:: Positive Technologies

Telecom Network Attack Discovery

Exposes threats to 5G and the general telecoms infrastructure

BENEFITS

5G tailored

Tailored to identify telecom-specific attacks targeting 5G and other telecom assets

Virtualized

Detects malicious activity in core network including SDN/NFV traffic

Privacy

All information on attacks and consequences are only stored locally on-net

Automation

Integrates seamlessly with generic SIEM and sandbox solutions

Telecom Network Attack Discovery is the first 5G and the general telecoms–focused deep threat analysis system. Positive Technologies unique combination of expertise has allowed the direct import of industry leading telecom security research into a proven network threat analysis platform—creating comprehensive perimeter protection, while also safeguarding the interior of the network. The system makes hidden threats visible, detects suspicious activity even in encrypted traffic, and streamlines incident investigation.

Gain a full insight to your telecom network

TNAD identifies over 70 protocols and parses the 30 most common ones up to and including the layer 7. This provides a complete picture of activity within your telecom network, identifying security flaws and threats from your existing infrastructure, through virtualization, non-standalone 5G (NSA-5G) and all the way to a standalone 5G (SA-5G) network.

Detect hidden threats

The system automatically detects attacker attempts to penetrate the OSS network and identifies hacker presence on virtualized infrastructure based on multiple indicators, including use of hacker tools and backdoor transmission of data to attackers' servers. So, nullifying advanced persistent threats (APT).

Deliver more effect dedicated telecom security

TNAD provides telecom operators full network security visibility across all existing and 5G perimeters. These include remote access by vendor, critical as networks evolve to SA 5G, APIs access for new partners delivered by the Network Exposure Function, MEC to core connectivity, IoT devices management and many more. The TNAD retains all relevant metadata and raw traffic to quickly and easily verify an attacks success, reconstruct the kill chain, and gather evidence. This is extended to retrospective analysis by the traffic import/export feature facilitating investigation of security incidents.

TNAD detects:

- Identified 5G-specific security threat including new risks in vectors such as Network Exposure Function (NEF)
- Abuse of remote OSS/BSS access
- API exploitation and abnormalities from MEC to third-party API connectivity
- SDN and NFV network threats
- Anomalies in user plane GTP-U traffic
- Exploitation of misconfiguration and existing vulnerabilities in Core/IT networks
- Data integrity checks

Usage scenarios

Monitoring of policy compliance

TNAD detects misconfigurations and instances of security policy non-compliance that can pave the way for attackers. Examples include OSS and Orchestrator credentials stored in clear-text, unencrypted messages and management/control plane protocols, remote access utilities, and tools that hide network activity.

Detection of attacks on the external telecom perimeter and in the virtualized infrastructure

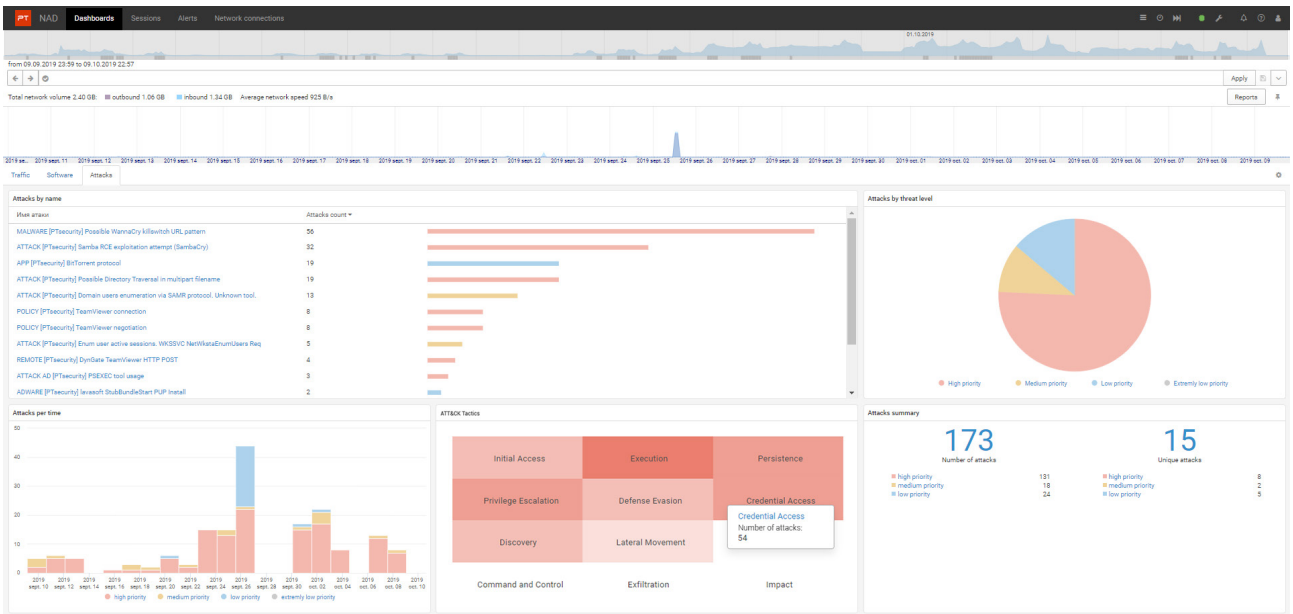
Thanks to embedded machine learning technologies, advanced analytics, unique threat detection rules, indicators of compromise, and retrospective analysis, TNAD detects attacks both at the earliest stages and after attackers may have already penetrated the infrastructure.

