POSITIVE TECHNOLOGIES

PT Network Attack Discovery

Makes hidden threats visible

ptsecurity.com

About Positive Technologies

19 **years**
of experience
in security development
and research

900 **employees:**
security engineers,
developers, analysts,
and others

250 **experts**
at our security
research center

200+
zero-day vulnerabilities
discovered yearly

200+
corporate security audits
performed for clients annually

50%
of all industrial and telecom
vulnerabilities are discovered
by our experts

We protect enterprise information systems from cyberthreats by:

- Creating products and solutions
- Performing security audits
- Investigating incidents
- Researching threats

A trusted name

Terna
LUKOIL
ROSNEFT
sky
GAZPROM
JOINT-STOCK COMPANY
VimpelCom™
SK telecom
du
Raiffeisen BANK
UniCredit Bank
SBERBANK
SAMSUNG
Postel
Hanwha
التجاري وفا بنك
Attijariwafa bank

Our projects

FIFA WORLD CUP
RUSSIA
2018

Challenge
Protect services for fan movement, volunteer recruitment, and transportation contractors.

What we did
Aligned cybersecurity and performed non-stop monitoring of all infrastructure.

Result
Supported safe and continuous functioning of all information systems.

ptsecurity.com

phd
Positive
Hack
Days

Annual international practical security forum attracting over 8,000 participants.

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

During the cyberbattle, the SOC uses our products to monitor infrastructure and detect attacks.

phdays.com

Analytics and research

OVER 20+ PUBLICATIONS YEARLY:

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

Web Application Vulnerabilities: Statistics for 2018
2019
PT
Attacks on web applications: 2018 in review
PT
POSITIVE RESEARCH
2019
Vulnerabiliti in online b applicati
2019
POSITIVE TECHNOLOGIES

ptsecurity.com/ww-en/analytics

Why monitor internal network traffic?

Perimeter protection is not enough

In 2019, at **93% of companies,** our pentesters succeeded in breaching the network perimeter and accessing the local network*

Minimum **30 minutes** were needed for penetrating a local network. The average time needed was four days*

206 days is the average dwell time of hackers in the infrastructure prior to detection.**

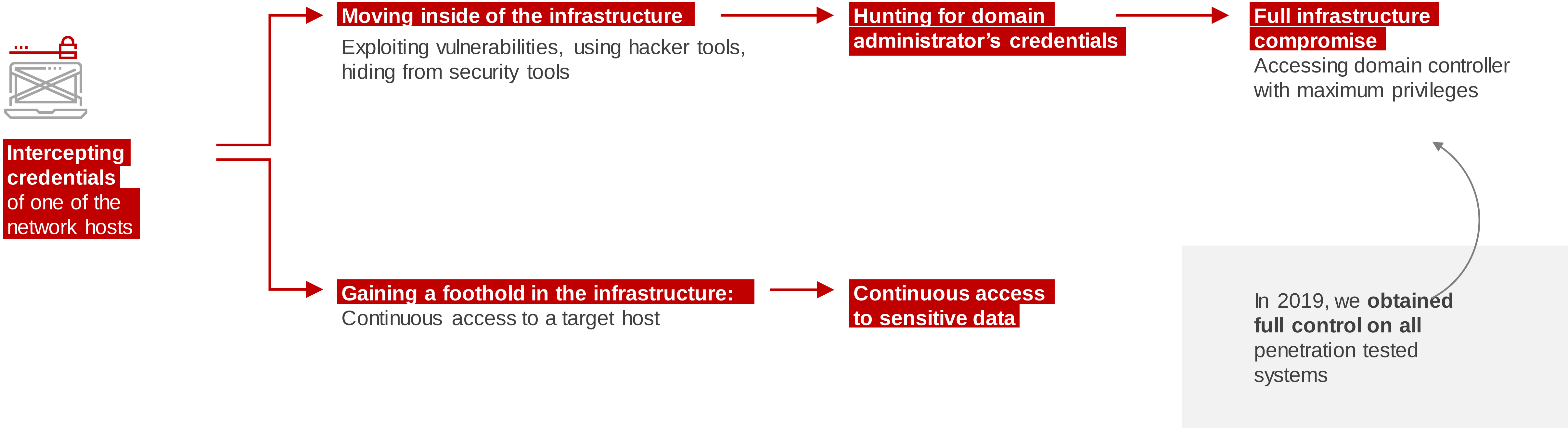
Any corporate network is vulnerable to attacks, even if its perimeter is well protected.

When malefactors reach the internal network, their actions become are invisible for perimeter security tools.

Need to monitor both external and internal traffic

* External pentests results – 2020, Positive Technologies
** 2019 Cost of a Data Breach Report, Ponemon institute

It only takes a few steps for the hackers to win



Intercepting credentials of one of the network hosts

Moving inside of the infrastructure
Exploiting vulnerabilities, using hacker tools, hiding from security tools

Hunting for domain administrator's credentials

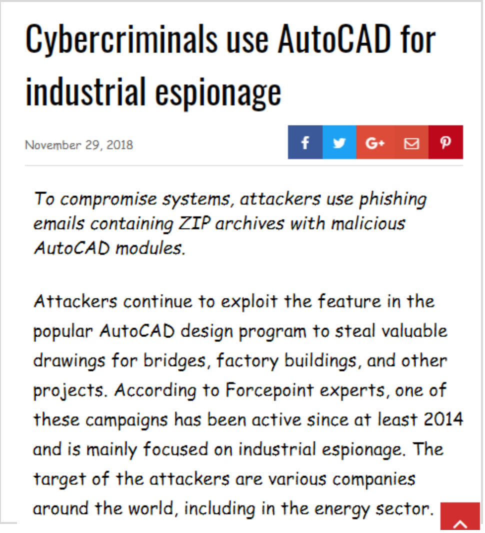
Full infrastructure compromise
Accessing domain controller with maximum privileges

Gaining a foothold in the infrastructure:
Continuous access to a target host

Continuous access to sensitive data

In 2019, we **obtained full control on all** penetration tested systems

Consequences



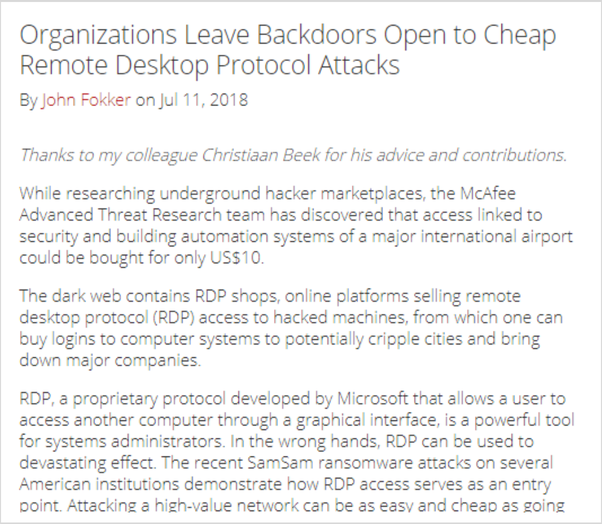
Cybercriminals use AutoCAD for industrial espionage

November 29, 2018

To compromise systems, attackers use phishing emails containing ZIP archives with malicious AutoCAD modules.

Attackers continue to exploit the feature in the popular AutoCAD design program to steal valuable drawings for bridges, factory buildings, and other projects. According to Forcepoint experts, one of these campaigns has been active since at least 2014 and is mainly focused on industrial espionage. The target of the attackers are various companies around the world, including in the energy sector.

hackernews.blog/cybercriminals-use-autocad-for-industrial-espionage-2/



Organizations Leave Backdoors Open to Cheap Remote Desktop Protocol Attacks

By John Fokker on Jul 11, 2018

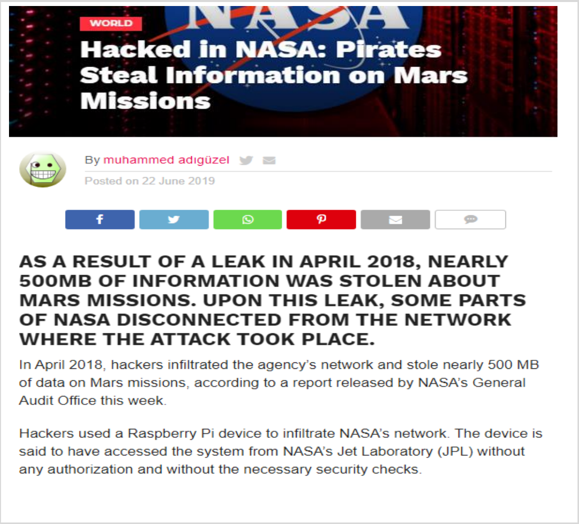
Thanks to my colleague Christiaan Beek for his advice and contributions.

While researching underground hacker marketplaces, the McAfee Advanced Threat Research team has discovered that access linked to security and building automation systems of a major international airport could be bought for only US$10.

The dark web contains RDP shops, online platforms selling remote desktop protocol (RDP) access to hacked machines, from which one can buy logins to computer systems to potentially cripple cities and bring down major companies.

RDP, a proprietary protocol developed by Microsoft that allows a user to access another computer through a graphical interface, is a powerful tool for systems administrators. In the wrong hands, RDP can be used to devastating effect. The recent SamSam ransomware attacks on several American institutions demonstrate how RDP access serves as an entry point. Attacking a high-value network can be as easy and cheap as going

securingtomorrow.mcafee.com/other-blogs/mcafee-labs/organizations-leave-backdoors-open-to-cheap-remote-desktop-protocol-attacks/



WORLD

Hacked in NASA: Pirates Steal Information on Mars Missions

By muhammed adıgüzel

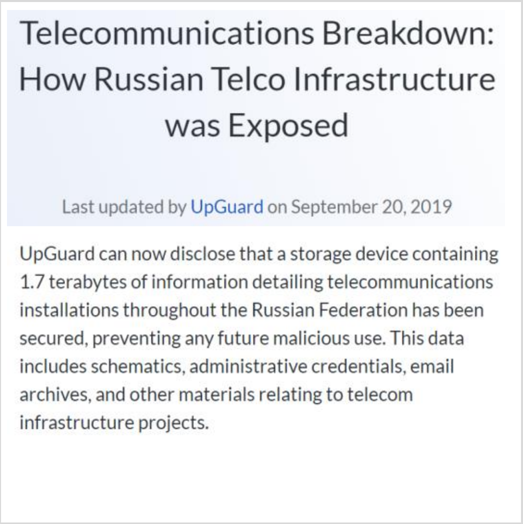
Posted on 22 June 2019

AS A RESULT OF A LEAK IN APRIL 2018, NEARLY 500MB OF INFORMATION WAS STOLEN ABOUT MARS MISSIONS. UPON THIS LEAK, SOME PARTS OF NASA DISCONNECTED FROM THE NETWORK WHERE THE ATTACK TOOK PLACE.

In April 2018, hackers infiltrated the agency's network and stole nearly 500 MB of data on Mars missions, according to a report released by NASA's General Audit Office this week.

Hackers used a Raspberry Pi device to infiltrate NASA's network. The device is said to have accessed the system from NASA's Jet Laboratory (JPL) without any authorization and without the necessary security checks.

techannels.com/hacked-in-nasa-pirates-steal-information-on-mars-missions/

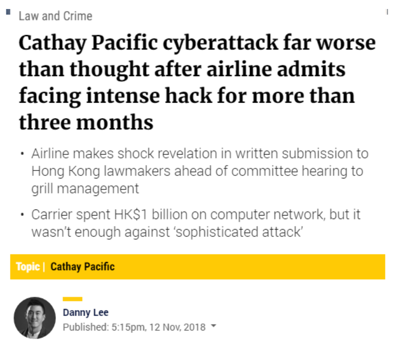


Telecommunications Breakdown: How Russian Telco Infrastructure was Exposed

Last updated by UpGuard on September 20, 2019

UpGuard can now disclose that a storage device containing 1.7 terabytes of information detailing telecommunications installations throughout the Russian Federation has been secured, preventing any future malicious use. This data includes schematics, administrative credentials, email archives, and other materials relating to telecom infrastructure projects.

upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure#/security-lapse-russia/



Law and Crime

Cathay Pacific cyberattack far worse than thought after airline admits facing intense hack for more than three months

- Airline makes shock revelation in written submission to Hong Kong lawmakers ahead of committee hearing to grill management
- Carrier spent HK$1 billion on computer network, but it wasn't enough against 'sophisticated attack'

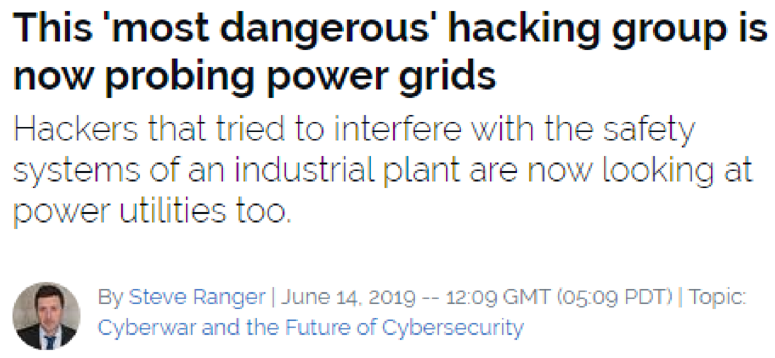
Topic | Cathay Pacific

Danny Lee
Published: 5:15pm, 12 Nov, 2018

When malefactors hack the domain controller, the threat is quite hard to localize.

Example: Hong Kong Airlines
Attacks continued three months after passengers' data leak was detected.

scmp.com/news/hong-kong/law-and-crime/article/2172796/cathay-pacific-cyberattack-far-worse-previously-thought



This 'most dangerous' hacking group is now probing power grids

Hackers that tried to interfere with the safety systems of an industrial plant are now looking at power utilities too.

By Steve Ranger | June 14, 2019 -- 12:09 GMT (05:09 PDT) | Topic: Cyberwar and the Future of Cybersecurity

zdnet.com/article/this-most-dangerous-hacking-group-is-now-probing-power-grids/

How to identify attackers inside the network?

