positive
technologies

LEADER IN RESULT-DRIVEN CYBERSECURITY

POSITIVE TECHNOLOGIES

PROTECTING THE WORLD FROM NON-TOLERABLE EVENTS* WITH THE LATEST TECHNOLOGY

1

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security products and solutions.

Our mission is to safeguard businesses and entire industries against the threat of cyberattacks.

Who we protect

Critical national infrastructure

- Government
- Bank
- Industrial
- Global Events
- Healthcare
- Telecom

2

Positive Technologies**' global experience and expertise** covers almost all continents and regions, including MENA, LATAM, South- East Asia, India, China, and Africa.

3

Global Events

- Sochi Olympic Games
- FIFA World Cup
- Phygital Games of the Future

Publicly traded	MOEX: **POSI**
R&D in cyber security, years	22+
Customer Count, worldwide	4k
Creative environment, specialists and experts	2.8k
Leading integrators as partners	300+

*Non-tolerable event – an event resulting from a cyber attack that makes it impossible to achieve an organization's operational and/or strategic goals or that results in significant disruption to its core business

WHY POSITIVE TECHNOLOGIES?

1

Result-driven cybersecurity

Stop justifying your security budget! PT products provide measurable protection, giving you the data you need to make informed security decisions

2

Expertise

Fueled by real-world insights from penetration testing, forensics, and cyber investigations, our products are built to effectively identify and thwart cyberattacks

3

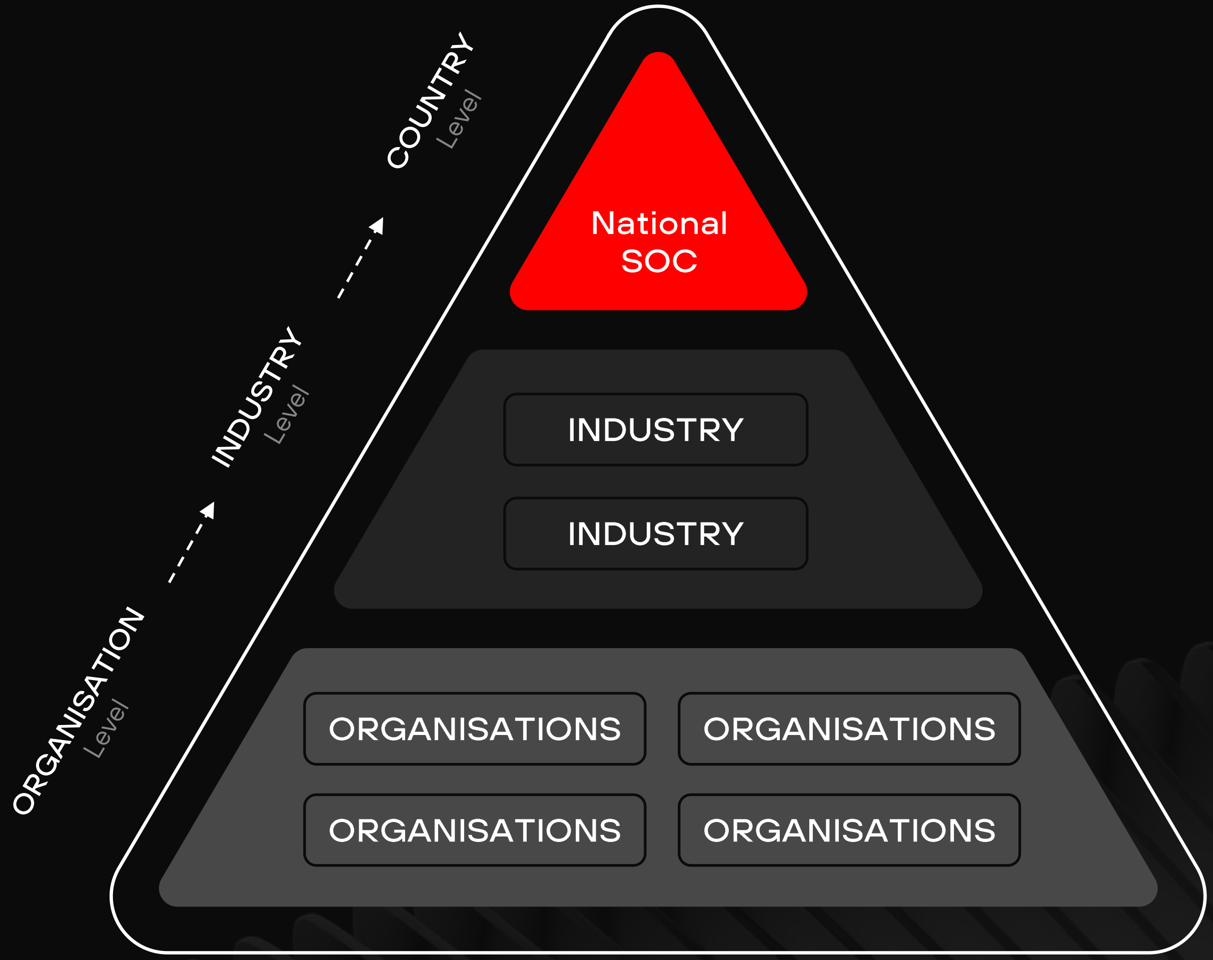
Secure future

We constantly look for new ways to accumulate knowledge about hacking tactics and techniques in order to improve our products and technologies

WE BUILD CYBERSECURITY AT ANY LEVEL

We create corporate, industry, and national cybersecurity centers based on our own products and solutions.

Qualitative results-based performance indicators



WORLD-CLASS TEAM

ETHICAL HACKERS AND CYBERSECURITY EXPERTS AT YOUR SIDE

1

Positive Technologies teams detect and investigate attacks, identify vulnerabilities in your perimeter, and minimize incident impact—preventing financial losses and protecting critical data.

