positive technologies

PT Network Attack Discovery

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

ADVANTAGES

Reveals attackers in east-west traffic

Detects hacker tools and modified malware

Helps в meet information protection requirements

Can be integrated with SIEM systems and sandboxes

Quick deployment
Requires less than 1 hour to be put into commercial operation

PT Network Attack Discovery — is a network traffic analysis (NTA) system used to monitor malicious activity on the perimeter and inside of a network. It is a convenient investigation tool that detects malicious activity even in encrypted traffic. PT NAD knows what to look for in your company's network.

Get the full view

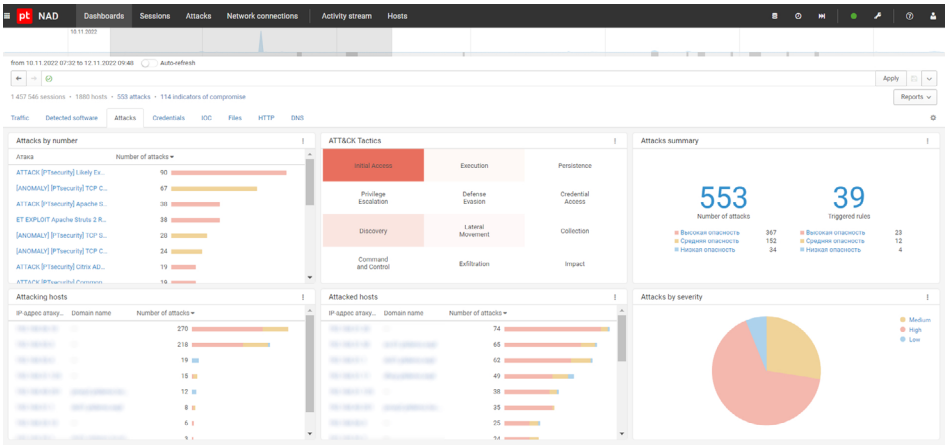
PT NAD identifies over 100 protocols as well as nine tunnel protocols and parses the 35 most common ones up to and including the L7 level. Based on the parsing and analysis of more than 1,200 protocol parameters, PT NAD builds network node models. This provides a clear picture of what is going on in the infrastructure and helps identify security flaws that can weaken security and enable attack progression. PT NAD keeps tabs on every host in the network, minimizes the use of uncontrolled IT infrastructure components, and reduces the risk of hacking a company via these components.x.

Detect hidden threats and targeted attacks

PT NAD automatically detects network penetration attempts and the presence of attackers in the infrastructure based on multiple indicators, such as the tools used or data transferred to attacker servers

Make SOCs more effective

PT NAD — is an indispensable source of data for SIEM solutions. It stores metadata and raw traffic, helps to quickly find and identify suspicious sessions, as well as export and import traffic. PT NAD provides SOCs with full network visibility, makes it easier to verify whether an attack was successful, helps trace the attack chain and gather evidence.



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

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

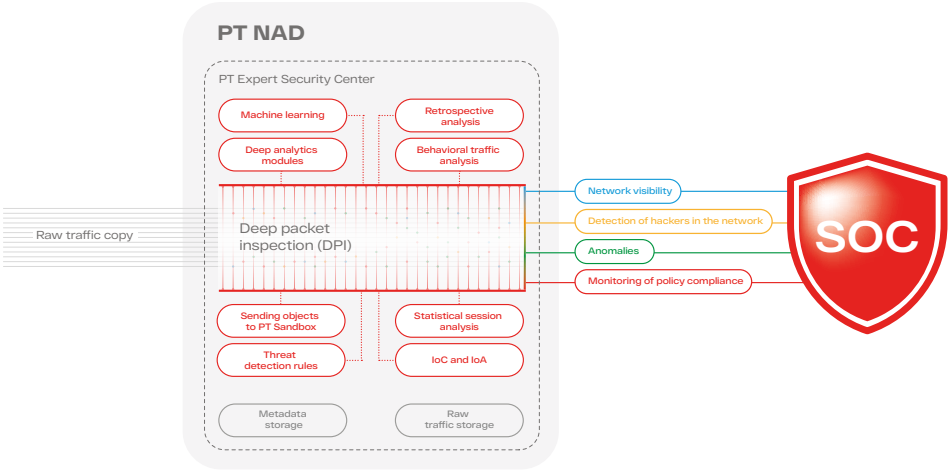
PT NAD DETECTS:

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

Application scenarios

- **Monitoring of policy compliance.** PT NAD detects misconfigurations and instances of security policy non-compliance that can pave the way for attackers. Examples include credentials transmitted in clear text, weak passwords, remote access utilities, and tools that hide network activity.
- **Detection of attacks on the perimeter and in the infrastructure.** Thanks to embedded deep analytics modules, unique threat detection rules, indicators of compromise, and retrospective analysis, 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.

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.

ptsecurity.com
pr@ptsecurity.com