All security monitoring tools (ex SIEM, EDR) have their blind spots. They can be cleared by means of traffic analysis.

Use of hacker tools

To detect PowerView (AD reconnaissance tool), logging of the event 1644 must be enabled: it will show LDAP activity of PowerView. Such events can be generated in large numbers.
An alternative solution will be to detect malicious activity in traffic.

SIEM does not detect some types of attacks

For example, a DCShadow attack involves creating a fake domain controller, which does not provide data about events to SIEM. However, when a new object is added to the domain-controller configuration, this can be clearly viewed in traffic.

Exploitation of vulnerabilities

For example, a critical remote Windows desktop vulnerability CVE-2019-0708 which is exploited during legitimate processes can only be detected by events indirectly. Traffic analysis can offer more accurate detection.

Malware detection

SIEM detects malicious activity based on events detected by antivirus tools and firewalls. Firewalls detect malware based on IP addresses: if an address changes or a new one is created, firewalls will miss them. If malware is packed, an antivirus will most likely overlook it. Hiding malware activity in a network requires a lot of effort, so whatever is overlooked by antivirus tools and firewalls can be detected in traffic.

How to monitor network traffic?

Network traffic analysis (NTA)* systems

- Analyze traffic both on the perimeter and in the infrastructure.
- Detect attacks using a combination of detection techniques.
- Provide information necessary for event investigation.

Many Gartner clients have reported that NTA/NDR tools have detected suspicious network traffic that other perimeter security tools had missed.

Market Guide for Network Detection and Response, Gartner, 2020

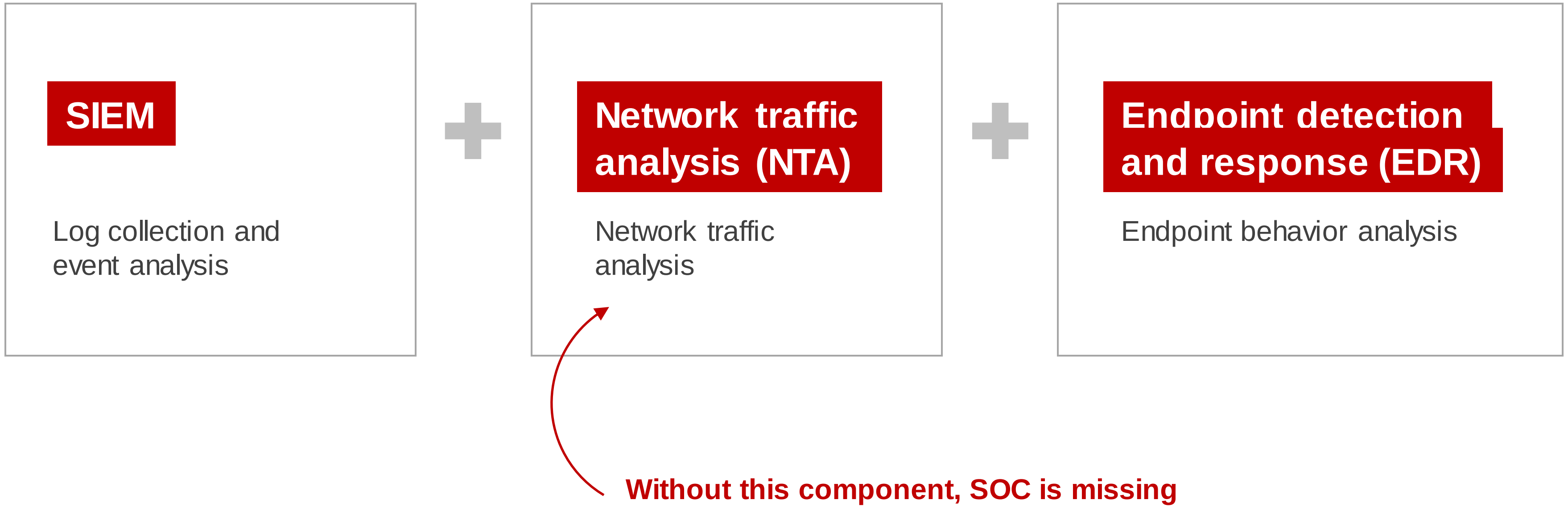
SOCs recognize NTA as one of the best threat detection technologies.

Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey, SANS Institute 2019

*NTA systems can also be called NDR systems (network detection and response)

NTA is a vital SOC tool

SOC is not only about SIEM. SOC visibility triad according to Gartner*:



SIEM

Log collection and event analysis

Network traffic analysis (NTA)

Network traffic analysis

Endpoint detection and response (EDR)

Endpoint behavior analysis

Without this component, SOC is missing events at the network level,
which increases attackers' chances to stay unnoticed.

* Applying Network-Centric Approaches for Threat Detection and Response, Gartner, 2019

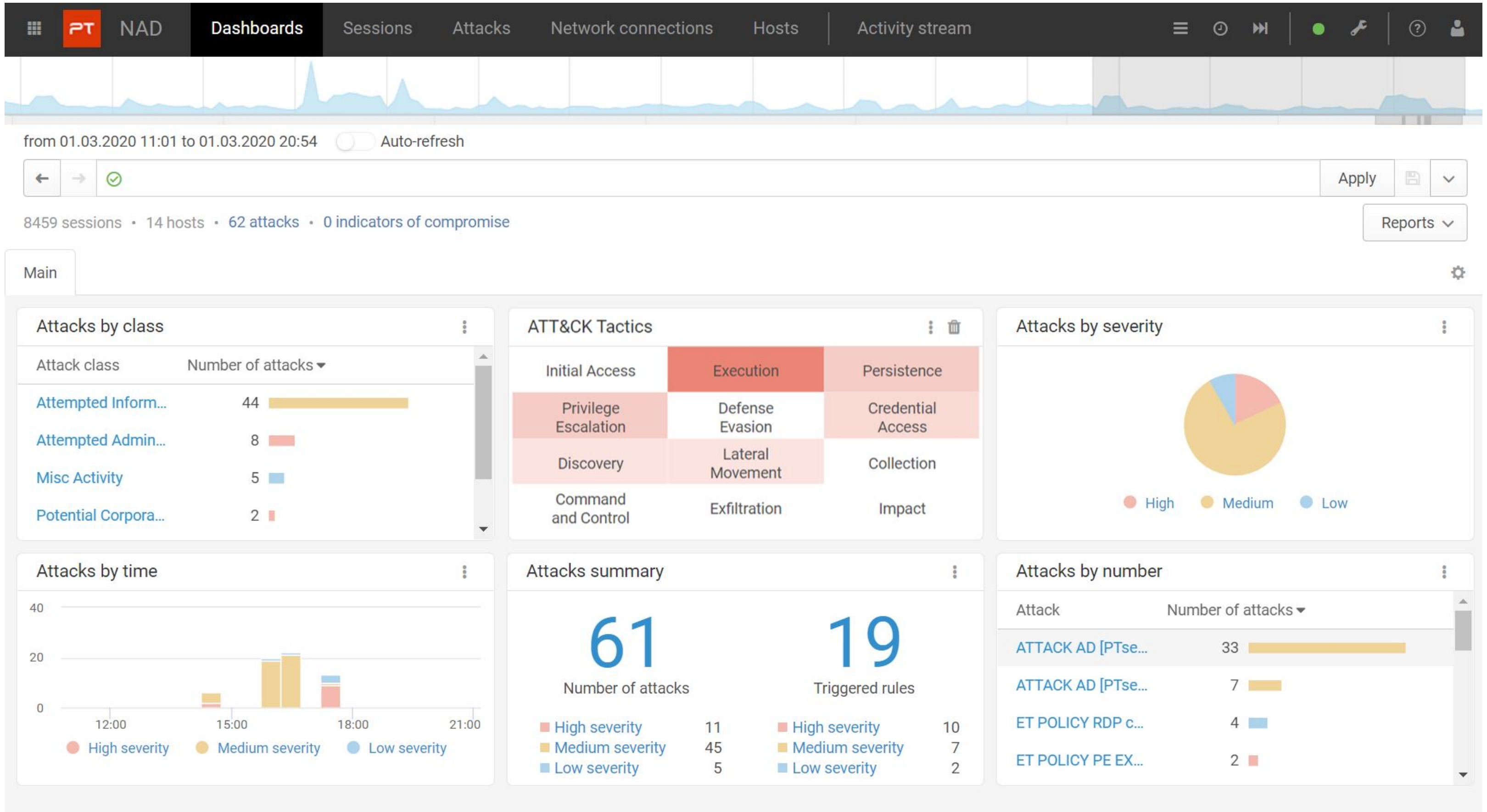
The Positive Technologies **solution**

ptsecurity.com

PT Network Attack Discovery

PT NAD is a deep network traffic analysis system designed to detect attacks on the perimeter and inside the network.

The system makes hidden threats visible, detects suspicious activity even in encrypted traffic, and helps investigate incidents.



from 01.03.2020 11:01 to 01.03.2020 20:54

8459 sessions • 14 hosts • 62 attacks • 0 indicators of compromise

Attacks by class

Attack class	Number of attacks
Attempted Inform...	44
Attempted Admin...	8
Misc Activity	5
Potential Corpora...	2

ATT&CK Tactics

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

Attacks by severity

Attacks by time

High severity ● Medium severity ● Low severity

Attacks summary

61		19	
Number of attacks		Triggered rules	
High severity	11	High severity	10
Medium severity	45	Medium severity	7
Low severity	5	Low severity	2

Attacks by number

Attack	Number of attacks
ATTACK AD [PTse...	33
ATTACK AD [PTse...	7
ET POLICY RDP c...	4
ET POLICY PE EX...	2

Key functions

Provides network visibility

PT NAD identifies 85 protocols and parses the 30 most common ones up to and including the L7 level. This provides a full picture of what is going on in the infrastructure and helps identify security flaws that can enable attacks.

Detects hidden threats

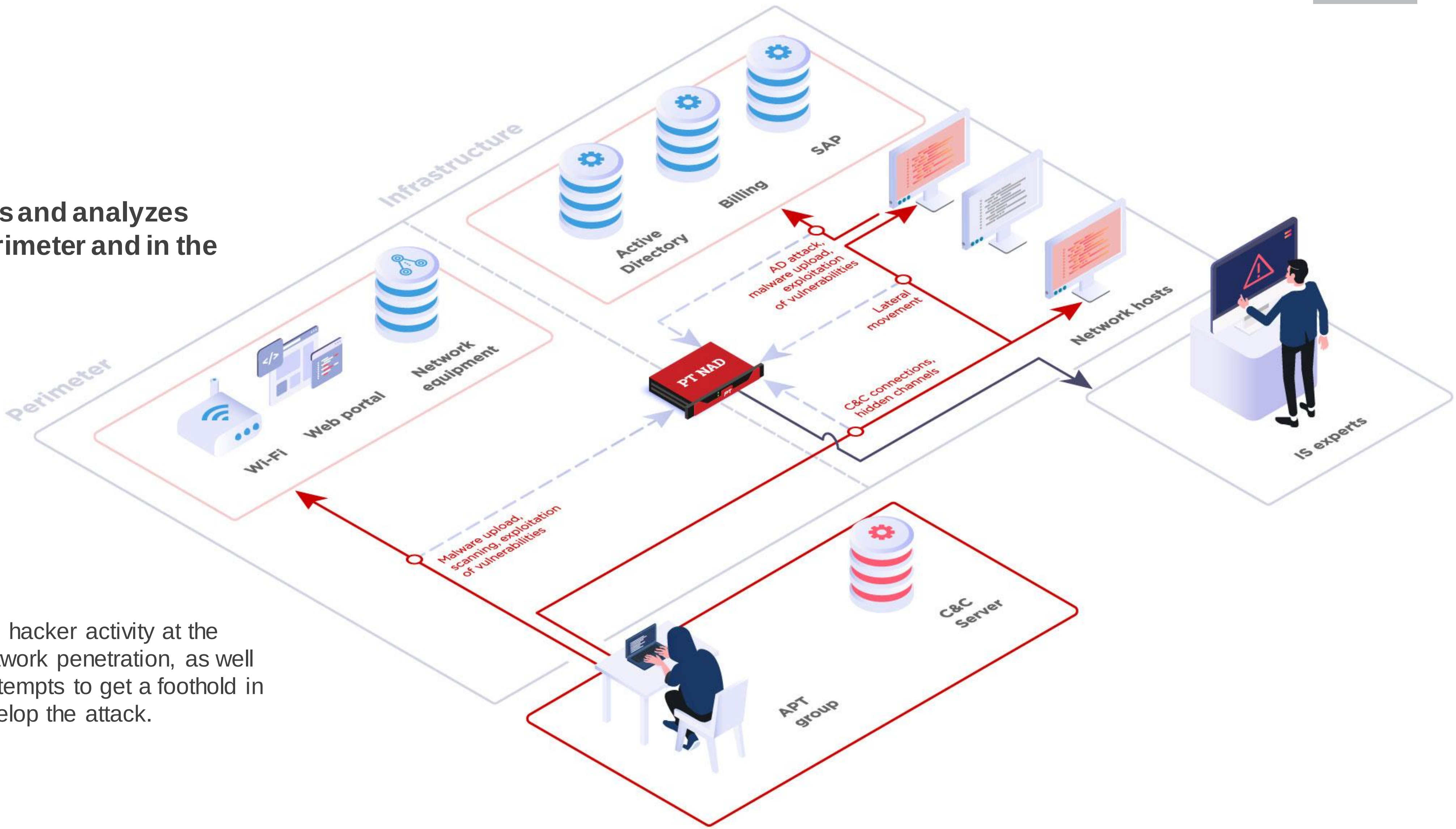
The system automatically detects attacker attempts to penetrate the network and identifies hacker presence in the infrastructure based on multiple signs, including the use of hacker tools and transmission of data to the attackers' servers.