2

The attack team **PT SWARM** simulates real-world hacker tactics.
On the defensive side, **PT Expert Security Center (PT ESC)** tracks threats, investigates behavior, and refines defenses to stay ahead of emerging risks.
PT ESC is the largest expert security center in Eastern Europe.

3

Our company is known globally as a visionary leader in ethical **security research.** For over 22 years, our team of experts has been ahead of the curve on the latest industry threats and trends, and we're always looking for ways to improve our solutions and services.

PT SWARM

Ethical hackers develop and execute attacks, acting like real cybercriminals with 99% success rate

PT ESC

Works in collaboration with the company's cybersecurity team to repel attacks in real-time

300+

Corporate system security audits conducted each year

200+

Security experts in Incident Response, Threat Intelligence, Detection Engineering, SOC, Anti-malware Lab

250+

Zero-day vulnerabilities identified over the past 3 years

5 APT

Groups uncovered annually

STANDOFF

LARGEST CYBER BATTLE IN THE WORLD

Unparalleled interactive Standoff 365 model city 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
- 20+ teams of hackers from around the world compete
- Top-notch researchers test how well the virtual State F's infrastructure is protected

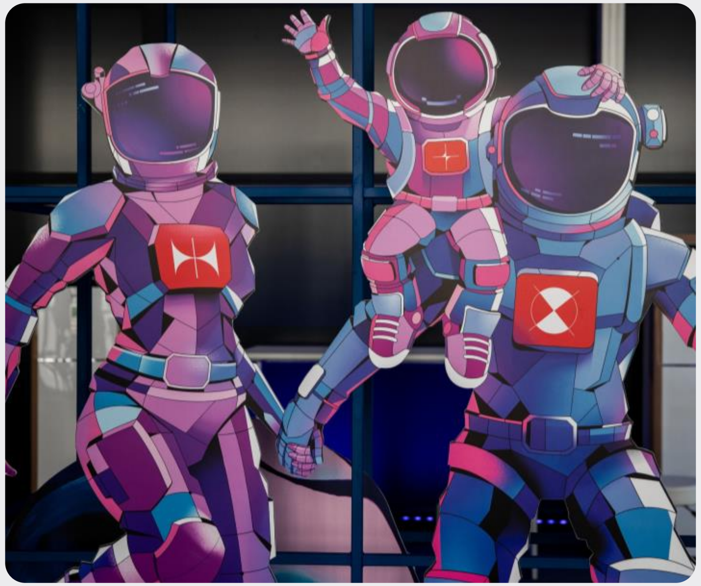
OUR FLAGSHIP PROJECTS

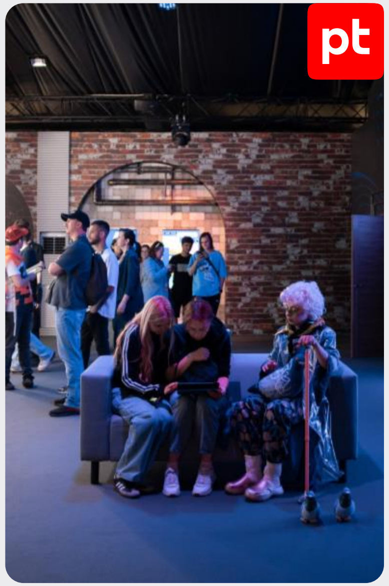
BUILDING THE CYBERSECURITY COMMUNITY

phd Positive Hack Days Fest

An international cyberfestival for those who want to dive into the world of cybersecurity

An international forum on practical security held in Moscow annually since 2011. PHD hosts hundreds of talks and workshops, covering the most interesting topics in information security





SECURITY RESEARCH

Quarterly reports on the latest cyberthreats and trends, forecasts and investigations of hacker activity, industry-specific information.

positive

SECURITY
EXPERTISE
PENTEST
PROTECT
ANALYSIS
PREVENT
DETECT
THREAT

2022 Сборник исследований по практической безопасности рус

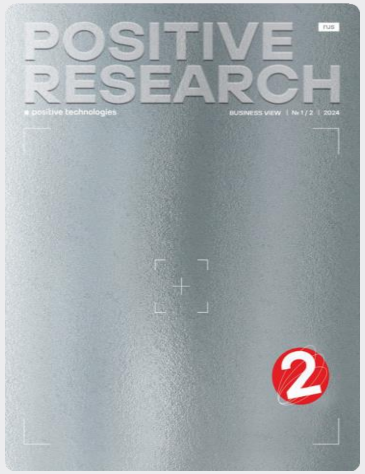
POSITIVE RESEARCH rus

positive technologies TECHNICAL GUIDE | № 2 / 2023

NEW

POSITIVE RESEARCH rus

positive technologies BUSINESS VIEW | №1 / 1 | 2024



POSITIVE RESEARCH rus

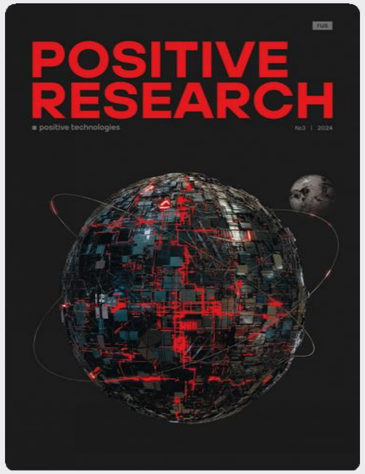
positive technologies BUSINESS VIEW | № 1 / 2 | 2024

2

eng

POSITIVE RESEARCH

positive technologies №3 | 2024



POSITIVE RESEARCH rus

positive technologies №3 | 2024

200+

all security research since 2002

44

security research in 2024 including digests of trending vulnerabilities

positive
technologies

CYBERSECURITY LANDSCAPE

TYPICAL CHALLENGES IN CYBERSECURITY

1

Dependency is growing

Cyberthreats are a source of a wide variety of business impacts due to the growing dependency on sophisticated IT technology, and must be appropriately managed

2

Needs for diversity

A high concentration of suppliers from one country or region can aid attackers and increase vendor dependence

3

Lack of trust

Auditors' reports, certificates of compliance, or analysis of cyber defense maturity do not provide the maximum degree of confidence in cyber resilience

4

High cost of talents

The lack of cyber professionals forces companies to raise pay or put up with the shortage and take extra risks

TYPICAL CHALLENGES IN CYBERSECURITY

How we guarantee maximum cyber resilience

Our solutions are based on 22 years of research, experience, and expertise of hundreds of information security experts. Positive Technologies products and services ensure cyberattacks don't disrupt the critical operations and strategic objectives of businesses and governments.

