps to strengthen the "human element" against cyberattacks

Security assessment of web applications

Minimizes risk of successful cyberattacks on external and internal network perimeter

OSS/BSS security assessment

Shows how well the given specific telecom management systems are protected from attacks performed by a hacker

Security assessment of mobile applications

Improves the security of your clients' data and prevents fraud

Security assessment of POS/ATM

Assesses physical and logical access to POS/ATM, improves the security posture of POS/ATM

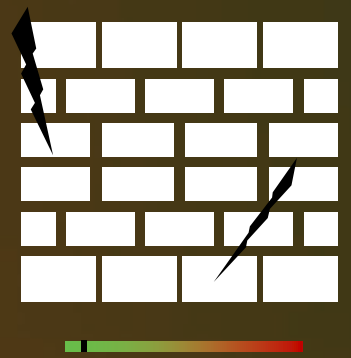
You don’t need secure everything. You only secure what is important from a business perspective.

What is non-tolerable event

Every organization can define cybersecurity events that lead to consequences it is not willing to tolerate. Non-tolerable events are emergency situations that result from malicious activity and lead to the inability to achieve operational and strategic goals or cause long-term disruption of core operations.

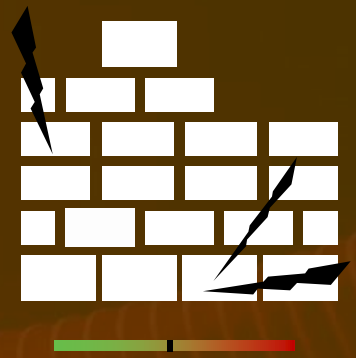
CYBERSECURITY PERFORMANCE

FULLY FUNCTIONAL



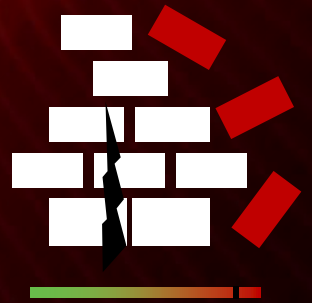
Tolerable damage

PARTIALLY FUNCTIONAL



Damage below the threshold value

NOT FUNCTIONAL



Damage above the threshold value

Non-tolerable events (example)

FINANCIAL LOSSES

Example: 10-15% worth of net profit theft from organization's accounts

BUSINESS INTERRUPTIONS

Example: operational processes failures or shutdowns due to critical IT systems unavailability

DATA LOSS OR UNWANTED CHANGES

Example: unauthorized changes leading to incorrect performance results reporting or failure to achieve them

SENSITIVE DATA LEAKS

Example: large-scale employees', clients', and contractors' personal data leakage, or any sensitive business information leakage

Result Driven Cyber Security (RDCS)

Innovative approach to build end-to-end cybersecurity system to protect from non-tolerable events

Non-Tolerable Events

- lead to unacceptable damage for business defined by business

---

Key elements of the RDCS project

- Cyber Capability
- Adding products and solutions to cover non-protected areas

Cyber Transformation

Enhancing network and processes to make hacker attacks longer and mode difficult

Cyber Resilience

Implementing services that continuously test resilience of the network

Guarantee of results

Guarantee that non-tolerable event won’t happen.

Non-tolerable events by industry

Finance

Disruption of the organization's business processes:

- Disruption of banking services
- Downtime in the operation of corporate infrastructure
- Disruption of systems required for mandatory exchange of information with government authorities
- Disruptions in the operation of the digital ecosystem (of the organization or its partners)

Government

Disruption of the organization's operations:

- Interruption or unavailability of informational services and government services for citizens
- Unavailability of systems required for the duties assigned to government agencies
- Unavailability of systems required for interdepartmental interaction
- Unavailability of emergency public announcement systems or interruptions in their operation

Telecom

Disruptions in communication and broadcasting:

- Disruption of broadcast when it must be running
- Interruptions in broadcasting on a regional scale
- Disruptions in the operation of the digital ecosystem (of the organization or its partners)
- Malfunctioning of telecommunication equipment and disruption of subscriber communications due to hacking of internal infrastructure

Manufacturing

Disruptions in company activity:

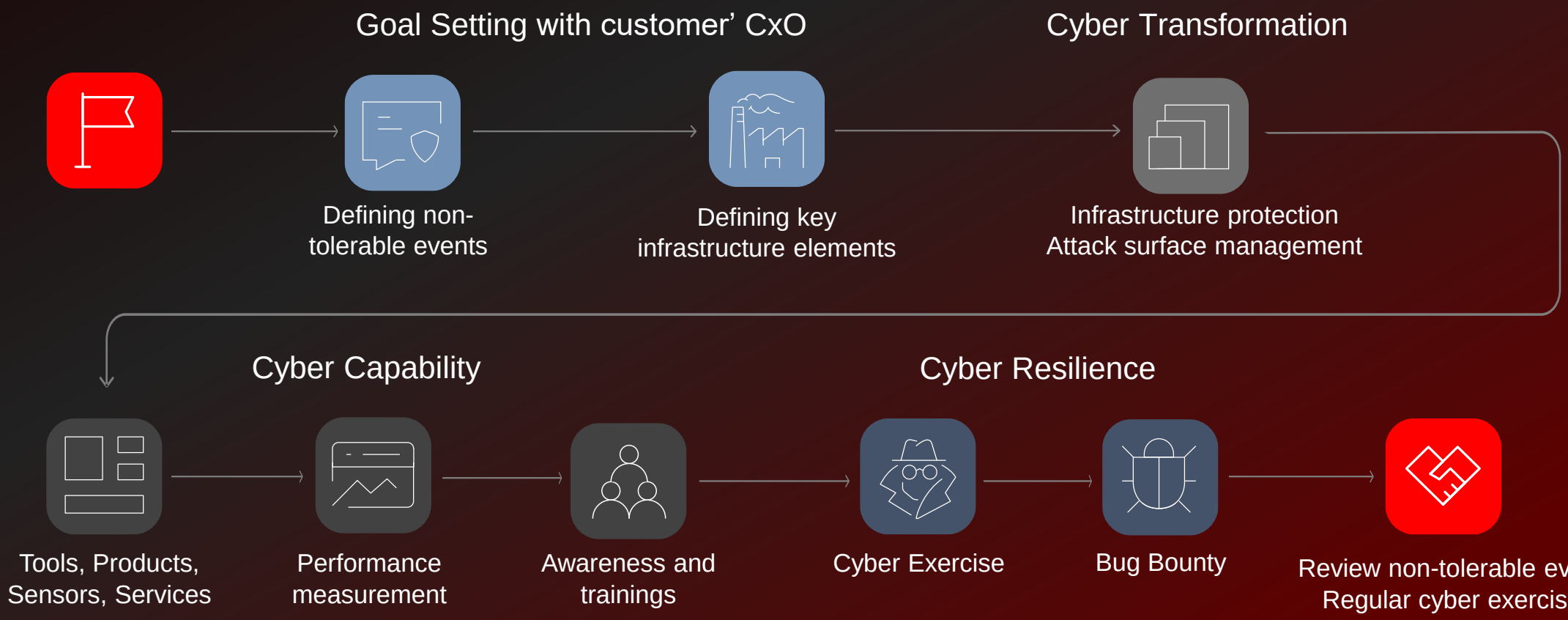
- Disruption or downtime of production facilities and technological equipment
- Downtime in the operation of corporate infrastructure
- Technological accident that causes environmental damage and life-threatening emergencies due to hacking of process control systems
- Production downtime or extensive product defects due to hacking and modifications in the production process
- Disruptions in the operation of the digital ecosystem (of the organization or its partners)

Tech

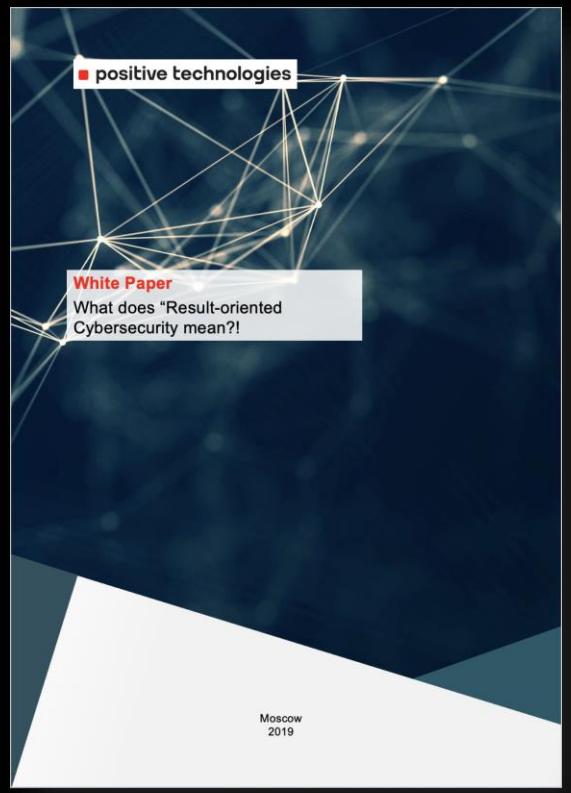
Disruption of the organization's business processes:

- Disruptions or unavailability of client services
- Downtime in the operation of corporate infrastructure
- Hacking of clients' systems through the company's infrastructure
- Failures in software development and delivery of updates to customers
- Disruptions in the operation of the digital ecosystem (of the company or its partners)