Makes SOCs more effective

PT NAD provides SOCs with full network visibility, makes it easier to verify whether an attack was successful, reconstruct the kill chain and gather evidence. To do this, PT NAD stores metadata and raw traffic, helps quickly find sessions and identify suspicious ones, and supports exporting and importing traffic.

How PT NAD works

PT NAD captures and analyzes traffic on the perimeter and in the infrastructure.


Infrastructure
Active Directory
Billing
SAP
Perimeter
Wi-Fi
Web portal
Network equipment
PT NAD
AD attack, malware upload, exploitation of vulnerabilities
Lateral movement
C&C connections, hidden channels
Malware upload, scanning, exploitation of vulnerabilities
Network hosts
IS experts
C&C Server
APT group

This allows detecting hacker activity at the earliest stages of network penetration, as well as during attacker attempts to get a foothold in the network and develop the attack.

PT NAD detects

- Attacker lateral movement
- Threats in encrypted traffic
- Connection to automatically generated domains
- Non-compliance with IS policies
- Use of hacker tools
- Exploitation of vulnerabilities in the network
- Malware activity
- Signs of previously unnoticed attacks
- Hiding activities from security tools

Threats in encrypted traffic

Thanks to advanced analytics, PT NAD accurately detects malware hidden in TLS or custom protocols.

PT NAD detects

Attacker lateral movement

PT NAD detects attacker attempts to expand their presence in the infrastructure by observing them as they perform reconnaissance, remote command execution, and conduct Active Directory and Kerberos attacks.

PT NAD detects

Use of hacker tools

PT Expert Security Center (PT ESC) investigates complex attacks, constantly explores new threats, and monitors hacker activities. Based on obtained knowledge, our experts create PT NAD rules that help detecting all popular hacking tools in action

PT NAD detects

Exploitation of vulnerabilities
in the network

PT NAD detects

A unique vulnerability database is constantly updated with data about new vulnerabilities, including those that have not yet been included in the CVE database. This helps PT NAD quickly detect exploitation attempts.

Positive Technologies is a **MAPP member**. We receive information about zero-day vulnerabilities in Microsoft's products. That's why PT NAD's customers get protection faster.

Malware activity

PT NAD detects malware by its activity in the network. Hackers can easily hide malware from antivirus tools, whereas hiding its network activity is much more difficult. By analyzing network activity, PT NAD helps localize threats

PT NAD detects

Signs of previously unnoticed attacks

As soon as the PT NAD database is updated with data on new cyberthreats, the system performs **retrospective analysis of traffic** to check network for threats. This allows discovering the presence of attackers in record time.

PT NAD detects

Hiding malicious activity
from security tools

PT NAD detects DNS, HTTP, SMTP, and ICMP tunnels used by attackers to steal data, enable malware communication with the C&C server, and hide their activity from security team

PT NAD detects

Connection to automatically generated domains

PT NAD detects

Thanks to machine learning technology, PT NAD identifies connection with domain names created with the domain generation algorithm (DGA). This helps to detect malware that uses DGA to maintain connection with the attacker's C&C server.

Non-compliance
with IS policies

PT NAD helps detect **transfer of unencrypted data and messages**, use of VPN tunnels, TOR, remote access utilities, proxies, and messengers usually prohibited by IS policies in companies.

PT NAD detects

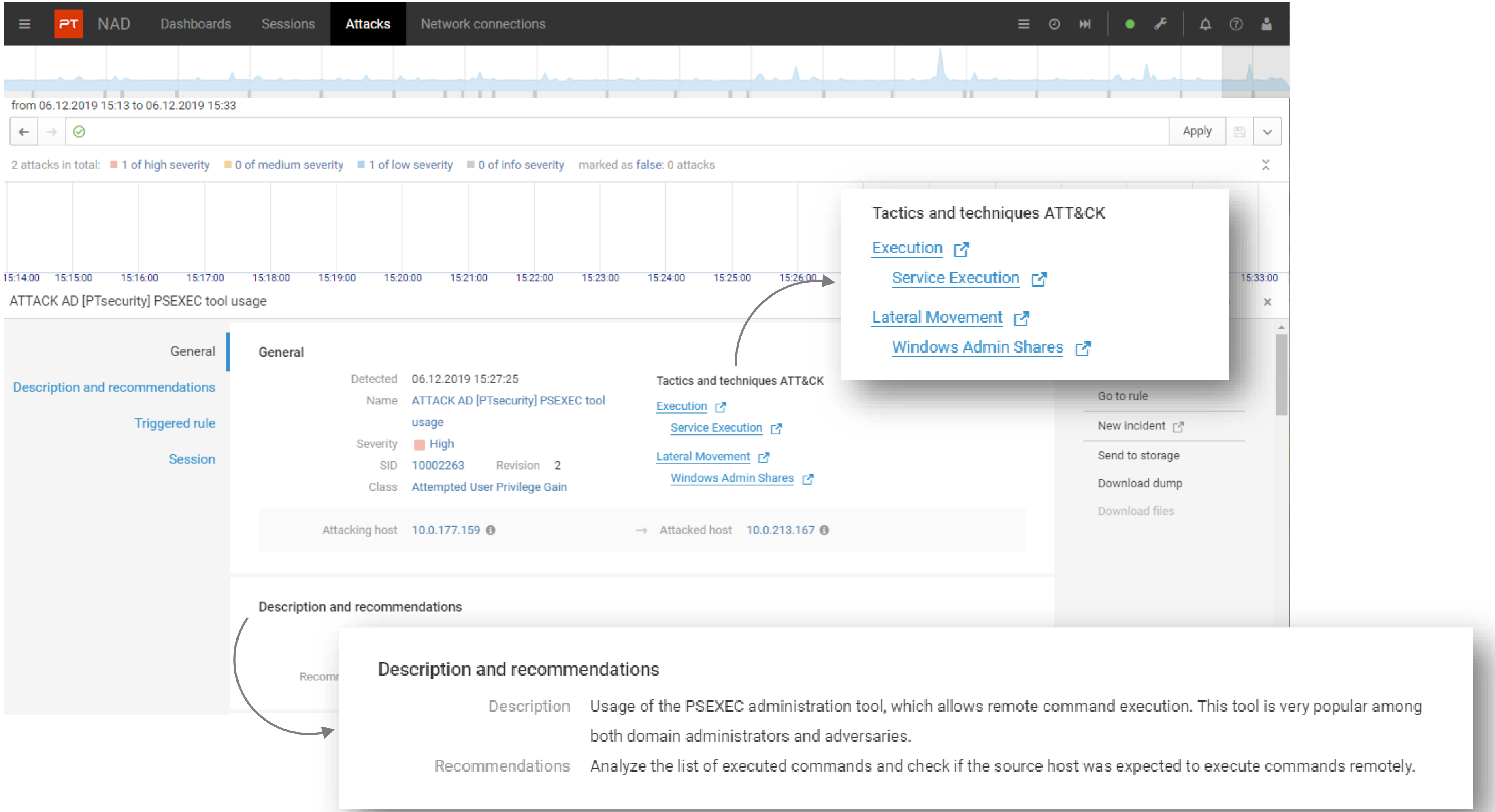
ATT&CK techniques covered by PT NAD

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	CMSTP	External Remote Services	Valid Accounts	CMSTP	Brute Force	Account Discovery	Component Object Model and Distributed COM	Data from Network Shared Drive	Commonly Used Port	Exfiltration Over Alternative Protocol	Network Denial of Service
Exploit Public-Facing Application	Command-Line Interface	Scheduled Task		Connection Proxy	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Man in the Browser	Connection Proxy	Exfiltration Over Command and Control Channel	Resource Hijacking
External Remote Services	Component Object Model and Distributed COM	Valid Accounts		DCShadow	Exploitation for Credential Access	Network Service Scanning	Pass the Hash		Custom Command and Control Protocol		Service Stop
Spearphishing Attachment	Exploitation for Client Execution	Web Shell		Exploitation for Defense Evasion	Kerberoasting	Network Share Discovery	Pass the Ticket		Custom Cryptographic Protocol		
Spearphishing Link	Mshta	Windows Management Instrumentation Event Subscription		Mshta		Password Policy Discovery	Remote Desktop Protocol		Data Encoding		
Trusted Relationship	PowerShell			Obfuscated Files or Information		Permission Groups Discovery	Remote Services		Data Obfuscation		
Valid Accounts	Scheduled Task			Redundant Access		Remote System Discovery	Third-party Software		Domain Generation Algorithms		
	Scripting			Scripting		Security Software Discovery	Windows Admin Shares		Fallback Channels		
	Service Execution			Software Packing		System Owner/User Discovery	Windows Remote Management		Multi-hop Proxy		
	Third-party Software					System Service Discovery			Multi-Stage Channels		
	User Execution								Multiband Communication		
	Windows Management Instrumentation								Multilayer Encryption		
	Windows Remote Management								Remote Access Tools		
	XSL Script Processing								Remote File Copy		
									Standard Application Layer Protocol		
									Standard Cryptographic Protocol		
									Standard Non-Application Layer Protocol		
									Uncommonly Used Port		

up to 20%	20–50%	over 50%

PT NAD detects over 50% of techniques used by attackers during initial access, lateral movement, and command and control communications.

Detection of ATT&CK tactics and techniques



from 06.12.2019 15:13 to 06.12.2019 15:33

2 attacks in total: 1 of high severity 0 of medium severity 1 of low severity 0 of info severity marked as false: 0 attacks

ATTACK AD [PTsecurity] PSEXEC tool usage

General

Detected	06.12.2019 15:27:25
Name	ATTACK AD [PTsecurity] PSEXEC tool usage
Severity	🟥 High
SID	10002263 Revision 2
Class	Attempted User Privilege Gain

Tactics and techniques ATT&CK

- Execution
  - Service Execution
- Lateral Movement
  - Windows Admin Shares

Attacking host 10.0.177.159 → Attacked host 10.0.213.167

Description and recommendations

Tactics and techniques ATT&CK

- Execution
  - Service Execution
- Lateral Movement
  - Windows Admin Shares

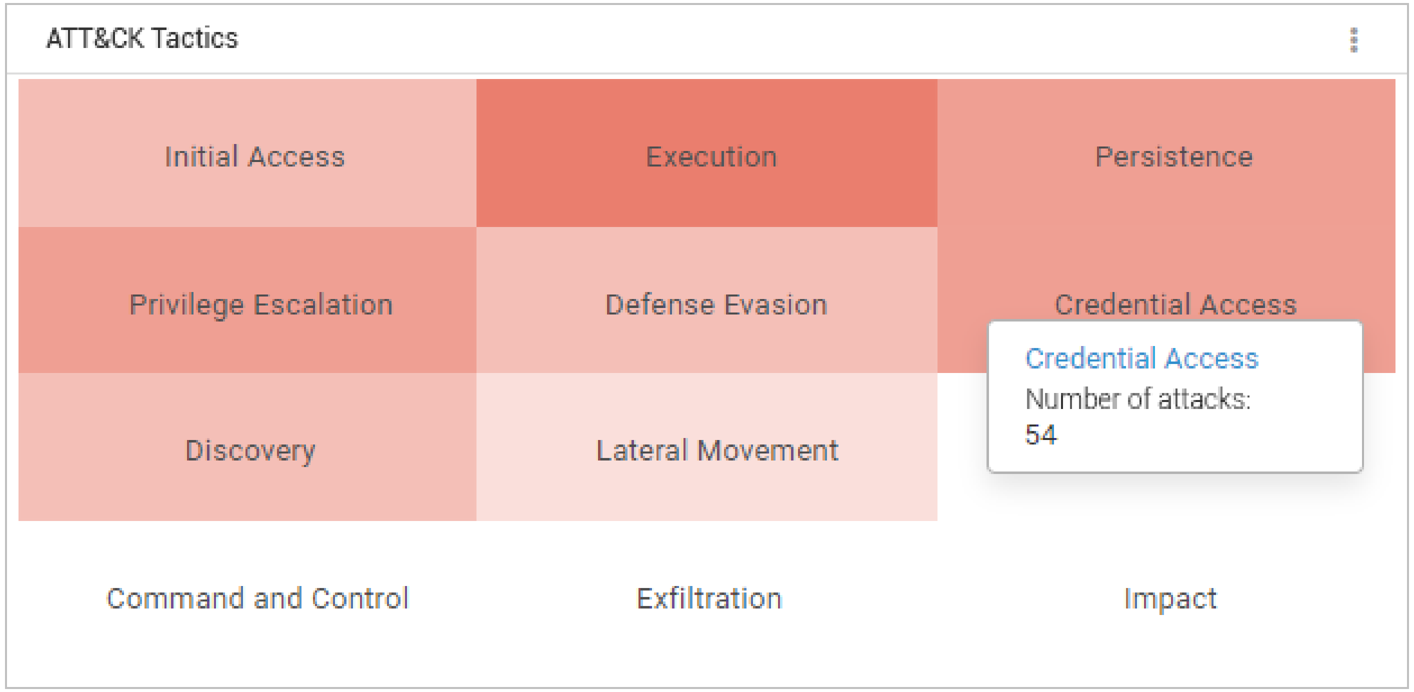
Description and recommendations

Description	Usage of the PSEXEC administration tool, which allows remote command execution. This tool is very popular among both domain administrators and adversaries.
Recommendations	Analyze the list of executed commands and check if the source host was expected to execute commands remotely.

An attack card contains data about used ATT&CK tactics and techniques.

This helps to understand which stage of attack attackers are in and quickly choose compensating measures.