What is result-driven cybersecurity?

Positive Technologies detects and prevents attacks automatically before non-tolerable damage is done to the company. We conduct cyberexercises and publicly test our products to demonstrate that the result-driven approach to information security truly works.

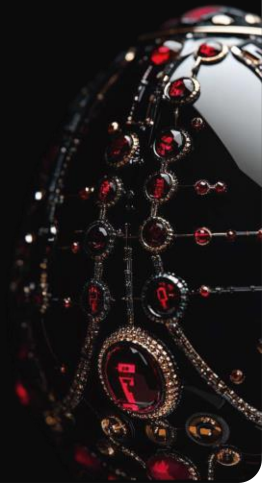
KEY PRINCIPLES OF RESULT-DRIVEN CYBERSECURITY

TIME TO RESPONSE < TIME TO ATTACK

For a cyberattack to never be successful, defenders must spend less time on detection, containment, and elimination than threat actors spend on attacks

Cyber resilience must be proven

You face a choice: withstand simulated attacks or be a long-term target for highly skilled hackers pursuing your prized assets



What you get as a result

Transparency
Diversity
Independency
Efficiency

RESULT-DRIVEN CYBERSECURITY APPROACH

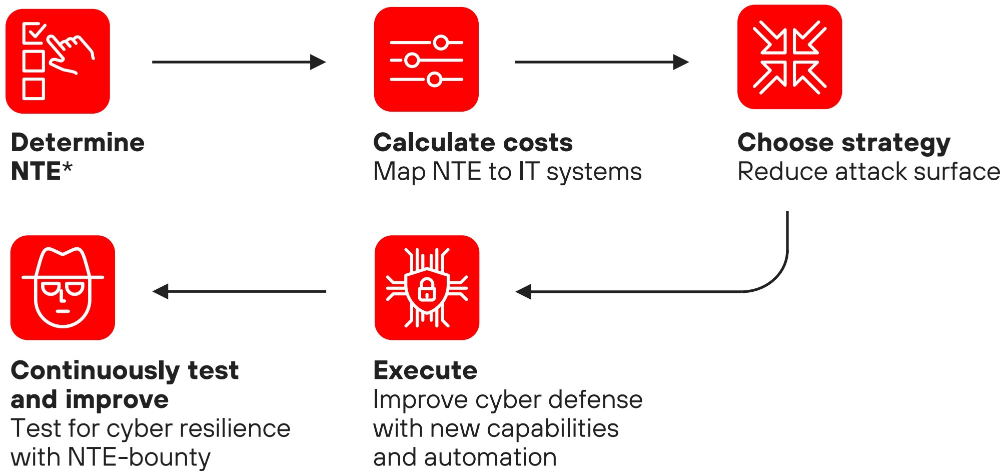
1

Typical challenges

- Cyber dependency is growing
- Needs for cyber diversity
- Lack of trust in cyber defense
- High cost of cyber professionals

2

How it works



Determine NTE*

Calculate costs
Map NTE to IT systems

Choose strategy
Reduce attack surface

Execute
Improve cyber defense with new capabilities and automation

Continuously test and improve
Test for cyber resilience with NTE-bounty

*NTE - non-tolerable events

OUTCOME OF A CYBERATTACK WITH SEVERE CONSEQUENCES TO **CORE BUSINESS**

Examples

- $X million stolen
- X personal data records stolen
- Online banking in operational for X hours
- Transactions stopped for X hours

WE HELP MAKE THE RIGHT DECISIONS

Should we invest in security?

Should we invest in security?

How much to invest?

We compare marginal cost and marginal benefit of investment.

What should we invest in?

We estimate ROI for multiple security measures and find the best route.

Is security investment cost-effective?

We determine Expected Net Benefits with the new measures, and probability of attack.

Results-Driven Cybersecurity

WHAT YOU GET AS A RESULT?

Processes, technical controls, configuration and integration for a secure development

OUR PORTFOLIO

PRODUCTS

Infrastructure security

PT Network Attack Discovery (NDR)
Early detection of threats and targeted attacks in network traffic

MaxPatrol VM
Next-generation vulnerability management

Application security

PT Application Inspector
Comprehensive SAST/SCA scanner

PT Container Security
Protection for containers

PT BlackBox (DAST)
Application vulnerability detection

PT Application Firewall PRO
Zero-day threat protection

Industrial security

PT Industrial Security Incident Manager
Unified OT security and infrastructure monitoring solution

PT Industrial Cybersecurity Suite (ICS) SCADA protection
Integrated platform to protect industrial systems from cyberthreats

Our flagship projects

STANDOFF 365

- Cyberbattle
- Cyberbones
- Cyberrange
- Bug Bounty

positive education

phd Positive Hack Days Fest

positive hack camp

Based on our products, we have developed several solutions to leverage Positive Technologies experience in protecting businesses of all types and implement national and international security standards. The Standoff 365 Platform improves business security through hands-on cyber exercises and security system research.

