INTEGRATED SOC PLATFORM

Unified Visibility. Automated Response.
Proven Resilience. For IT and OT.

Solution overview

The Positive Technologies SOC Solution is a cohesive ecosystem designed for high-load enterprises and critical infrastructure. It unifies three powerful components: MaxPatrol SIEM for event correlation, MaxPatrol EDR for endpoint defense, and PT Network Attack Discovery (NAD) for traffic analysis.

Built to operate in air-gapped environments, this platform ensures data sovereignty—no data leaves your perimeter. From detecting "fileless" malware in memory to identifying lateral movement across encrypted traffic, the solution covers the entire kill chain. It is sized to handle massive bursts of data while providing granular forensic capabilities

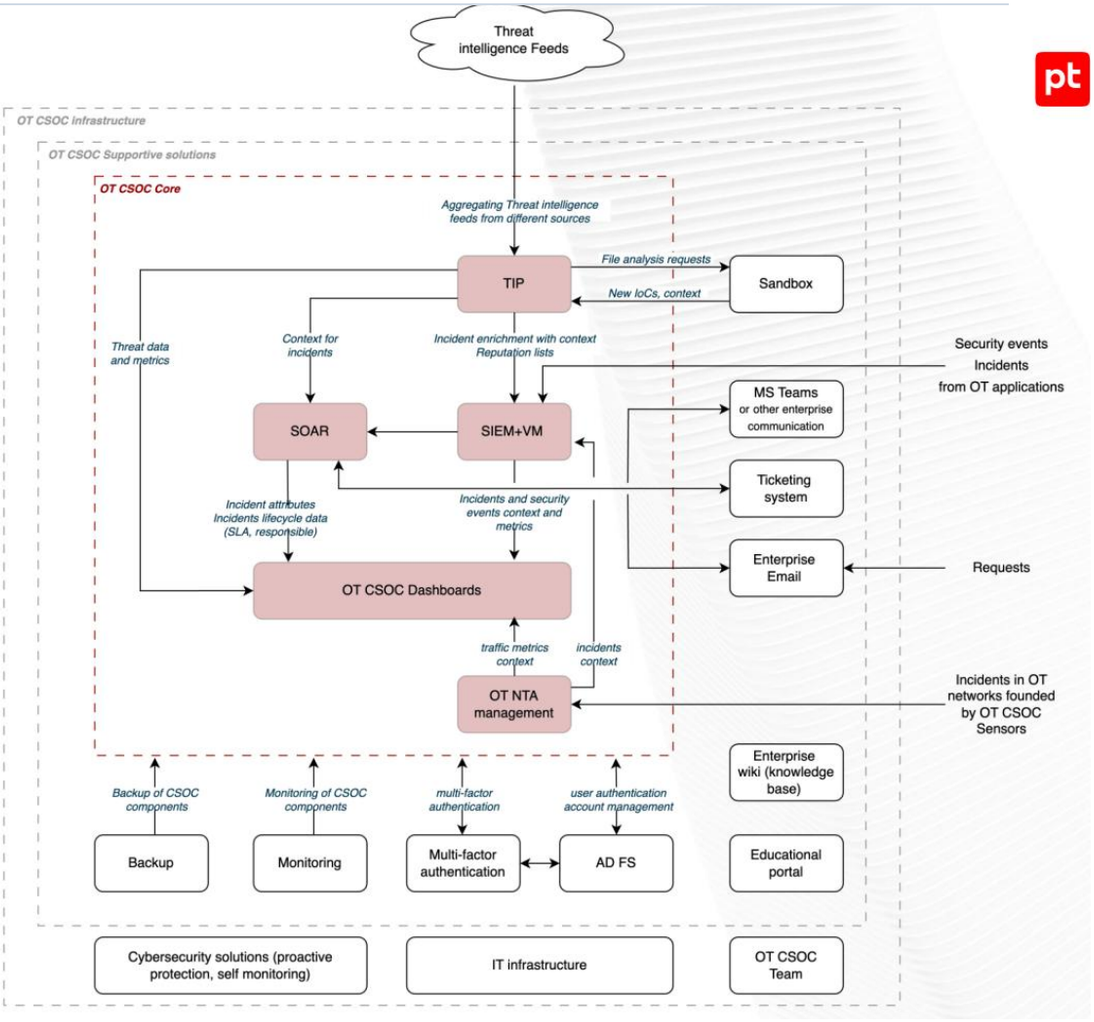
Typical OT SOC Core Architecture

Specialized IT and OT Traffic Analysis

Unlike a standard IT SOC, this architecture includes a specific OT NTA (Network Traffic Analysis) management module. This module ingests "Incidents in OT networks founded by OT CSOC Sensors." This is critical for industrial environments because standard IT tools often fail to interpret proprietary industrial protocols (like Modbus, DNP3, or Profinet) or detect anomalies in physical process control traffic.