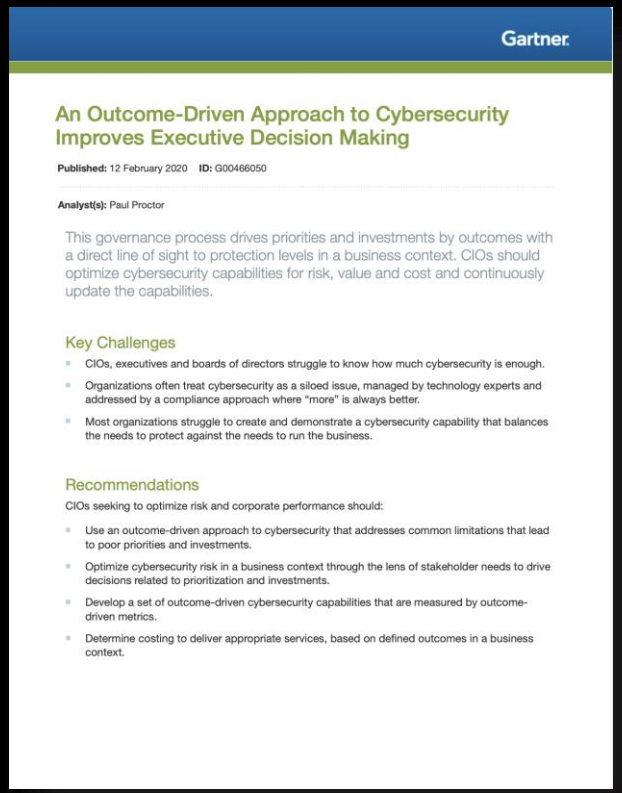
RDCS by PT process and roadmap



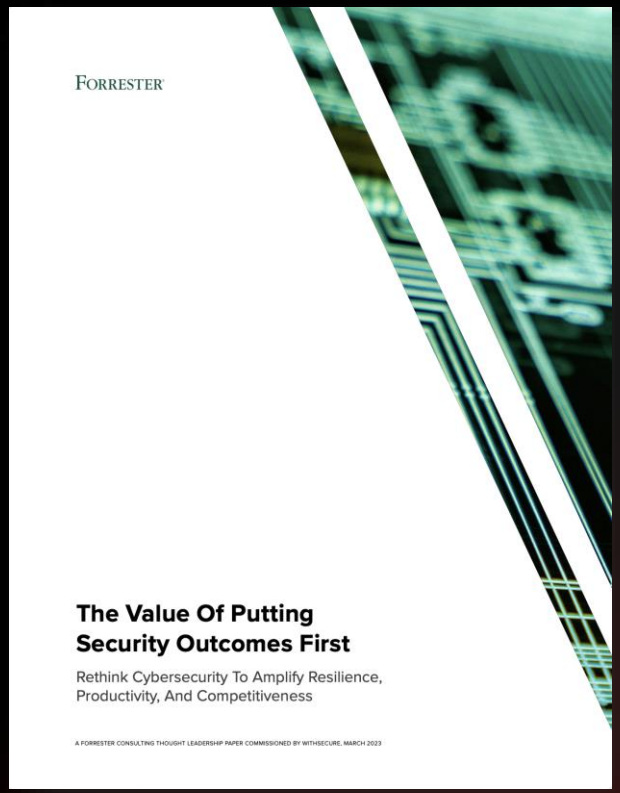
We aren’t alone on this way



Positive Technologies
2019



Gartner
2020



Forrester
2023

Autopilot for RDCS

Growing together

1. **Detects attackers** and determines what assets they managed to reach.

2. **Predicts possible attack scenarios**, including company-specific non-tolerable events.

3. **Stops attacks** before the company suffers irreparable damage.

MaxPatrol O2

MaxPatrol O2 is an autopilot
for results-oriented cybersecurity, which:

- **Detects attackers** and determines what assets they managed to reach.
- **Predicts possible attack scenarios**, including company-specific non-tolerable events.
- **Stops attacks** before the company suffers irreparable damage.

Enables businesses (CEOs) to prevent non-tolerable events, demand specific security outcomes, and continuously monitor the current level of protection.

Enables the CISO to justify and provide understandable for business results-oriented cybersecurity with just one or two employees in the face of staffing shortages, without spending resources on cybersecurity automation.

1

Enables companies to address challenges of results-oriented cybersecurity without expanding their expert team or spending resources on automating SOC processes.

2

Suggests what non-tolerable events the suspicious activity may lead to, and how many steps are left until the risks materialize.

3

Provides the operator with collected chains of attacker activity with full context.

4

Considers risks to business processes and offers an optimal response scenario automatically or manually, if adjustments are needed.

5

Utilizes Positive Technologies unique expertise gained in regular cyberexercises, Bug Bounty Positive Dream Hunting, and Standoff.

6

Brings together Positive Technologies products that function as sensors, exchange knowledge, and provide comprehensive IT system protection with minimal human involvement.

PT is a strong vendor to ally

Fundamentals of Positive

White hackers Expertise

Offensive and defensive services

PT ESC: Incident Response, Threat Research
PT SWARM: Security Research Team

Offensive

- Web and mobile application assessment
- Complex penetration testing (any system)
- Red Team
- Bug Bounty platform

Defensive

- Incident investigation
- Compromise assessment
- Malware analysis
- Monitoring/Blue team

Combination

- Cyber trainings

Technologies & Expertise

Wide range product portfolio and unique threat content

Result-driven approach

Approach that makes non-tolerable events impossible to reach

Contacts

Egor Rykov

Head of Business Development in Iran

erykov@ptsecurity.global