SERVICES

Offensive

- Security Assessment (IT, OT, ATM/POS)
- Red Teaming
- PT MAZE
  A service for protecting mobile applications from reverse engineering

Defensive

- Compromise Assessment
- Digital Forensics & Incident Response
- Threat Intelligence

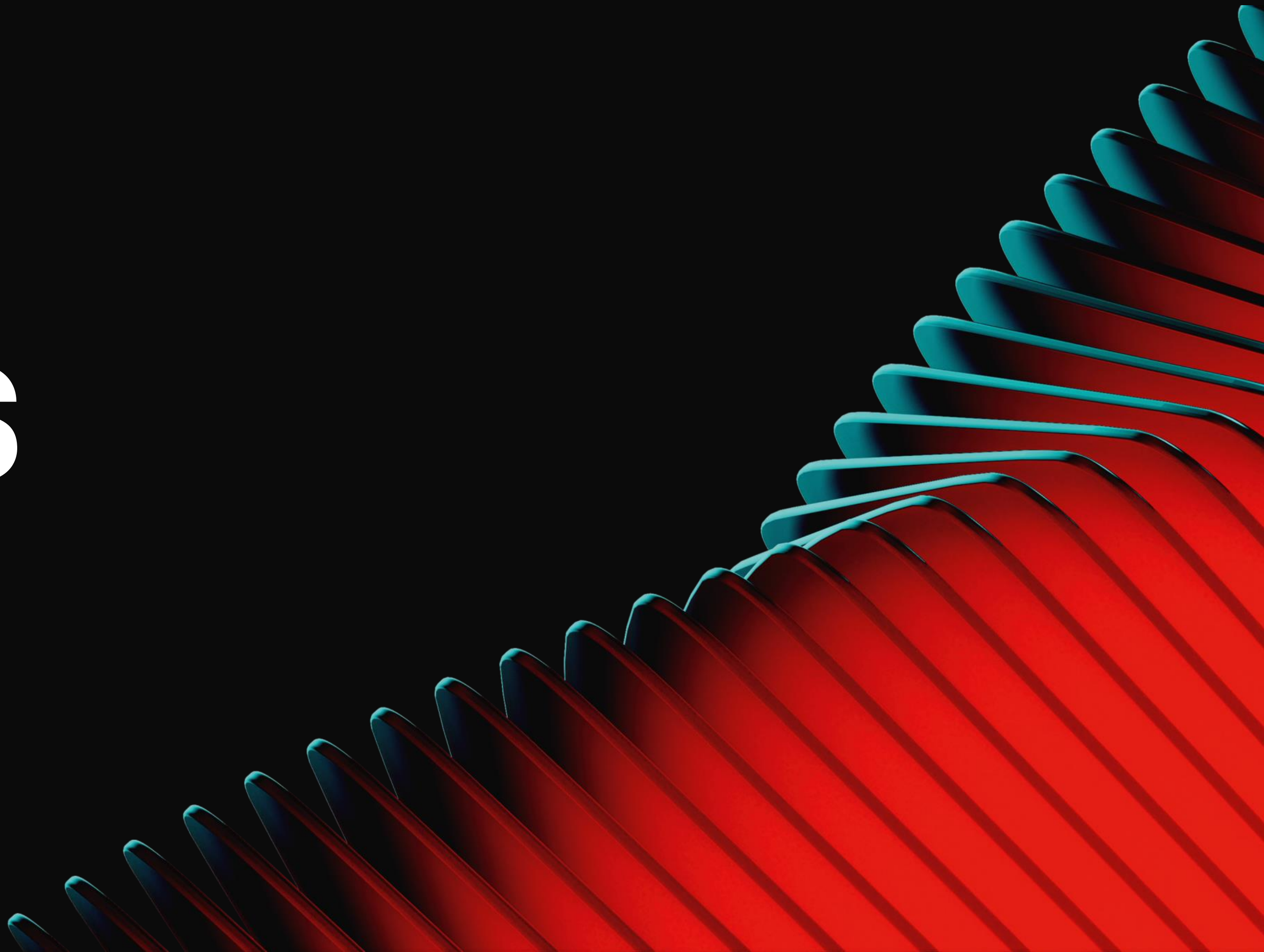
CONSULTANCY

- Result Driven Cybersecurity
- DevSecOps Consulting
- SOC transformation

We also offer cybersecurity services and consulting, including continuous security assessment of business, response to and investigation of challenging information security incidents, and security monitoring of corporate information systems.

positive technologies

OUR PRODUCTS



PT NETWORK ATTACK DISCOVERY

EARLY DETECTION OF THREATS AND TARGETED ATTACKS IN NETWORK TRAFFIC

PRODUCT OVERVIEW

PT NAD is a deep network traffic analysis NDR system that detects attacks both at the perimeter and inside your network. It identifies anomalous network behavior—even in encrypted traffic—and helps investigate incidents.

CHALLENGES SOLVED

1 **False positives create excessive alerts**
Flexible, self-learning ML algorithms train automatically for seven days based on company traffic, reducing false positives and improving SOC efficiency.

2 **Attack investigation**
Metadata is collected and analyzed to support timely decisions and recommend effective responses.

3 **Network security policy monitoring**
Configuration errors and security policy violations (e.g., unfinished sessions, weak passwords, unauthorized remote access tools, or tools for concealing network activity) are identified to enhance network security.

4 **Suspected hacking group presence**
Build threat hunting process within the company based on PT NAD, test hypotheses (e.g., the presence of hackers in the network) and identify hidden threats that standard information security tools might miss.