Heat map of ATT&CK tactics and techniques



ATT&CK Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Credential Access
Number of attacks:
54

Discovery

Lateral Movement

Command and Control

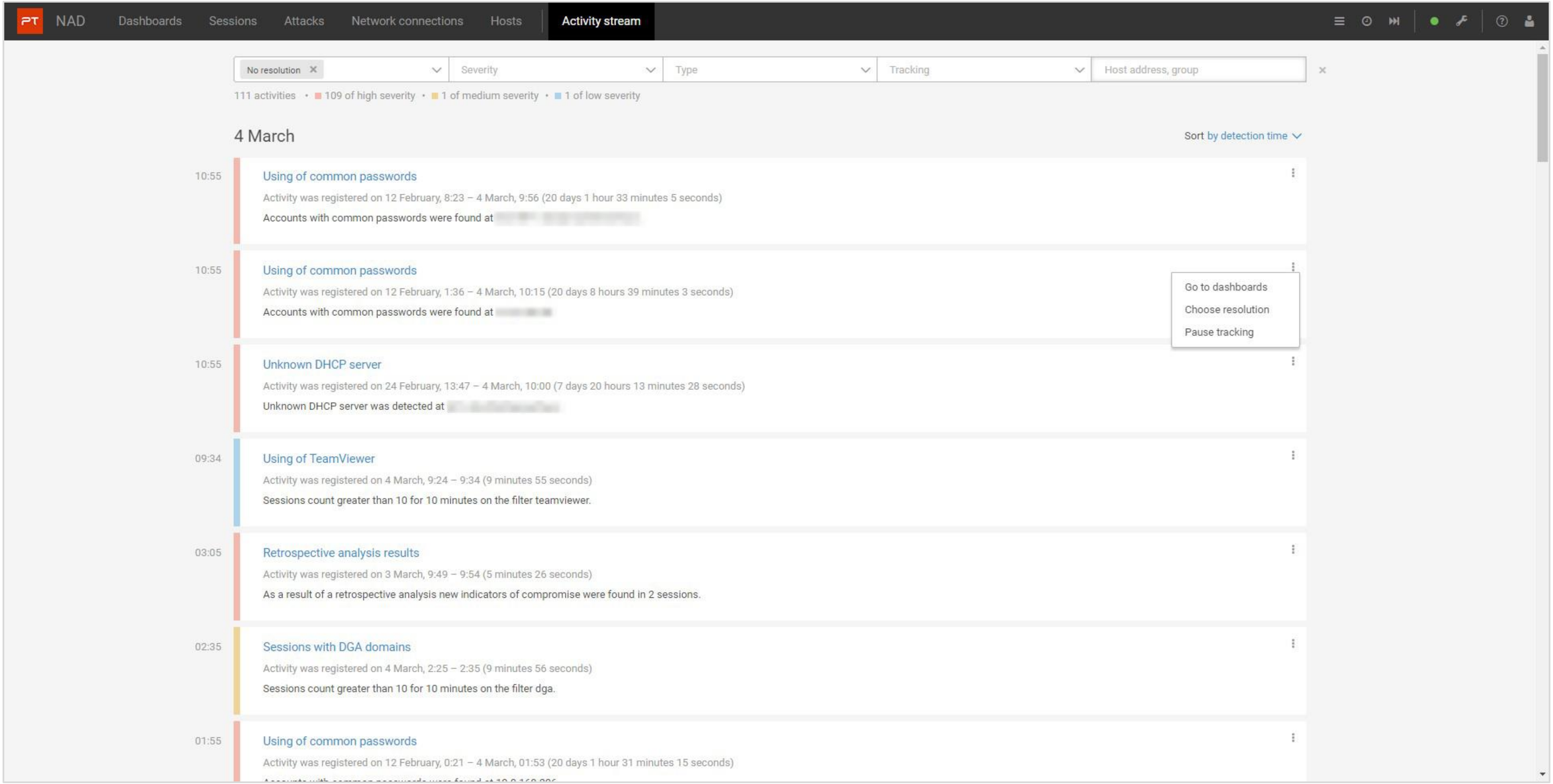
Exfiltration

Impact

The heat map on a dashboard provides a comprehensive view on a phase of cyberattacks.

Every tactic is clickable and shows the frequency of techniques used.

Learn about new attacks and threats in a single feed



111 activities • 109 of high severity • 1 of medium severity • 1 of low severity

4 March

Sort by detection time

10:55 Using of common passwords
Activity was registered on 12 February, 8:23 – 4 March, 9:56 (20 days 1 hour 33 minutes 5 seconds)
Accounts with common passwords were found at [redacted]

10:55 Using of common passwords
Activity was registered on 12 February, 1:36 – 4 March, 10:15 (20 days 8 hours 39 minutes 3 seconds)
Accounts with common passwords were found at [redacted]

10:55 Unknown DHCP server
Activity was registered on 24 February, 13:47 – 4 March, 10:00 (7 days 20 hours 13 minutes 28 seconds)
Unknown DHCP server was detected at [redacted]

09:34 Using of TeamViewer
Activity was registered on 4 March, 9:24 – 9:34 (9 minutes 55 seconds)
Sessions count greater than 10 for 10 minutes on the filter teamviewer.

03:05 Retrospective analysis results
Activity was registered on 3 March, 9:49 – 9:54 (5 minutes 26 seconds)
As a result of a retrospective analysis new indicators of compromise were found in 2 sessions.

02:35 Sessions with DGA domains
Activity was registered on 4 March, 2:25 – 2:35 (9 minutes 56 seconds)
Sessions count greater than 10 for 10 minutes on the filter dga.

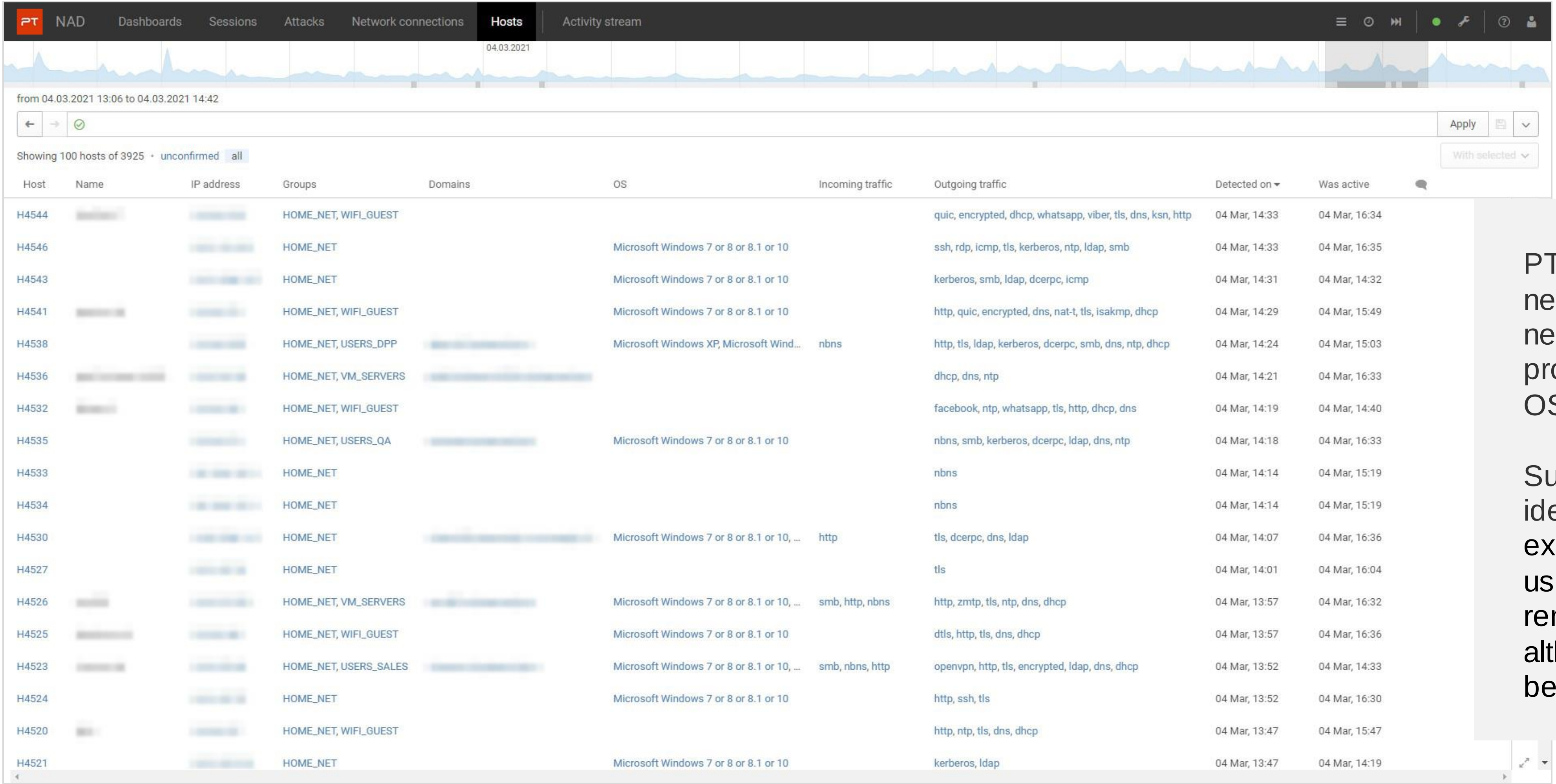
01:55 Using of common passwords
Activity was registered on 12 February, 0:21 – 4 March, 01:53 (20 days 1 hour 31 minutes 15 seconds)

Each activity in the feed contains the date and time of the last detection, severity level, period of activity, and a brief description

Activity feed collects a list of identified threats in one place, combines messages about similar activities into one, and allows you to manage them.

You can mark the issue as resolved or no longer track such activity.

Monitor network hosts



from 04.03.2021 13:06 to 04.03.2021 14:42

Showing 100 hosts of 3925 • unconfirmed all

Host	Name	IP address	Groups	Domains	OS	Incoming traffic	Outgoing traffic	Detected on	Was active
H4544	[redacted]	[redacted]	HOME_NET, WIFI_GUEST				quic, encrypted, dhcp, whatsapp, viber, tls, dns, ksn, http	04 Mar, 14:33	04 Mar, 16:34
H4546		[redacted]	HOME_NET		Microsoft Windows 7 or 8 or 8.1 or 10		ssh, rdp, icmp, tls, kerberos, ntp, ldap, smb	04 Mar, 14:33	04 Mar, 16:35
H4543		[redacted]	HOME_NET		Microsoft Windows 7 or 8 or 8.1 or 10		kerberos, smb, ldap, dcerpc, icmp	04 Mar, 14:31	04 Mar, 14:32
H4541	[redacted]	[redacted]	HOME_NET, WIFI_GUEST		Microsoft Windows 7 or 8 or 8.1 or 10		http, quic, encrypted, dns, nat-t, tls, isakmp, dhcp	04 Mar, 14:29	04 Mar, 15:49
H4538		[redacted]	HOME_NET, USERS_DPP	[redacted]	Microsoft Windows XP, Microsoft Wind...	nbns	http, tls, ldap, kerberos, dcerpc, smb, dns, ntp, dhcp	04 Mar, 14:24	04 Mar, 15:03
H4536	[redacted]	[redacted]	HOME_NET, VM_SERVERS	[redacted]			dhcp, dns, ntp	04 Mar, 14:21	04 Mar, 16:33
H4532	[redacted]	[redacted]	HOME_NET, WIFI_GUEST				facebook, ntp, whatsapp, tls, http, dhcp, dns	04 Mar, 14:19	04 Mar, 14:40
H4535		[redacted]	HOME_NET, USERS_QA	[redacted]	Microsoft Windows 7 or 8 or 8.1 or 10		nbns, smb, kerberos, dcerpc, ldap, dns, ntp	04 Mar, 14:18	04 Mar, 16:33
H4533		[redacted]	HOME_NET				nbns	04 Mar, 14:14	04 Mar, 15:19
H4534		[redacted]	HOME_NET				nbns	04 Mar, 14:14	04 Mar, 15:19
H4530		[redacted]	HOME_NET	[redacted]	Microsoft Windows 7 or 8 or 8.1 or 10, ...	http	tls, dcerpc, dns, ldap	04 Mar, 14:07	04 Mar, 16:36
H4527		[redacted]	HOME_NET				tls	04 Mar, 14:01	04 Mar, 16:04
H4526	[redacted]	[redacted]	HOME_NET, VM_SERVERS	[redacted]	Microsoft Windows 7 or 8 or 8.1 or 10, ...	smb, http, nbns	http, zmtp, tls, ntp, dns, dhcp	04 Mar, 13:57	04 Mar, 16:32
H4525	[redacted]	[redacted]	HOME_NET, WIFI_GUEST		Microsoft Windows 7 or 8 or 8.1 or 10		dtls, http, tls, dns, dhcp	04 Mar, 13:57	04 Mar, 16:36
H4523	[redacted]	[redacted]	HOME_NET, USERS_SALES	[redacted]	Microsoft Windows 7 or 8 or 8.1 or 10, ...	smb, nbns, http	openvpn, http, tls, encrypted, ldap, dns, dhcp	04 Mar, 13:52	04 Mar, 14:33
H4524		[redacted]	HOME_NET		Microsoft Windows 7 or 8 or 8.1 or 10		http, ssh, tls	04 Mar, 13:52	04 Mar, 16:30
H4520	[redacted]	[redacted]	HOME_NET, WIFI_GUEST				http, ntp, tls, dns, dhcp	04 Mar, 13:47	04 Mar, 15:47
H4521		[redacted]	HOME_NET		Microsoft Windows 7 or 8 or 8.1 or 10		kerberos, ldap	04 Mar, 13:47	04 Mar, 14:19

PT NAD users will know if a new host has appeared on the network, an application protocol has changed, or the OS has changed.

Such data can also help identify suspicious activity. For example, if a user started using the SSH protocol to remotely control the OS, although they did not do it before, it is worth investigating.

Benefits

Detects malicious activities in internal traffic

PT NAD analyzes both north/south and east/west traffic and detects lateral movement, attempts to exploit vulnerabilities, and attacks against end users in the domain and internal services.

Detects even modified malware

In order to be able to create rules, our experts constantly explore existing hacker techniques, tools, and malware samples. One rule covers the entire malware family. As a result, PT NAD alerts about all the dangerous threats and detects even modified versions of malware.

Keeps attacks private

PT NAD is an on-premise solution. All data is stored on client infrastructure, never leaving the corporate perimeter. Information on attacks and damage is not transmitted to the outside, minimizing reputational risks.

