positive
technologies

PT Network Attack Discovery

Early detection of threats and complex targeted attacks
Expert investigation using a network traffic copy

ADVANTAGES

Reveals lateral movement of attackers throughout the network

Detects 150 attacker tactics and techniques, including hacker tools and modified malware

Helps meet information protection requirements

Can be integrated with MaxPatrol SIEM and PT Sandbox, as well as with similar solutions by other vendors

Quick deployment
Requires less than one hour to be put into commercial operation

PT Network Attack Discovery is a network traffic behavioral analysis (NTA) system used to detect hidden cyberattacks. PT NAD accurately detects attacker actions in a network, facilitates incident investigations, and helps with threat hunting. PT NAD knows what to look for in your company's network.

Get the full view

The system uses advanced machine learning technologies to profile the behavior of all network devices and detect any deviations from their normal activity. This approach allows our customers to tailor PT NAD to an infrastructure that needs protection and detect business-critical threats that traditional methods fail to recognize.

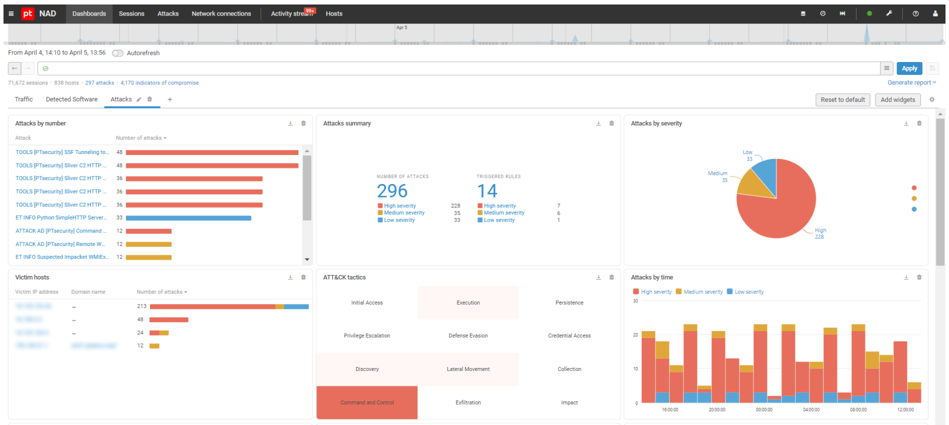
Detect hidden threats and targeted attacks

PT NAD identifies over 100 network protocols as well as 13 tunnel protocols, and parses the 35 most common ones up to and including the L7 level. Based on the parsing and analysis of more than 1,200 protocol parameters, PT NAD builds network node models.

This provides a clear picture of what is going on in the infrastructure and helps identify security flaws that can weaken security and enable attack progression. PT NAD keeps tabs on every node in the network, minimizes the use of uncontrolled IT infrastructure components, and reduces the risk of hacking a company via these components.

An essential tool of SOCs

PT NAD is an indispensable source of data for SIEM solutions. The system inventorizes network hosts and helps to quickly find and identify suspicious sessions. All data on detected events and threats is automatically transferred to a SIEM system. PT NAD provides SOCs with full network visibility, facilitates attack investigation, helps trace the attack chain, and gather evidence.



From April 4, 14:10 to April 5, 13:56 Autorefresh

71,672 sessions · 838 hosts · 297 attacks · 4,170 indicators of compromise

Attacks by number

Attack	Number of attacks
TOOLS [PTsecurity] SSF Tunneling to...	48
TOOLS [PTsecurity] Sliver C2 HTTP ...	48
TOOLS [PTsecurity] Sliver C2 HTTP ...	36
TOOLS [PTsecurity] Sliver C2 HTTP ...	36
TOOLS [PTsecurity] Sliver C2 HTTP ...	36
ET INFO Python SimpleHTTP Server...	33
ATTACK AD [PTsecurity] Command ...	12
ATTACK AD [PTsecurity] Remote W...	12
ET INFO Suspected Impacket WMIEx...	12

Attacks summary

NUMBER OF ATTACKS 296		TRIGGERED RULES 14	
High severity	228	High severity	7
Medium severity	35	Medium severity	6
Low severity	33	Low severity	1

Attacks by severity

Victim hosts

Victim IP address	Domain name	Number of attacks
[redacted]	–	213
[redacted]	–	48
[redacted]	–	24
[redacted]	[redacted]	12

ATT&CK tactics

Initial Access	Execution	Persistence
Privilege Escalation	Defense Evasion	Credential Access
Discovery	Lateral Movement	Collection
Command and Control	Exfiltration	Impact

Attacks by time

An operator sees detailed information about suspicious activity on the dashboard.
This helps to quickly respond to incidents and conduct investigations.