KEY BENEFITS

180

attacker tactics and techniques,
including hacker tools and modified malware, documented in MITRE ATT&CK

SOC

seamless integration
compatible with SIEM and Sandbox, as well as similar solutions by other vendors

1+1

easy deployment
agentless architecture that deploys in 1 hour and first detects within 1 hour

INFRASTRUCTURE SECURITY

MAXPATROL VM

NEXT-GENERATION VULNERABILITY MANAGEMENT THAT STOPS HACKERS IN THEIR TRACKS

PRODUCT OVERVIEW

A next-generation vulnerability management system that lets you build a full-fledged vulnerability management process and monitor the security of your IT infrastructure at all times without giving hackers a chance to exploit vulnerabilities.

CHALLENGES SOLVED

1	**Identifies and prioritizes vulnerabilities**	MaxPatrol VM leverages its continuously updated knowledge base to assess the asset security level.
2	**DAST web application scanner**	The system allows for full-fledged DAST scanning of web applications.
3	**Compliance management**	Check for compliance of the infrastructure with information security requirements to prevent hacking through misconfigurations.
4	**Helps establish a vulnerability management process**	MaxPatrol VM lets you define scanning and remediation policies and control compliance with them.

KEY BENEFITS

Collection of >3,000 asset parameters

A full picture of your IT environment thanks to unique asset discovery technology

Rapid vulnerability detection

without rescanning and powered by stored asset intelligence

Expert support

and notifications of new trending vulnerabilities within 12 hours

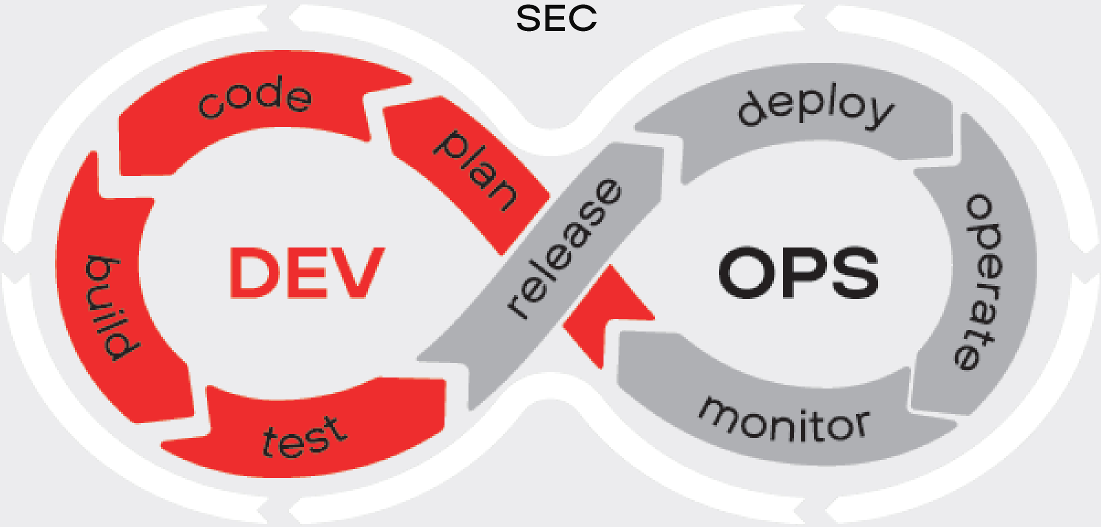
APPLICATION SECURITY

A COMPLETE SET OF PRODUCTS AND SERVICES
DESIGNED TO ENSURE SECURE SOFTWARE DEVELOPMENT

Products

- PT Application Inspector SAST/SCA
- PT Container Security
- PT BlackBox DAST
- PT Application Firewall PRO

Services



- SSDLC assessment and automation review
- AppSec tool integration and automation within the CI/CD pipeline
- Reusable pipeline components
- AppSec operationalization

PT APPLICATION INSPECTOR

COMPREHENSIVE SAST/SCA SCANNER

PRODUCT OVERVIEW

Is a comprehensive static application security testing (SAST) and software composition analysis (SCA) solution that provides high-quality analysis and convenient tools to automatically confirm vulnerabilities, significantly speeding up work with reports and simplifying cooperation between security specialists and developers.

ADVANTAGES

1	**Early detection**	PT AI integrates into your CI/CD pipelines, allowing security scans to run at the earliest stages of the SSDLC.
2	**Comprehensive security coverage**	Supports Static Application Security Testing (SAST) and Software Composition Analysis (SCA) to secure both custom code and open-source dependencies.
3	**Centralized quality gates**	Built-in capabilities to enforce quality gates across CI/CD systems, ensuring consistent security policies.
4	**Scalable and developer-friendly**	Automated processes and integration reduce manual work, making it easier for developers to adopt security practices.

KEY BENEFITS

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 CONTAINER SECURITY

PROTECTION FOR CONTAINERS

PRODUCT OVERVIEW

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 images, containers, and their infrastructure during the build, deployment, and execution phases. PT Container Security ensures cyber security protection at the container level.

ADVANTAGES

1	Comprehensive Protection	Safeguards runtime containers in Kubernetes environments.
2	Seamless Integration	Integrates with DevSecOps tools, SIEMs, and vulnerability management systems to streamline workflows.
3	Secure Configurations	Protects container artifacts (Helm charts and Dockerfiles).
4	Custom Policies	Enables tailored security policies and expertise packs to meet unique infrastructure needs.

KEY BENEFITS

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

PT BLACKBOX

PROTECTION FOR CONTAINERS

PRODUCT OVERVIEW

A dynamic and easy-to-use dynamic application security testing tool that helps find and eliminate vulnerabilities at the software testing and delivery stages. Web applications are a popular destination for attackers. Attacks of this kind can be used to spread malware, redirect users to malicious sites, or steal data through social engineering.
To detect vulnerabilities, PT BlackBox simulates the behavior of an attacker trying to exploit existing vulnerabilities.