Investigation of attacks

With TNAD, security teams can localize an attack, trace its chain, detect vulnerabilities in infrastructure, and implement countermeasures to prevent future incidents, for instance abuse of legitimate remote access for vendors, value-added services, or mobile device management. This is particularly relevant during the extended network transition to a full standalone 5G infrastructure.

Threat hunting

TNAD delivers exceptional threat hunting. MNOs can test hypotheses about their security to detect the hidden threats that slip by ordinary cybersecurity solutions. Such as the detection of silent APT threats and complex protection of the core network and its interfaces.



The dashboard helps security specialists to investigate and quickly react to suspicious activity

TNAD supports on:

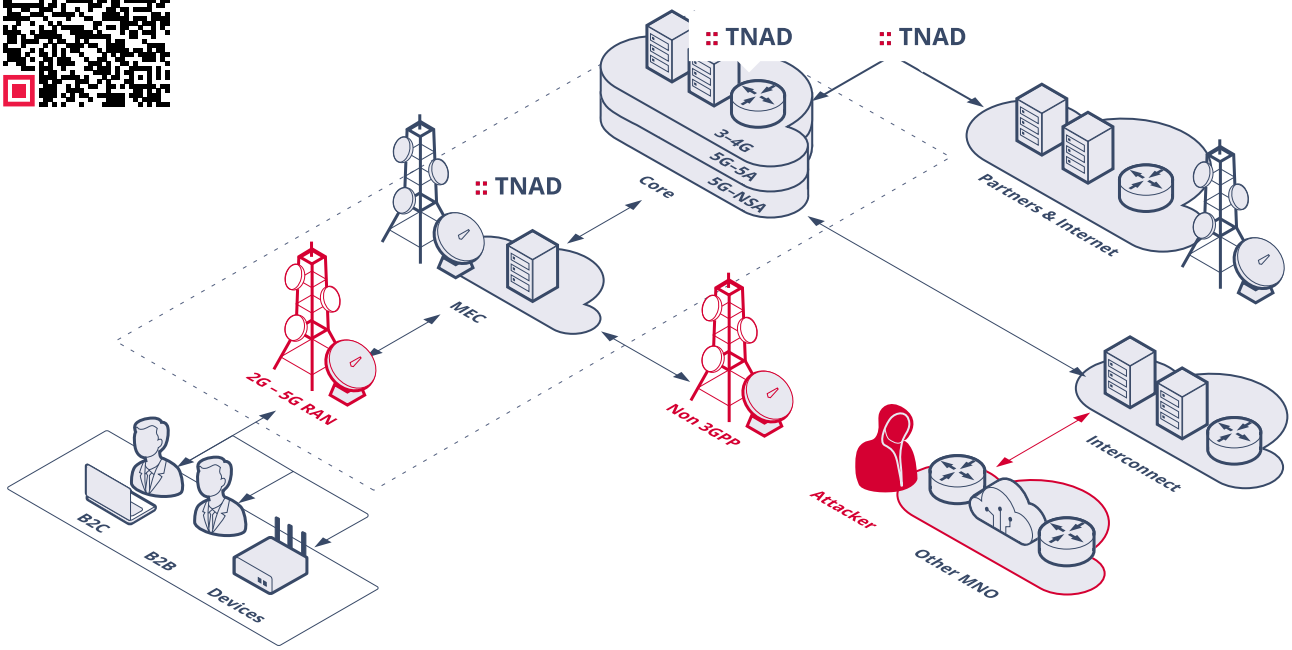
- 2G, 3G, 4G, NSA-5G, SA-5G management plane traffic inspection
- Abuses in DCI protocols (MEC)
- Network functions virtualization bypassing
- Virtualized host abuse
- Sessions hijacking
- Discovering threats in encrypted traffic
- Use of hacking tools
- Lateral movement
- Malware/bot activity
- Signs of previously unnoticed attacks
- Attempts to hide activity from security tools
- Non-compliance with standard security policies
- Security incident investigation

How is your company being attacked?

Check your network and perimeter. Request a free TNAD trial on our website:

How it works

TNAD captures and analyzes traffic on the external telecom perimeter and in both virtualized (NFV) and hardware-based infrastructure. This allows detection of the hackers activity to deny the initial network penetration, as well proactive exposure of intruders attempts to get a foothold in the network and pursue their attack.



positive-tech.com
contact@positive-tech.com

About Positive Technologies

Positive Technologies is a global cybersecurity company. Its flagship Telecom Cybersecurity Suite enables network operators to drive business performance while protecting their subscribers and services. By providing greater visibility into infrastructure vulnerabilities and securing customer services, Positive Technologies helps to strengthen loyalty, drive revenue with value-added security offerings, and protect emerging telecom technologies such as 5G and the IoT.

PT-AG_TNAD_PB_A4.ENG.0003.03