Support by PT Expert Security Center

Positive Technologies Expert Security Center leverages its expertise to assist information security experts or even takes the full lead in monitoring network traffic events and investigating attacks.

PT NAD usage scenarios

ptsecurity.com

Usage scenarios

PT

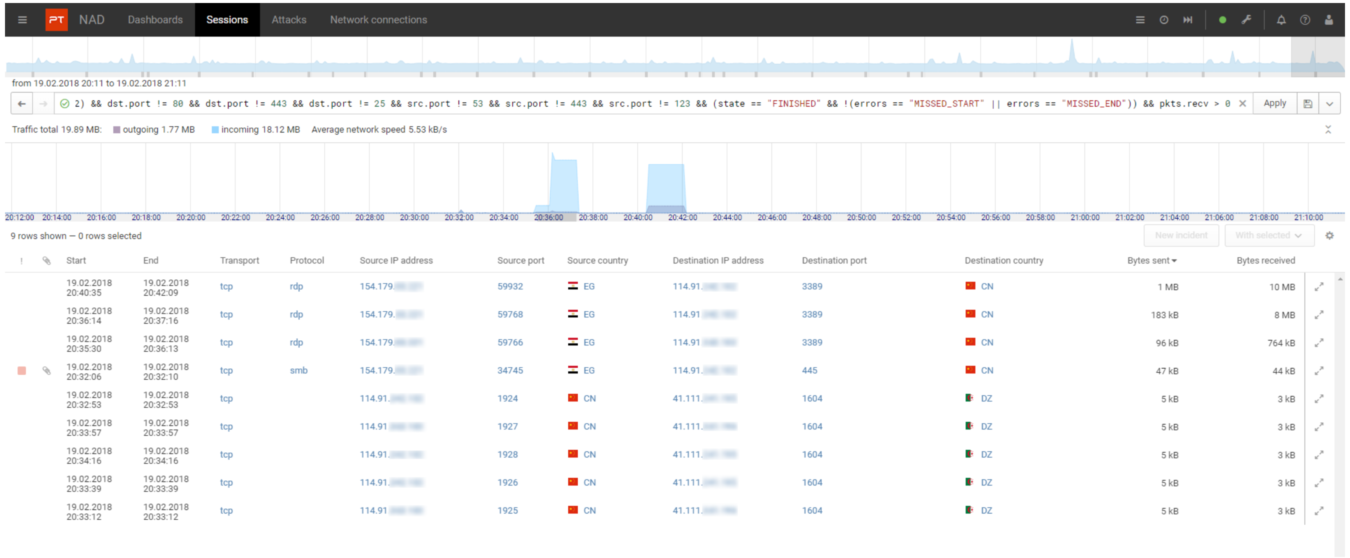
PT NAD

- Information security policy compliance control
- Detection of attacks on the perimeter and in the network
- Investigation of attacks
- Threat hunting

IS policy compliance control

PT NAD detects flaws in information systems' configuration and non-compliance with information security policy that can lead to the development of attacks.

Filters help quickly identify credentials stored in cleartext, unencrypted messages, remote access utilities, and tools that hide network activity.



from 19.02.2018 20:11 to 19.02.2018 21:11

```
2) && dst.port != 80 && dst.port != 443 && dst.port != 25 && src.port != 53 && src.port != 443 && src.port != 123 && (state == "FINISHED" && !(errors == "MISSED_START" || errors == "MISSED_END")) && pkts.recv > 0
```

Traffic total 19.89 MB: ■ outgoing 1.77 MB ■ incoming 18.12 MB Average network speed 5.53 kB/s

9 rows shown — 0 rows selected

!		Start	End	Transport	Protocol	Source IP address	Source port	Source country	Destination IP address	Destination port	Destination country	Bytes sent	Bytes received
		19.02.2018 20:40:35	19.02.2018 20:42:09	tcp	rdp	154.179.[redacted]	59932	EG	114.91.[redacted]	3389	CN	1 MB	10 MB
		19.02.2018 20:36:14	19.02.2018 20:37:16	tcp	rdp	154.179.[redacted]	59768	EG	114.91[redacted]	3389	CN	183 kB	8 MB
		19.02.2018 20:35:30	19.02.2018 20:36:13	tcp	rdp	154.179.[redacted]	59766	EG	114.91[redacted]	3389	CN	96 kB	764 kB
■	📎	19.02.2018 20:32:06	19.02.2018 20:32:10	tcp	smb	154.179.[redacted]	34745	EG	114.91.[redacted]	445	CN	47 kB	44 kB
		19.02.2018 20:32:53	19.02.2018 20:32:53	tcp		114.91.[redacted]	1924	CN	41.111.[redacted]	1604	DZ	5 kB	3 kB
		19.02.2018 20:33:57	19.02.2018 20:33:57	tcp		114.91[redacted]	1927	CN	41.111.[redacted]	1604	DZ	5 kB	3 kB
		19.02.2018 20:34:16	19.02.2018 20:34:16	tcp		114.91.[redacted]	1928	CN	41.111.[redacted]	1604	DZ	5 kB	3 kB
		19.02.2018 20:33:39	19.02.2018 20:33:39	tcp		114.91.[redacted]	1926	CN	41.111.[redacted]	1604	DZ	5 kB	3 kB
		19.02.2018 20:33:12	19.02.2018 20:33:12	tcp		114.91[redacted]	1925	CN	41.111.[redacted]	1604	DZ	5 kB	3 kB

100% of companies suffer from the non-compliance with information security policy*.

*Top cyberthreats on enterprise networks, Positive Technologies

Example

COMPLIANCE CONTROL

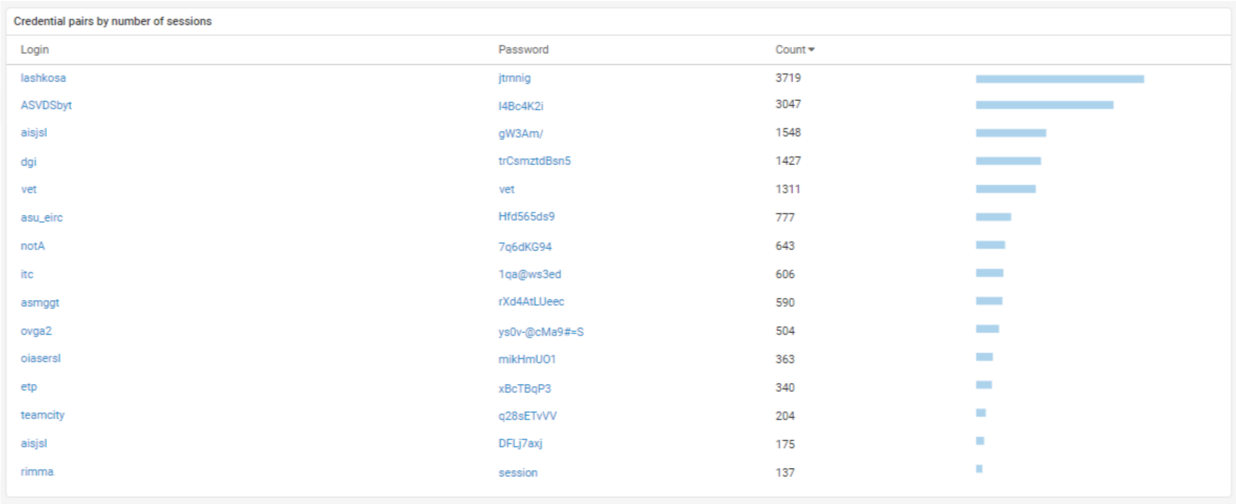
DETECTION OF ATTACKS

INVESTIGATION OF ATTACKS

THREAT HUNTING

Plaintext credentials are all over the network. Hackers can easily intercept them by compromising the network.

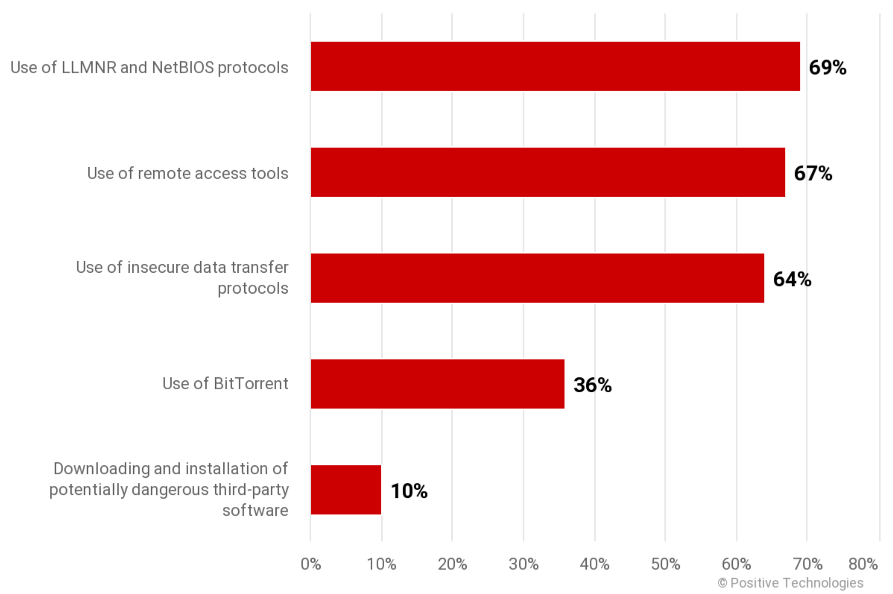
PT NAD filter helps configure a special widget to view all non-encrypted passwords and logins:



Credential pairs by number of sessions

Login	Password	Count ▾
lashkosa	jtmnig	3719
ASVDSbyt	I4Bc4K2i	3047
aisjsl	gW3Am/	1548
dgi	trCsmztdBsn5	1427
vet	vet	1311
asu_eirc	Hfd565ds9	777
notA	7q6dKG94	643
itc	1qa@ws3ed	606
asmggt	rXd4AtLUeec	590
ovga2	ys0v-@cMa9#=S	504
oiasersl	mikHmUO1	363
etp	xBcTBqP3	340
teamcity	q28sETvVV	204
aisjsl	DFLj7axj	175
rimma	session	137

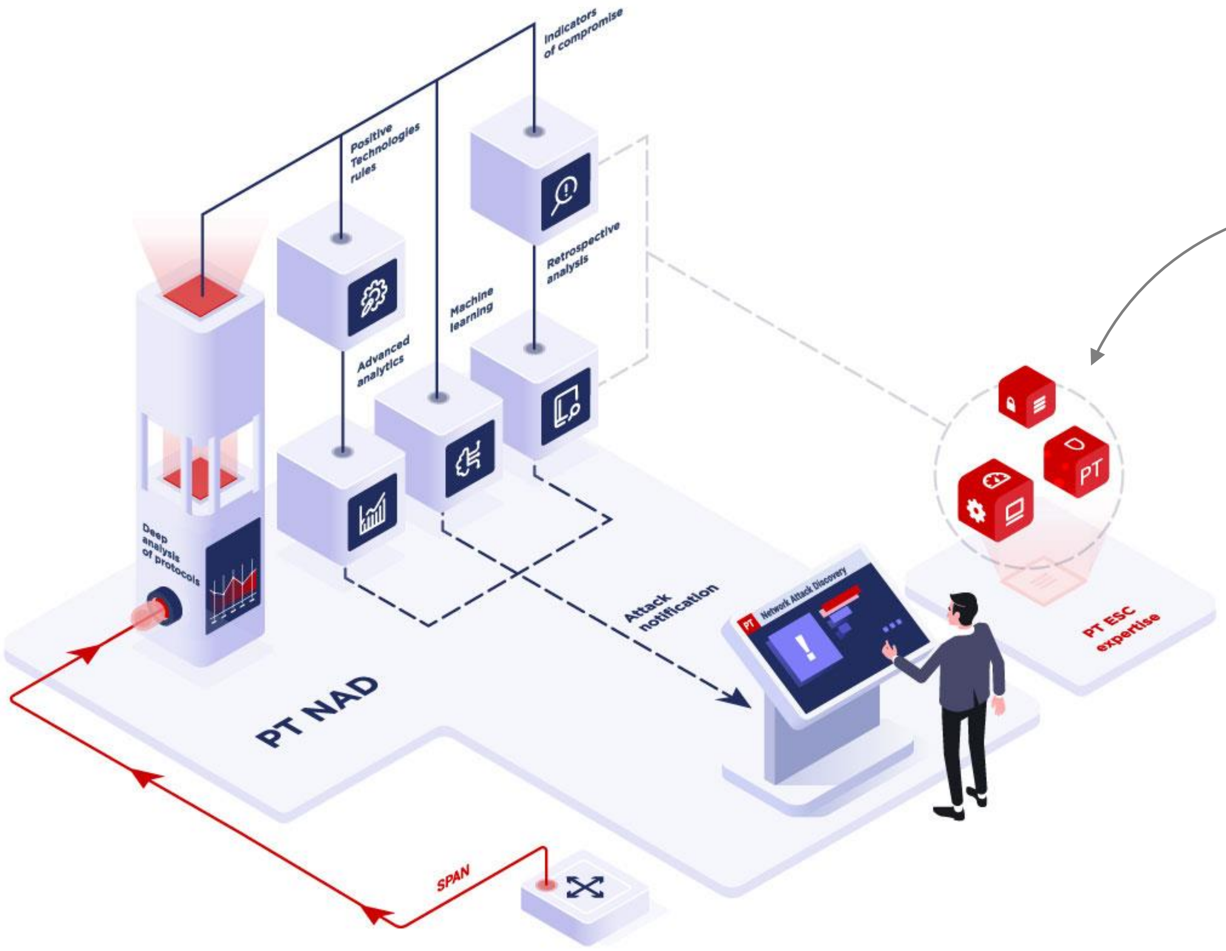
PT NAD shows you sessions in which plaintext data was transmitted, as well as senders' and recipients' host addresses.