ADVANTAGES

1	**Efficient scanning**	Lowers resource consumption by skipping duplicate pages during scans, optimizing performance.
2	**Advanced threat detection**	Uncovers hidden threats using a mix of signature and heuristic analysis with continuous updates.
3	**Customizable scans**	Users can fine-tune analysis parameters, including the scope of scanning and authorization settings, to meet specific requirements.
4	**API vulnerability coverage**	Direct API scanning enables you to identify potential vulnerabilities in critical backend systems.

KEY BENEFITS

98%

of IT applications contain vulnerabilities

91%

of applications allow hackers to steal sensitive data

84%

of applications enable hackers to gain access to web resources

PT APPLICATION FIREWALL PRO

ZERO-DAY THREAT PROTECTION

PRODUCT OVERVIEW

A flexible and precise tool to fully protect 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.

ADVANTAGES

1 **Adaptable architecture** — Microservice-based design enables deployment in diverse network environments, allowing components to integrate directly into application segments.

2 **Cost-efficient deployment** — Supports lightweight modules for Kubernetes-based or nginx servers, minimizing deployment and support costs.

3 **Advanced attack protection** — Safeguards against OWASP Top 10 threats, malicious bots with Google reCAPTCHA, and unauthorized web application access.

KEY BENEFITS

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

PT INDUSTRIAL SECURITY INCIDENT MANAGER

UNIFIED OT SECURITY AND INFRASTRUCTURE MONITORING SOLUTION

PRODUCT OVERVIEW

PT Industrial Security Incident Manager (PT ISIM) delivers comprehensive security for OT infrastructures and cyber-physical systems. The solution detects:

- Unauthorized operations
- Malicious activities
- Malware in both OT traffic and SCADA hosts

PT ISIM enables complete asset inventory management and scales seamlessly from a single site to an entire fleet.

ADVANTAGES

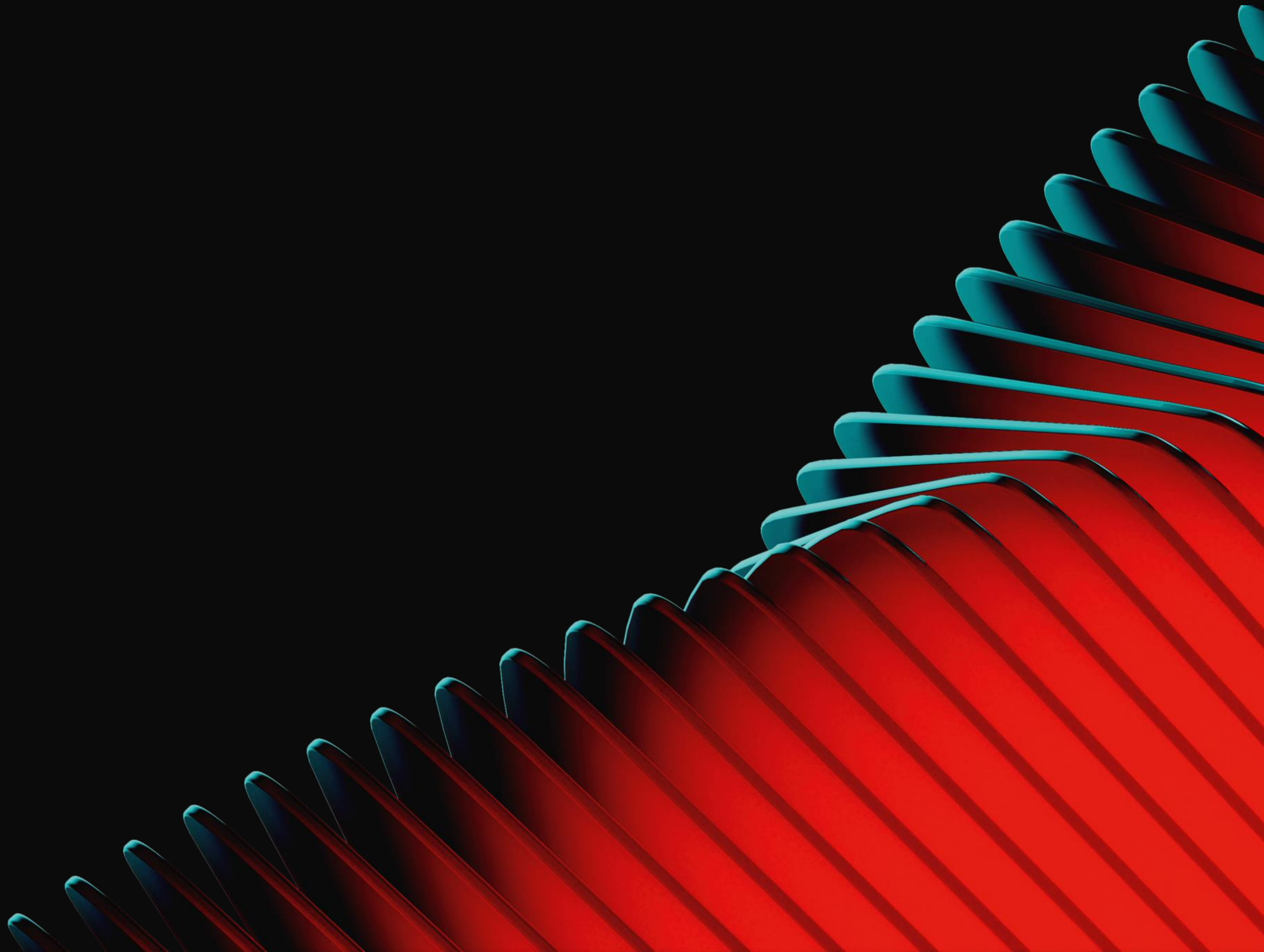
1	OT Network Integrity Control	Monitors network integrity and detects unauthorized devices/connections. Supports a wide range of industrial protocols.
2	Detection of Harmful & Abnormal Commands	Identifies rare but legitimate ICS operations (e.g., PLC firmware updates, forced variable changes, memory clears).
3	OT Traffic Anomalies & Threat Detection	Real-time detection of Malware activity, Proxy servers & tunnels, Weak/default passwords, Attacks on Windows/Linux systems & network devices
4	Asset Inventory & Host Monitoring	PT ISIM Endpoint collects: ▪ Inventory data (software, hardware, users, network connections). ▪ Security events from SCADA servers/workstations including out-of-the-box content for SCADA systems.
5	OT Network Integrity Control	▪ Monitors network integrity and detects unauthorized devices/connections. ▪ Supports a wide range of industrial protocols.