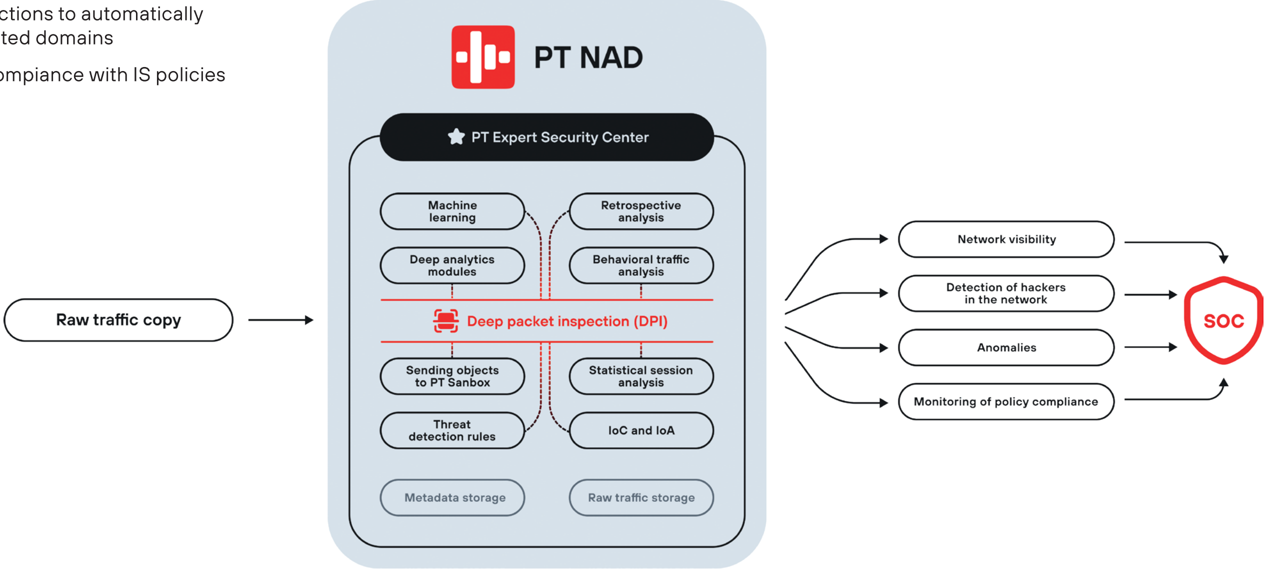
How is your company being attacked?
Check your network and perimeter.
Request a free PT NAD pilot at our website.

PT NAD DETECTS:

- Threats in encrypted traffic
- Use of hacker tools, including custom-made ones
- Lateral attacker movement
- Network anomalies
- Infected network hosts
- Attacks on the domain contoller
- Signs of previously unnoticed attacks
- Exploitation of vulnerabilities on the network
- Signs of malicious activity being hidden from security tools
- Connections to automatically generated domains
- Non-compiance with IS policies

Application scenarios

- **Detection of attacks on the perimeter and in the infrastructure, profiling of network hosts.** Thanks to embedded deep analytics modules, unique threat detection rules, and indicators of compromise, PT NAD detects attacks both at the earliest stages and after adversaries have already penetrated the infrastructure.
- **Investigation of attacks.** Infosec experts can localize an attack, trace kill chain, detect vulnerabilities in infrastructure, and implement countermeasures to prevent future incidents.
- **Threat hunting.** PT NAD helps organize threat hunting in a company, test hypotheses such as the presence of hackers in the network, and detect hidden threats that cannot be detected with standard cybersecurity tools.
- **Monitoring of compliance with infosec policies.** PT NAD detects misconfigurations and cases of non-compliance with infosec policies that can pave the way for attackers. Examples include incomplete sessions, dictionary passwords, use of remote access utilities and tools that hide network activity.


PT NAD
PT Expert Security Center
Machine learning
Retrospective analysis
Deep analytics modules
Behavioral traffic analysis
Deep packet inspection (DPI)
Sending objects to PT Sanbox
Statistical session analysis
Threat detection rules
IoC and IoA
Metadata storage
Raw traffic storage
Raw traffic copy
Network visibility
Detection of hackers in the network
Anomalies
Monitoring of policy compliance
SOC

How PT NAD works

PT NAD captures and analyzes network traffic on the perimeter and in the infrastructure using built-in DPI technology. TAP devices, network packet brokers, and active network equipment can be used as sources of traffic. By analyzing a copy of network traffic using statistical and behavioral modules, PT NAD detects hacker activity at the earliest stages of network penetration, as well as during attacker attempts to get a foothold in the network and continue the attack. PT NAD stores a copy of the raw traffic and uses it to generate metadata for retrospective analysis. After updating threat detection rules and IoCs from PT Expert Security Center, PT NAD automatically cross-checks collected traffic data and notifies SOC analysts about the hidden presence of any attackers in the network. By combining several mechanisms for complex threat detection, PT NAD provides visibility into a company's network, detects suspicious connections and network anomalies, and helps follow information security compliance.

global.ptsecurity.com
info@ptsecurity.com

Positive Technologies is an industry leader in result-driven cybersecurity and a major global providerof information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 4,000 organizations worldwide use technologies and services developed by our company.