Top 5 types of non-compliance with IS policies

*Top cyberthreats on enterprise networks, Positive Technologies

Detection of attacks on the perimeter and in the network



PT Expert Security Center updates rules and indicators of compromise twice a week. In order to update the database, PT NAD does not require constant connection to the Positive Technologies cloud.

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

Advanced analytics modules enable identification of complex threats and network anomalies. They take into account many parameters of the attacker's behavior and are not tied to the analysis of individual sessions, unlike the rules for attack detection.

Example

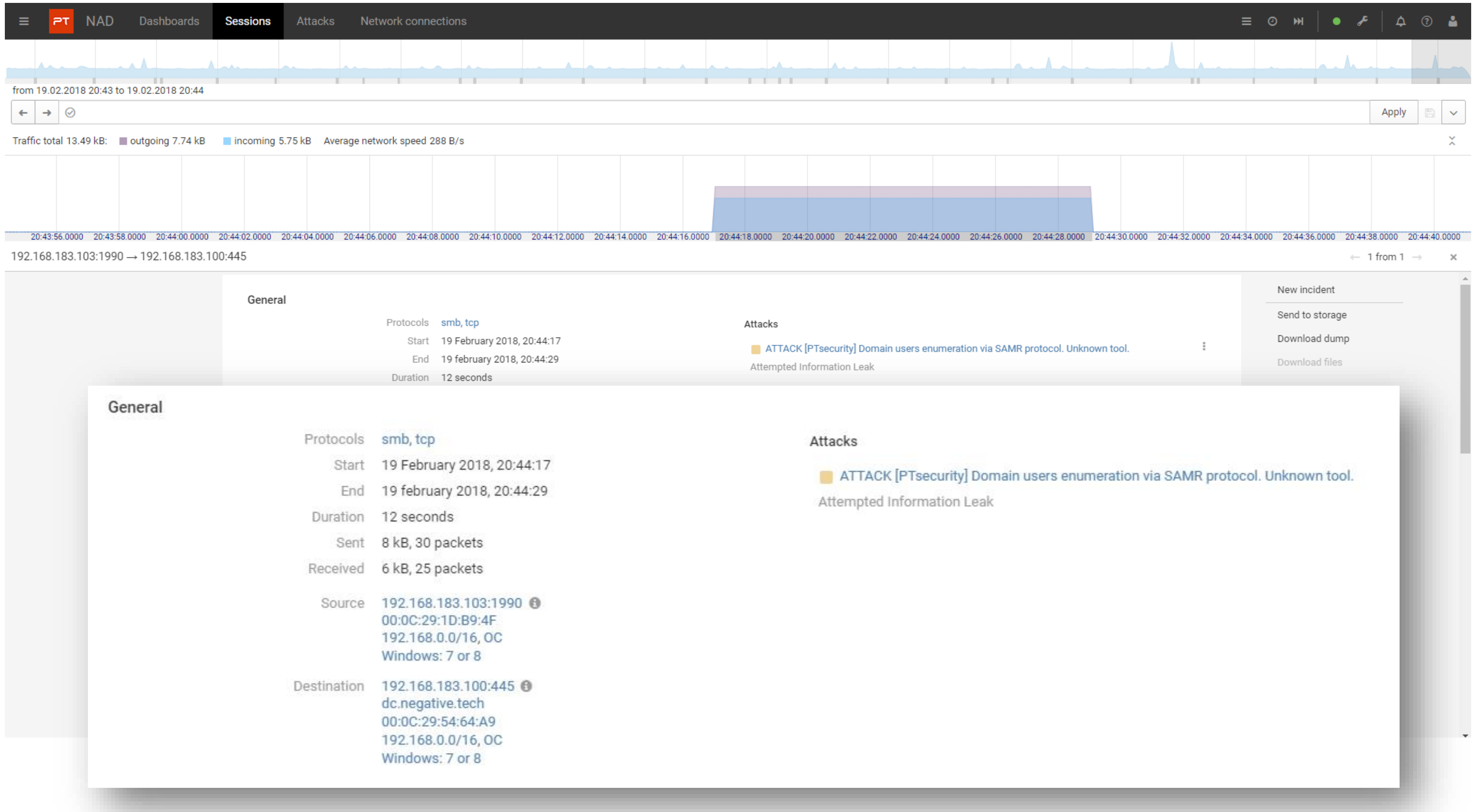
PT NAD interface: a rule is triggered for detecting SMB requests from illegitimate segment.

The goal of attackers is to compromise domain controller of the main company.

Step 1 Attackers penetrate the main company via less protected perimeter of one of its branches.

Step 2 Malefactors attack domain controller from a single network of the company.

Step 3 PT NAD analyzes the SMB protocol and detects illegitimate requests for obtaining a list of domain users.



from 19.02.2018 20:43 to 19.02.2018 20:44

Traffic total 13.49 kB: ▨ outgoing 7.74 kB ▨ incoming 5.75 kB Average network speed 288 B/s

192.168.183.103:1990 → 192.168.183.100:445

General

Protocols smb, tcp
Start 19 February 2018, 20:44:17
End 19 february 2018, 20:44:29
Duration 12 seconds

Attacks

ATTACK [PTsecurity] Domain users enumeration via SAMR protocol. Unknown tool.
Attempted Information Leak

General

Protocols smb, tcp
Start 19 February 2018, 20:44:17
End 19 february 2018, 20:44:29
Duration 12 seconds
Sent 8 kB, 30 packets
Received 6 kB, 25 packets

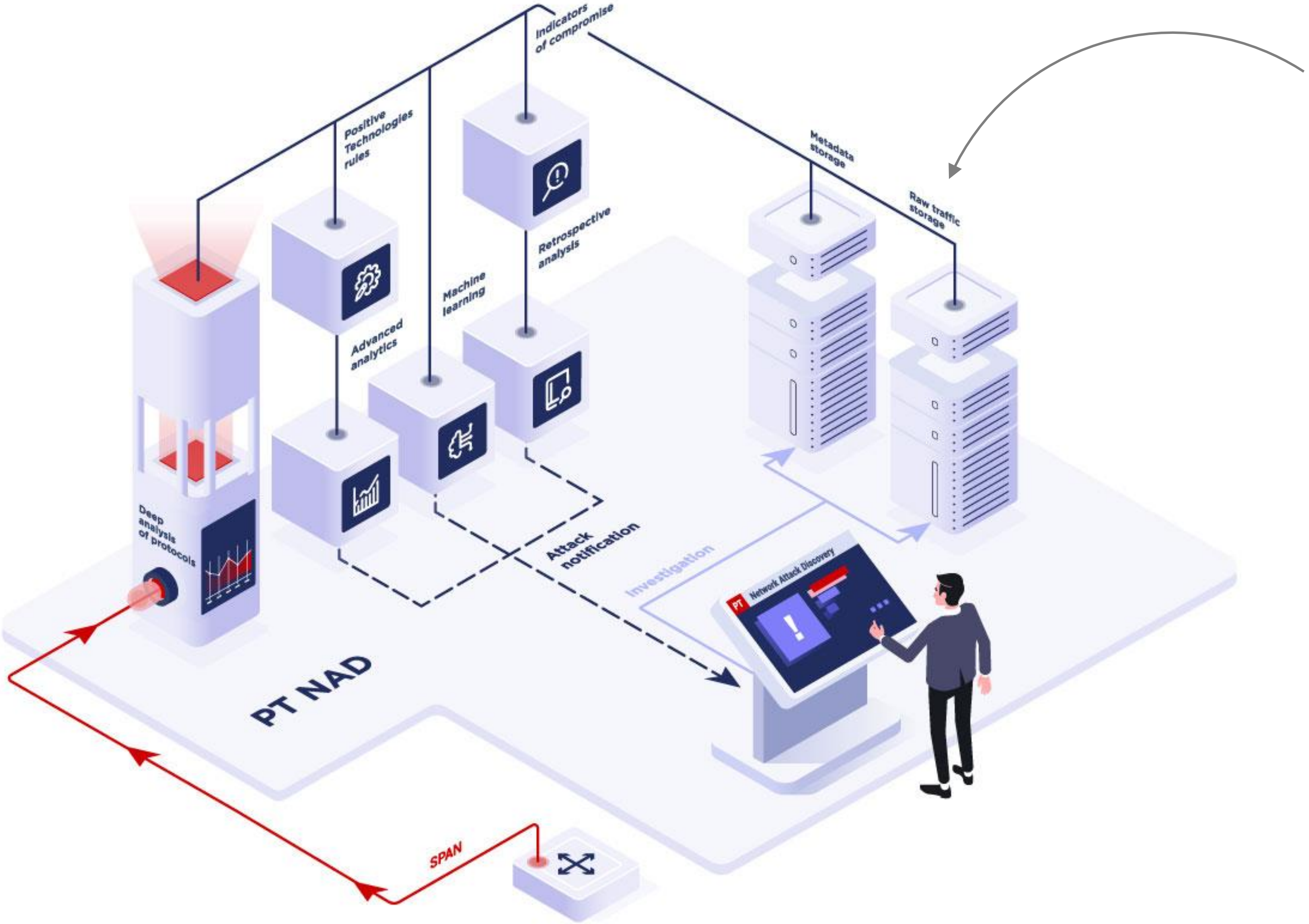
Source 192.168.183.103:1990
00:0C:29:1D:B9:4F
192.168.0.0/16, OC
Windows: 7 or 8

Destination 192.168.183.100:445
dc.negative.tech
00:0C:29:54:64:A9
192.168.0.0/16, OC
Windows: 7 or 8

Attacks

ATTACK [PTsecurity] Domain users enumeration via SAMR protocol. Unknown tool.
Attempted Information Leak

Investigation of attacks



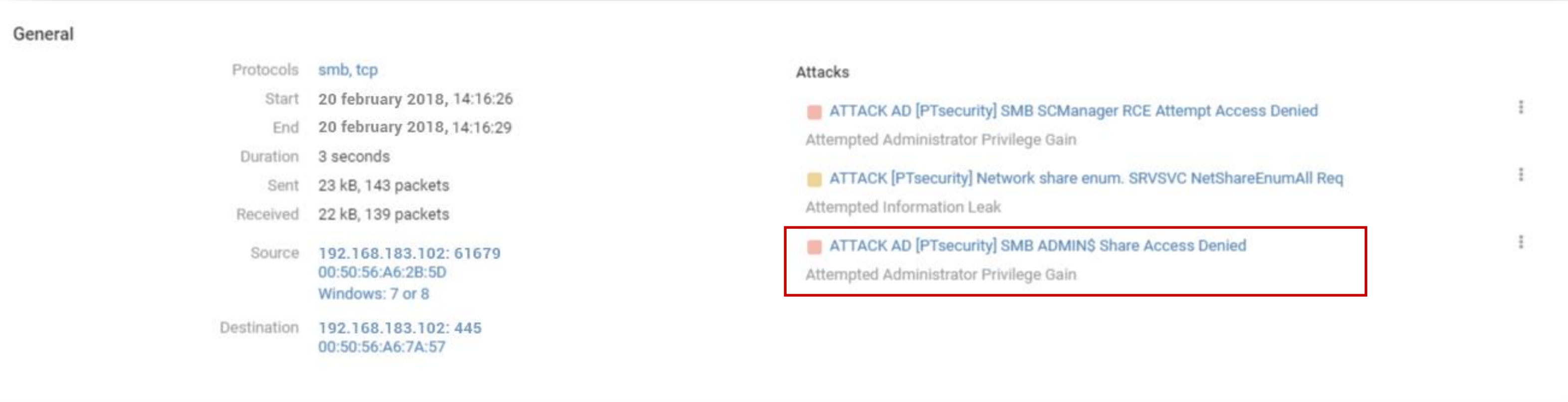
Flexible data storage system
Users can select parameters to store metadata and raw traffic, thus optimizing the storage size.

With PT NAD, an investigation expert can:

- Localize attack.
- Trace the attack path.
- Detect vulnerabilities in infrastructure.
- Set up measures to prevent similar attacks in the future.
- Gather evidence of malicious activity.

Example

1. PT NAD notifies about unsuccessful attempt to log in to domain controller from an account with insufficient rights.
2. A security engineer checked network activity on the host and detected several attempts to log in to other hosts from this host outside business hours.
3. The security engineer asked IT department to block the account and started investigation together with the PT ESC team.