KEY BENEFITS

130+	10+	10k+	Versatile product
network protocols supported by PT ISIM	industrial systems supported by PT ISIM Endpoint Agent	rules and threat indicators available out of the box	suited for all major industries, IIoT

positive technologies

OUR SERVICES



OFFENSIVE SERVICES

PT SWARM - ethical hackers develop and execute attacks, acting like real cybercriminals.

Security Assessment

Pinpointing vulnerabilities and providing recommendations for enhancing cybersecurity in IT, OT, and ATM/POS

31k

vulnerabilities on average
in corporate systems

Red Teaming

Simulate real-world attacks to evaluate your defenses and response readiness

5 days

to reach maximum privileges
during testing

PT MAZE

A service for protecting mobile applications from reverse engineering. Prevents cloning, tampering, unauthorized unlocking of paid features, and vulnerability scanning

10 days

to execute
a non-tolerable event

DEFENSIVE SERVICES

PT ESC specializes in incident response, investigation, and monitoring of corporate systems with PT products.

Compromise Assessment

Conduct a deep investigation of infrastructure using advanced techniques to detect hidden breaches. Early identification limits damage, prevents loss, and accelerates recovery

30min

average response time

Digital Forensics & Incident Response

Prevent further damage, reconstruct the full sequence of events, assess impact, and deliver clear recommendations to avoid recurrence

1k

detection rules developed

Threat Intelligence

Combines multiple intelligence sources, threat data feeds, and in-house research to provide actionable intelligence and strengthen cyber defense

80M+

IoC collected

DEVSECOPS CONSULTING STRATEGY

1

Assessment

Analyze the current application development security posture

2

Strategy

Create a strategy for a secure application development process

3

Implementation

Processes, technical controls, configuration and integration for a secure development

Tasks

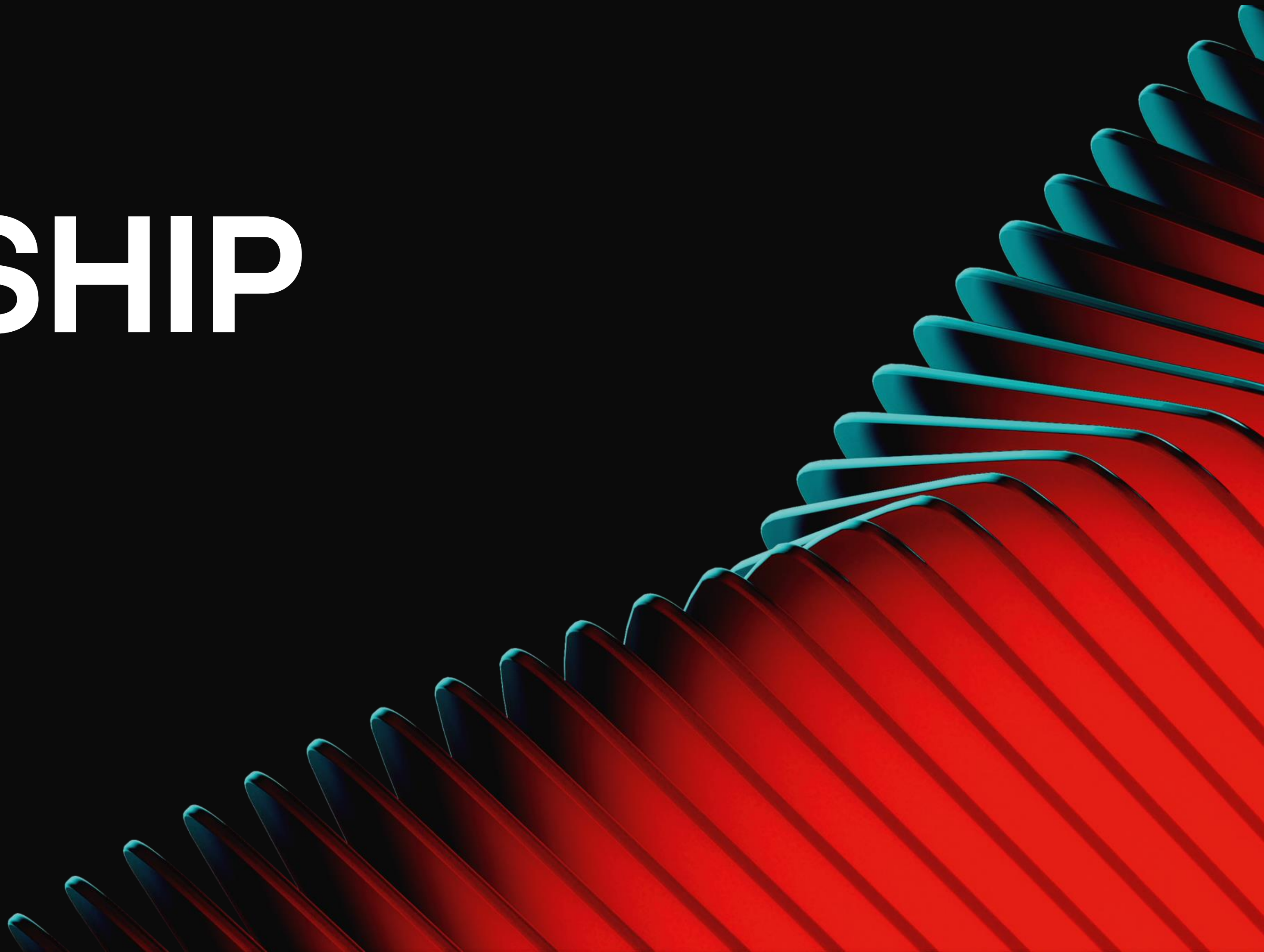
1. Initiate the Application Security program in the organization.
2. Prioritize tasks and stages of implementing AppSec initiatives.
3. Get the basic documents and artifacts to quick start.
4. Build a target "To Be" process structure.