Segregated Infrastructure Management

"OT CSOC Supportive solutions" are separated from the "OT CSOC Core." Essential services like Backup, Monitoring, MFA, and AD FS are treated as foundational support layers. This separation ensures that the security tools themselves are resilient, authenticated, and monitored, preventing the security center from becoming a single point of failure.



Core products

- **SIEM**

  The analytical core. Processes up to 100k EPS, correlates events across IT/OT, and drives automated incident management.

- **EDR**

  The hands on the ground. Blocks ransomware, isolates devices, and performs forensics on Windows & Linux endpoints.

- **NAD**

  The eyes on the network. Decrypts TLS, analyzes East-West traffic, and stores raw packets for deep investigation.

MAXPATROL SIEM

Next-Generation
Event Management & Analytics

Intelligent Correlation and UEBA

MaxPatrol SIEM goes beyond simple log aggregation. It features a fully integrated User and Entity Behavior Analytics (UEBA) engine that establishes heuristic baselines for users and devices. By analyzing peer groups and identity inference, it detects anomalies such as compromised accounts, insider threats, and privileged abuse that static rules miss.

The system provides real-time anomaly detection and supports automated programmed actions. It correlates vulnerabilities with assets to prioritize incidents based on actual risk.

Data Ingestion and Flexibility

The platform ingests security logs from a vast array of sources: Network devices, Security appliances, Applications, Servers, and Databases. It supports agentless collection via WMI, RPC, SSH, and ODBC.

Unlike "Black Box" solutions, MaxPatrol SIEM offers un-obfuscated parsers. Your operations team can view, edit, and create custom parsers. It includes a massive library of out-of-the-box connectors and an SDK for custom development.

Enterprise-Grade Performance

Designed for high-load environments, the architecture supports a Sustained Load of 50,000 EPS and a Peak Load of 70,000 EPS. For sudden spikes, it handles Bursts up to 100,000 EPS without dropping logs.

Storage is flexible and robust. The system supports Raw Event Storage, ensuring original logs are kept unfiltered for compliance. Retention policies allow for 3 months of online storage and 6+ months of total retention (with auto-archiving to cold storage/NAS).

Integration and operations

- Bidirectional SOAR Integration (CEF/LEEF)
- Proprietary & External Threat Intel (STIX/TAXII)
- Email & SMS Critical Notifications
- Native Parsers: Windows, Linux, AIX, Solaris
- Native Parsers: Oracle, DB2, Cisco, Juniper
- Network Sample Analysis (via NDR)
- Detects Ghost RAT & Deep Traffic
- Standard & Custom Reporting Engine
- Deployment: VM or Physical Hardware

PRE-CONFIGURED DETECTION SCENARIOS

- **Failed Logins & Account Changes**
- **Privilege Escalation Attempts**
- **Suspicious File Names & Paths**
- **Network Port Scans**
- **Default Credentials Usage**
- **Bandwidth Anomalies**
- **VPN Failures & Config Changes**
- **Non-Standard Port Usage**
- **Top Intrusion Signatures**
- **AV Update Failures**

- **Unified Operational Portal**

  A single pane of glass correlates alerts from disparate sources. The dashboard visualizes vulnerability correlation and supports custom reporting tailored to organizational needs.

- **Audit and Control**

  The system ensures full auditability by storing raw events without mandatory filtering. It supports granular Role-Based Access Control (RBAC) and integrates with the wider IT landscape via Syslog, ODBC, and API connectors.

positive technologies

MAXPATROL EDR

PROTECTING COMPANY AND EMPLOYEE DEVICES FROM SOPHISTICATED TARGETED ATTACKS

Deep Visibility and Protection

MaxPatrol EDR provides comprehensive coverage for Windows and Linux environments. It goes beyond signature matching by using behavioral analysis to detect unknown malware (RATs) and fileless threats. The agent collects full telemetry: process starts/stops, thread interactions, driver loads, and library injections. It monitors command line arguments and registry changes, ensuring that even sophisticated obfuscation techniques like malicious PowerShell or Office macros are detected.