General

Protocols	smb, tcp
Start	20 february 2018, 14:16:26
End	20 february 2018, 14:16:29
Duration	3 seconds
Sent	23 kB, 143 packets
Received	22 kB, 139 packets
Source	192.168.183.102: 61679 00:50:56:A6:2B:5D Windows: 7 or 8
Destination	192.168.183.102: 445 00:50:56:A6:7A:57

Attacks

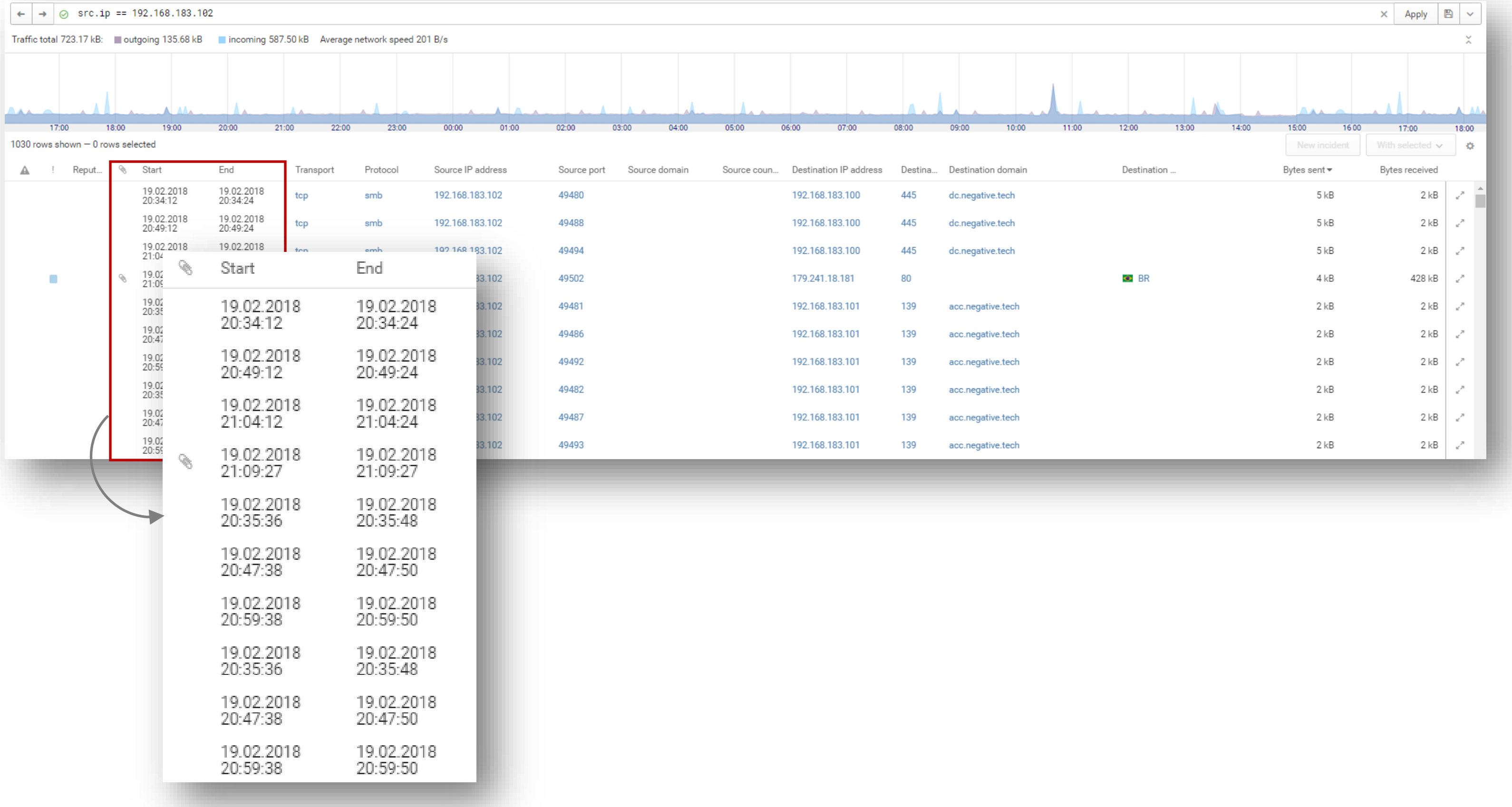
🟥 ATTACK AD [PTsecurity] SMB SCManager RCE Attempt Access Denied
Attempted Administrator Privilege Gain

🟨 ATTACK [PTsecurity] Network share enum. SRVSVC NetShareEnumAll Req
Attempted Information Leak

🟥 ATTACK AD [PTsecurity] SMB ADMIN$ Share Access Denied
Attempted Administrator Privilege Gain

Example

1. PT NAD notifies about unsuccessful attempt to log in to domain controller from an account with insufficient rights.
2. A security engineer checked network activity on the host and detected several attempts to log in to other hosts from this host outside business hours.
3. The security engineer asked IT department to block the account and started investigation together with the PT ESC team.



```
src.ip == 192.168.183.102
```

Traffic total 723.17 kB: ▨ outgoing 135.68 kB ▨ incoming 587.50 kB Average network speed 201 B/s

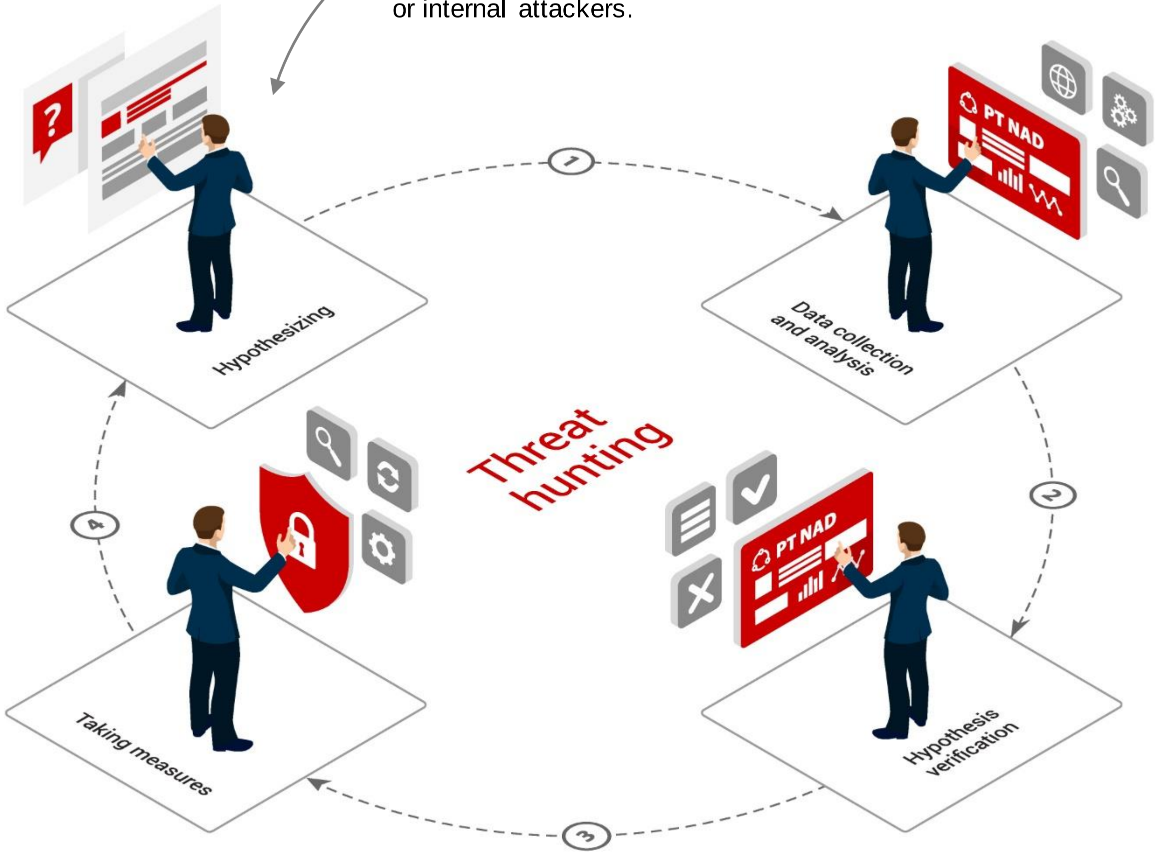
1030 rows shown — 0 rows selected

⚠	!	Reput...	Start	End	Transport	Protocol	Source IP address	Source port	Source domain	Source coun...	Destination IP address	Destina...	Destination domain	Destination ...	Bytes sent ▾	Bytes received
			19.02.2018 20:34:12	19.02.2018 20:34:24	tcp	smb	192.168.183.102	49480			192.168.183.100	445	dc.negative.tech		5 kB	2 kB
			19.02.2018 20:49:12	19.02.2018 20:49:24	tcp	smb	192.168.183.102	49488			192.168.183.100	445	dc.negative.tech		5 kB	2 kB
			19.02.2018 21:04:12	19.02.2018 21:04:24	tcp	smb	192.168.183.102	49494			192.168.183.100	445	dc.negative.tech		5 kB	2 kB
	■		19.02.2018 21:09:27	19.02.2018 21:09:27			3.102	49502			179.241.18.181	80		BR	4 kB	428 kB
			19.02.2018 20:35:36	19.02.2018 20:35:48			3.102	49481			192.168.183.101	139	acc.negative.tech		2 kB	2 kB
			19.02.2018 20:47:38	19.02.2018 20:47:50			3.102	49486			192.168.183.101	139	acc.negative.tech		2 kB	2 kB
			19.02.2018 20:59:38	19.02.2018 20:59:50			3.102	49492			192.168.183.101	139	acc.negative.tech		2 kB	2 kB
			19.02.2018 20:35:36	19.02.2018 20:35:48			3.102	49482			192.168.183.101	139	acc.negative.tech		2 kB	2 kB
			19.02.2018 20:47:38	19.02.2018 20:47:50			3.102	49487			192.168.183.101	139	acc.negative.tech		2 kB	2 kB
			19.02.2018 20:59:38	19.02.2018 20:59:50			3.102	49493			192.168.183.101	139	acc.negative.tech		2 kB	2 kB

Threat hunting

PT NAD helps organize threat hunting in a company and detect hidden threats that can not be identified with standard cybersecurity tools.

For example, hypotheses on the presence of hackers in the network, data leak, or internal attackers.



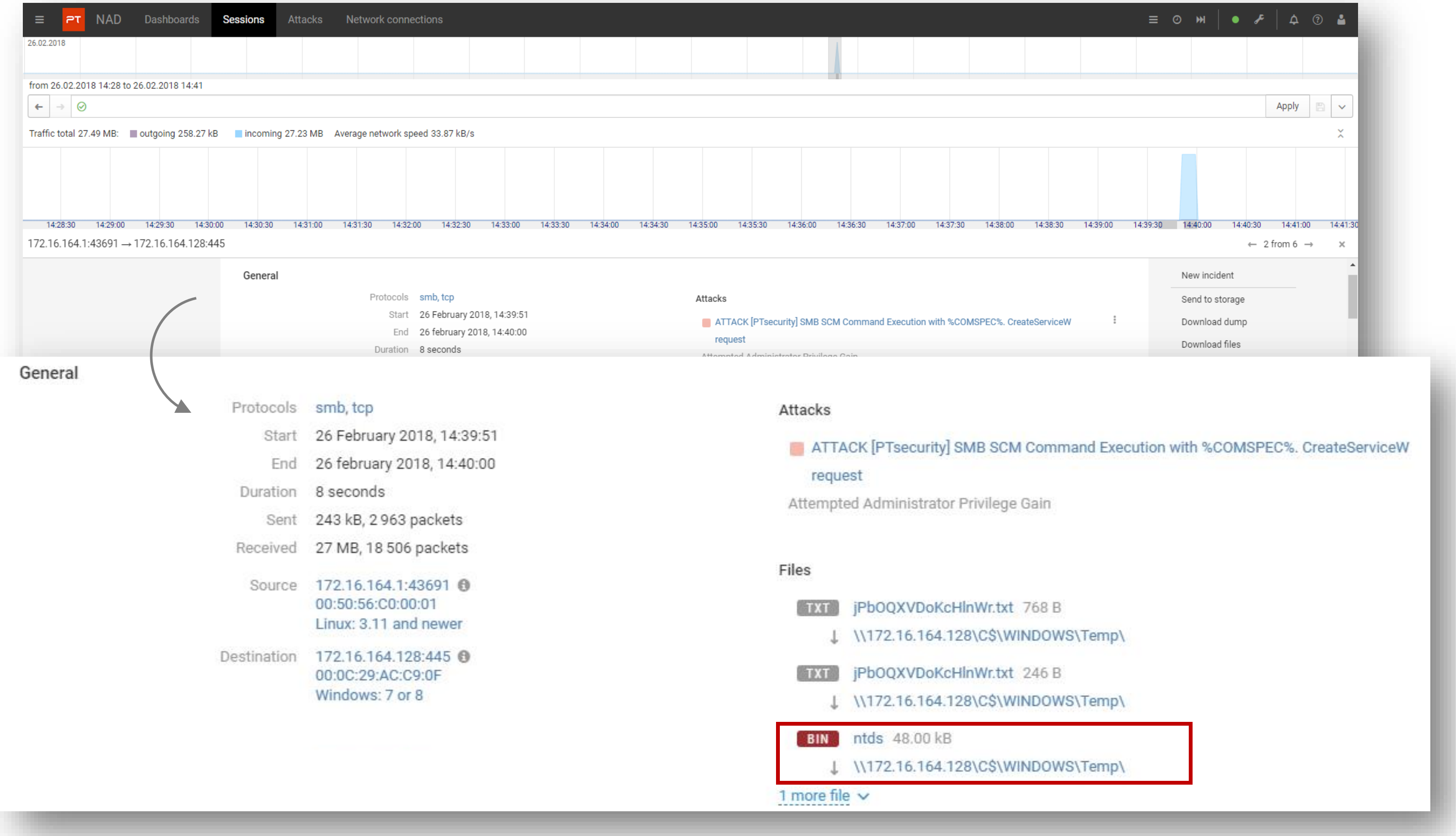
Example

There are no apparent signs of compromise in the system. A security analyst decided to check whether the domain controller had been hacked.

1. With the help of filters, the security analyst analyzed network activity directed at the domain controller.
2. The security analyst detected a request from an internal address for obtaining a list of domain users and several requests to log in to the domain controller. The last request was successful.
3. An ntds.dit* file was downloaded via the SMB protocol. The hypothesis is proved: the domain was compromised, and an investigation is required.