Results

- Roadmap for Application Security practices implementation
- Recommendations on organizational changes to help implement the strategy
- Security Architecture of Application Security tools
- Budget evaluation of strategy implementation
- Process map for DevSecOps practices
- Methodology for end-to-end defect prioritization
- Other artifacts to implement the strategy

positive technologies

OUR FLAGSHIP PROJECTS



STANDOFF 365 PLATFORM

STANDOFF 365

Improves business security through hands-on cyber exercises and security system research

1 Standoff Cyberbattle — An international offline event that brings together infosec specialists and security researchers to test and hone their skills on the most realistic infrastructure possible

2 Standoff Cyberrange — A virtual copy of corporate IT systems to test the skills of security researchers and infosec specialists

3 Standoff Cyberbones — An online simulator for investigating incidents from the Standoff Cyberbattle, allowing infosec specialists to better understand how to detect and respond to cyberthreats

4 Standoff Bug Bounty — A proven information security platform that pays white hat hackers to help companies identify vulnerabilities

HERE BUSINESSES AND WHITE HAT HACKERS JOIN FORCES

standoff365.com/en-US/

POSITIVE EDUCATION

BUILDING THE CYBERSECURITY COMMUNITY

positive education

Cybersecurity for beginners and professionals

Educational programs for leading universities
to give students a head start in their careers:
Positive Education materials written by our experts
are used at over 65 universities

POSITIVE EDUCATION

KEY INITIATIVES

IS A CYBERSECURITY ACADEMY DEDICATED TO TRAINING INFORMATION SECURITY PROFESSIONALS AND STRENGTHENING NATIONAL SOVEREIGNTY BY DEVELOPING LOCAL EXPERTISE

1

Corporate programs

Tailored training programs to build and execute effective, measurable cybersecurity strategies

- **Executives**
  Strategic training for senior leaders focused on building actionable cybersecurity programs and managing performance across the organization, with clear, measurable outcomes
- **Cybersecurity specialists**
  Hands-on, practical instruction for professionals to sharpen skills in threat mitigation, incident response, and performance measurement
- **Awareness training**
  Company-wide programs designed to embed a security-first mindset at every level—crucial for both national resilience and corporate defense

2

National educational programs

Partnering with governments to build national cybersecurity capacity and strengthen digital sovereignty

- **Academic**
  Designing and launching university-level initiatives to build a steady pipeline of skilled cybersecurity professionals and support national strategic goals
- **Train the trainers**
  Preparing qualified individuals to deliver high-impact cybersecurity training within their organizations and across sectors
- **Ethical hacker training**
  Equipping cybersecurity specialists with the skills to identify and remediate vulnerabilities through proactive, hands-on instruction

POSITIVE HACK CAMP

BUILDING THE CYBERSECURITY COMMUNITY

Positive Hack Camp

A free global program by Positive Education and CyberEd started in 2024. **70** students from **20** countries joined us for a 2-week deep dive into hands-on cybersecurity and real-life incident investigation

HOW CAN WE START

WE ARE READY TO HOLD A MEETING
AND SHARE OUR CASE STUDIES

1

Challenges

We discuss your challenges to develop an action plan

2

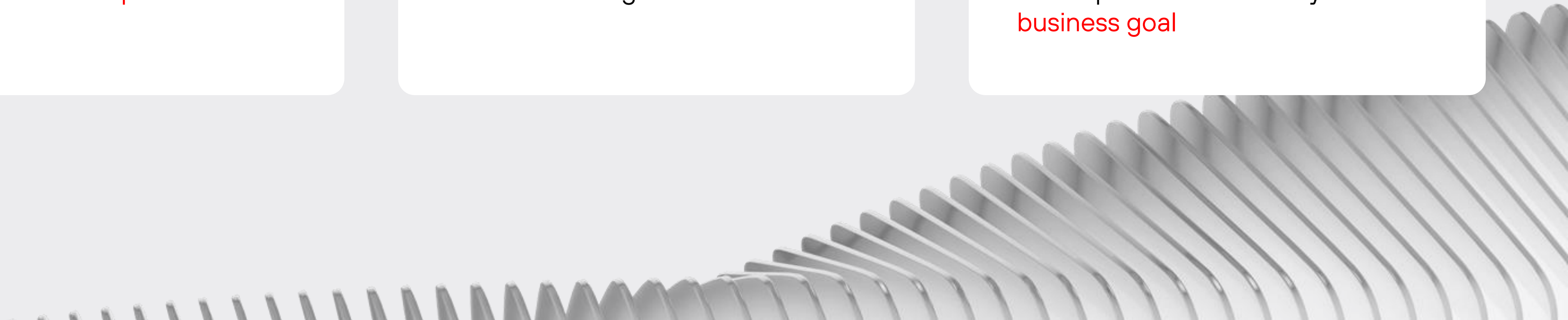
Solutions

We generate ideas and propose solution to bring real value

3

Execution

We deliver our unique approach and experience to reach your business goal



positive
technologies

Protect your business from cyberattacks with a measurable and result-driven approach. The Olympic Games and FIFA World Cup already have.

global.ptsecurity.com

info@ptsecurity.com