*The Ntds.dit file is a database that stores Active Directory data, including information about user objects, groups, and group membership

Card of a session in which a file with Active Directory data was downloaded



from 26.02.2018 14:28 to 26.02.2018 14:41

Traffic total 27.49 MB: ▨ outgoing 258.27 kB ▨ incoming 27.23 MB Average network speed 33.87 kB/s

172.16.164.1:43691 → 172.16.164.128:445

General

Protocols	smb, tcp
Start	26 February 2018, 14:39:51
End	26 february 2018, 14:40:00
Duration	8 seconds
Sent	243 kB, 2 963 packets
Received	27 MB, 18 506 packets
Source	172.16.164.1:43691 00:50:56:C0:00:01 Linux: 3.11 and newer
Destination	172.16.164.128:445 00:0C:29:AC:C9:0F Windows: 7 or 8

Attacks

🟥 ATTACK [PTsecurity] SMB SCM Command Execution with %COMSPEC%. CreateServiceW request
Attempted Administrator Privilege Gain

Files

TXT jPbOQXVDoKcHlnWr.txt 768 B
↓ \\172.16.164.128\C$\WINDOWS\Temp\

TXT jPbOQXVDoKcHlnWr.txt 246 B
↓ \\172.16.164.128\C$\WINDOWS\Temp\

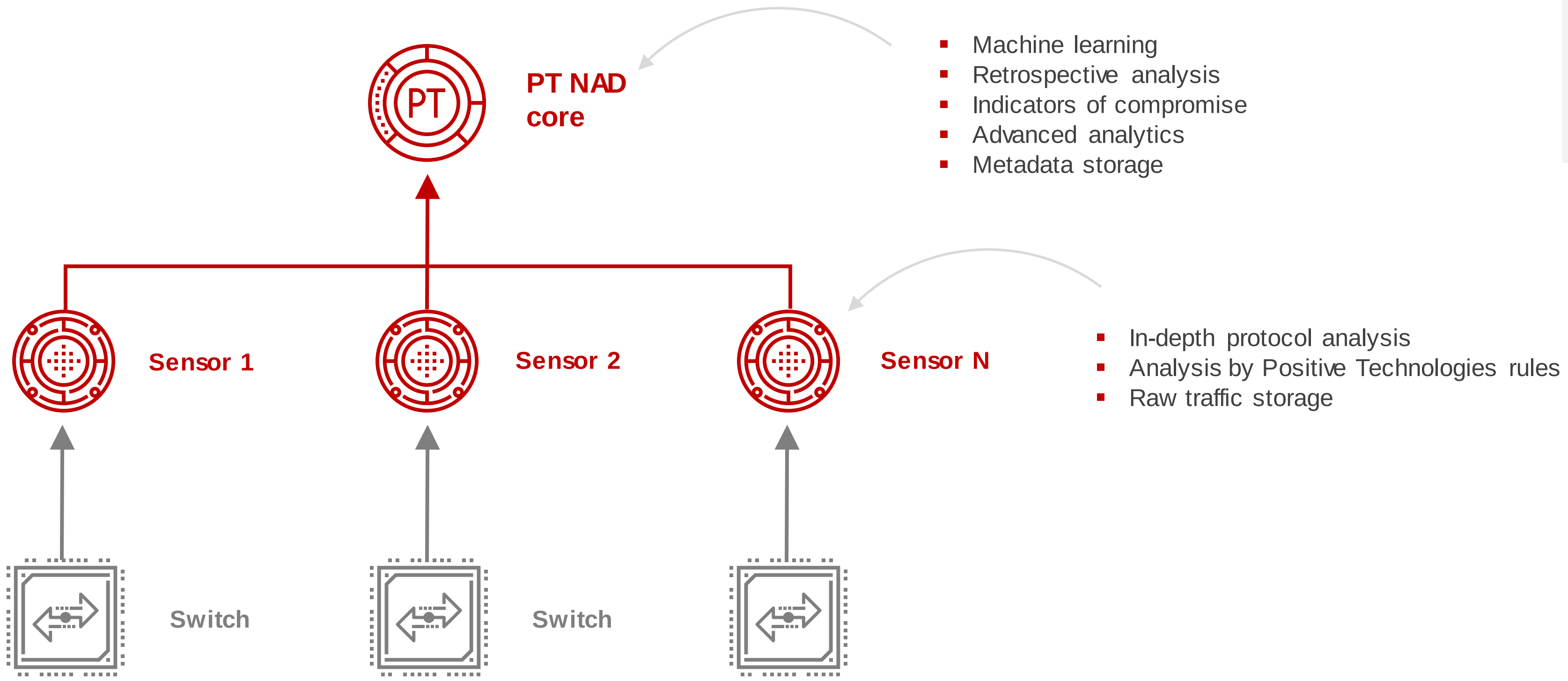
BIN ntds 48.00 kB
↓ \\172.16.164.128\C$\WINDOWS\Temp\

1 more file

PT NAD architecture

ptsecurity.com

Logical scheme



- Machine learning
- Retrospective analysis
- Indicators of compromise
- Advanced analytics
- Metadata storage

- In-depth protocol analysis
- Analysis by Positive Technologies rules
- Raw traffic storage

The core supports scaling out.

Integration with Positive Technologies products

ptsecurity.com

Integration options

MaxPatrol SIEM

security incident detection system

PT NAD informs MaxPatrol SIEM about attacks, network configuration, and asset connections. This gives a fuller picture of IT infrastructure and allows more accurate incident detection.
PT NAD can be delivered as an addition to MaxPatrol SIEM as a NAD sensor.

PT Sandbox

Advanced sandbox with customizable virtual environments

Performs static and dynamic analysis of files transferred in traffic, identifies malwares.
Automatically sends files malware status to PT NAD.

From the PT NAD interface, you can go to PT Sandbox in one click and view detailed information about the detected malicious file.

PT ESC, PT NAD, and PT Sandbox form a system for detection and prevention of targeted attacks.

A starting guide
for PT NAD projects

ptsecurity.com

Form factors and licensing

Delivery

Hardware appliance

to be deployed on the physical server

Performance: up to 10 Gbps

Virtual appliance

to be deployed on a virtual machine

Performance: up to 200 Mbps

Annual licensing

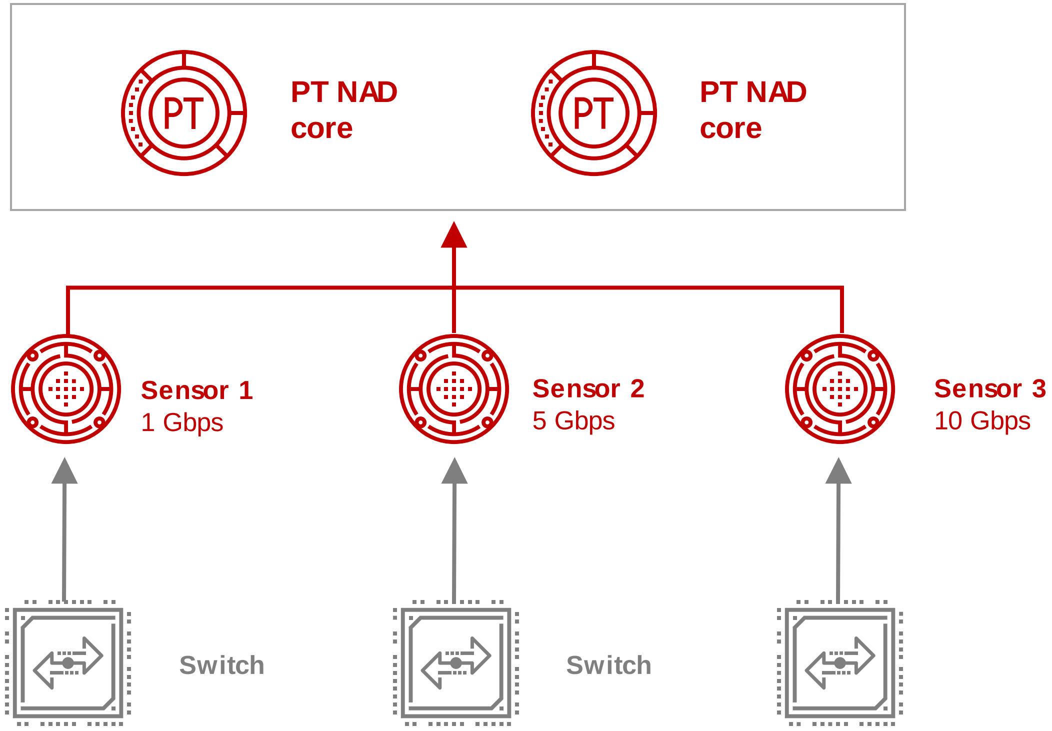
Basic license

Traffic throughput
(1, 2, 5, 10, 20, 50, or 100 Gbps)

Infrastructure licenses

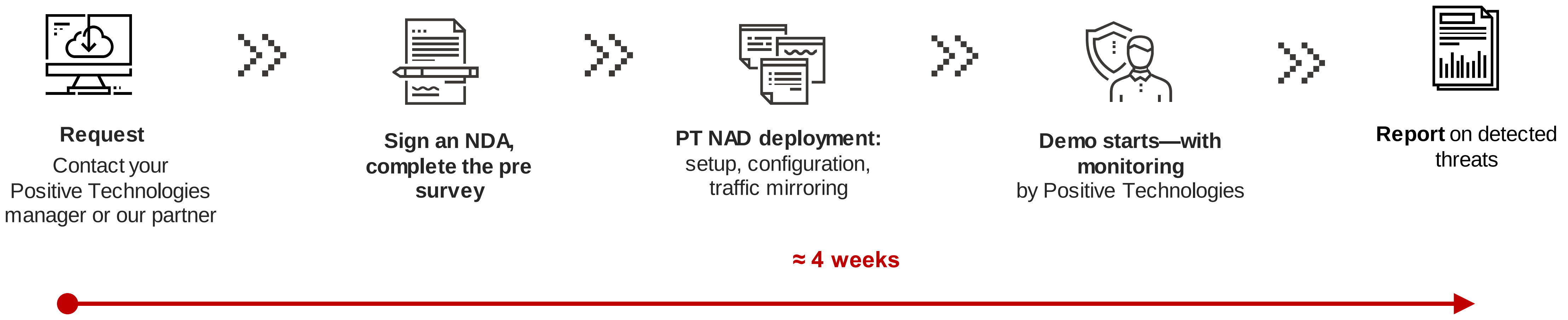
- System core
- Sensors for protocol and traffic analysis (up to **1,000**, **5,000**, or **10,000** Mbps)

Example of architecture



- **Standard license**
  20 Gbps
- **2 licenses**
  for the system's core
- **1 license**
  for 1 Gbps sensor
- **1 license**
  for 5 Gbps sensor
- **1 license**
  for 10 Gbps sensor

Check your network today with PT NAD and find hidden threats



Request
Contact your
Positive Technologies
manager or our partner

Sign an NDA,
complete the pre
survey

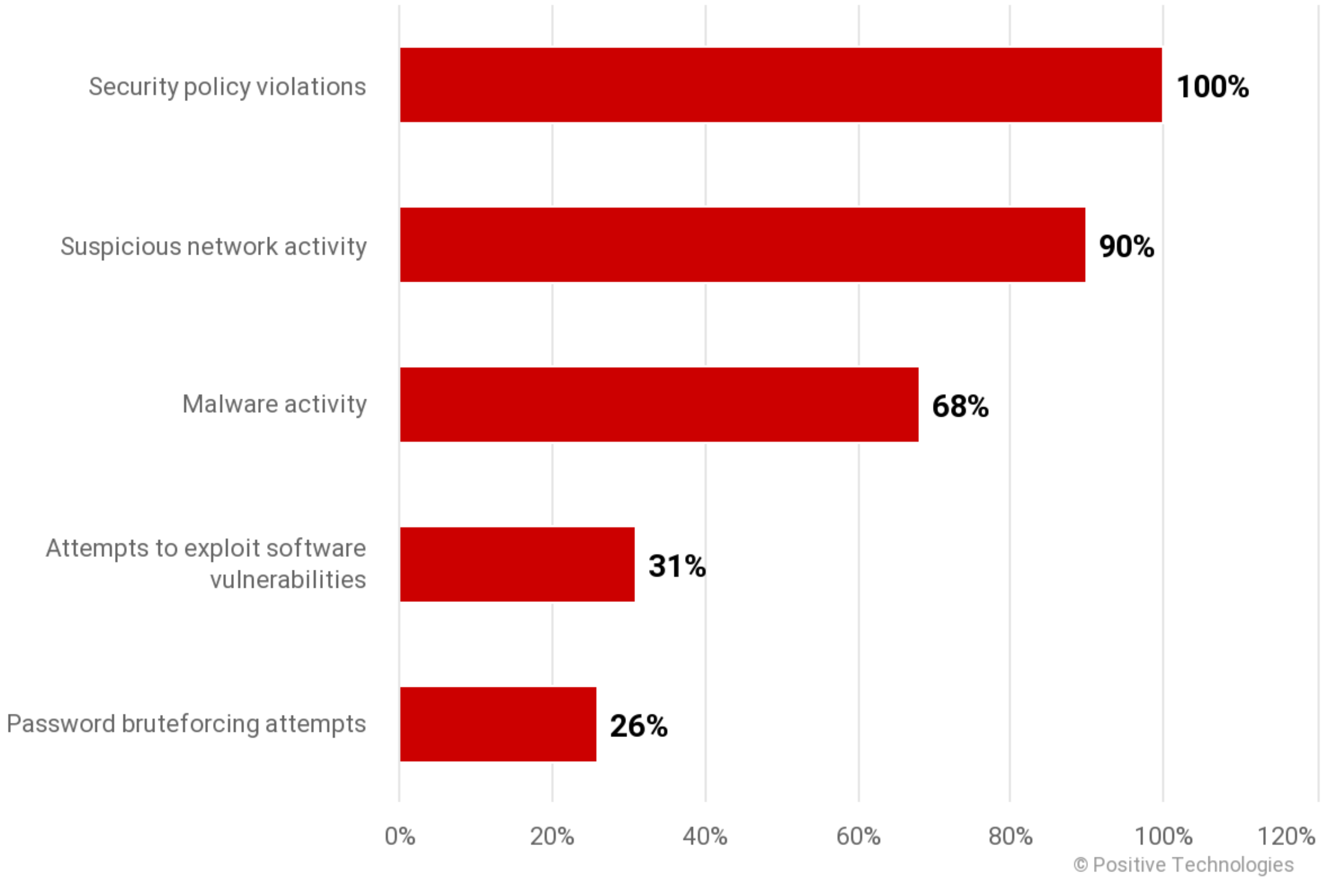
PT NAD deployment:
setup, configuration,
traffic mirroring

Demo starts—with
monitoring
by Positive Technologies

Report on detected
threats

≈ 4 weeks

Threats detected during pilot projects at 41 companies



GET A FREE PILOT:
ptsecurity.com/ww-en/products/network-attack-discovery/

[Top cyberthreats on enterprise networks. Network traffic monitoring: 2020 data](), Positive Technologies