Instant and active response on endpoints

Uses an extensive set of actions for automatic and timely responses to process termination, file deletion, device isolation, sending files for analysis, domain sinkholing, user account isolation, and remote shell operations.

Orchestrated playbooks can automatically terminate processes, delete files, and isolate devices from the network. Includes Ransomware Rollback to restore encrypted files.

Easy integration in infrastructures

Functions as a single agent for detection, response, and collection of telemetry and information about vulnerabilities on hosts, and supports all popular operating systems, VDI and geographically distributed networks, and air-gapped environments.

Dynamic threat detection

Detects attacks that leverage legitimate tools (PowerShell, WMI, CMD, Bash) and evade traditional signature-based analysis, and has a powerful correlation mechanism to detect APT actors and specific TTPs.

Tamper Protection

Agents are self-defending. Uninstallation requires a specific password. Updates occur without user interaction or reboots.

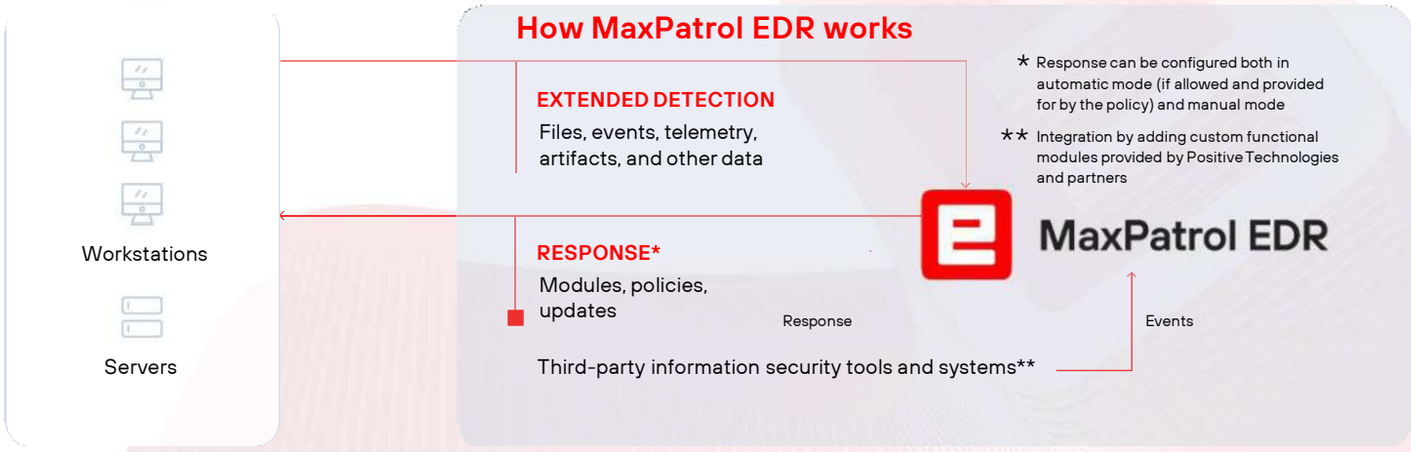
Timely and continuous detection of malware

Comes with expert rules provided by Positive Technologies Expert Security Center to identify threats and common attacker tactics and techniques from the MITRE ATT&CK matrix (top 50 for Windows and top 20 for Linux).

Key benefits

- **Static and behavioral analysis on the agent:**
  600+ correlation rules for Windows and 150+ for Linux
- **Autonomous agent**
  operation to secure devices outside the company perimeter
- **Flexible configuration**
  of detection and response rules, customizable file sandboxing

How MaxPatrol EDR works



Detection capabilities

- Fileless Malware & Memory Violations
- Malicious PowerShell/Scripts/Macros
- DLL Injection & Suspicious Loading
- Registry Changes & Persistence
- Socket Activity (Bind/Listen/Accept)
- DNS Requests & Network Connections
- Lateral Movement & Outbound Traffic
- Scheduled Task Manipulation

Control and Management

- USB Device Control
- Vulnerable App Discovery & Blocking
- Hash-based Whitelist/Blacklist (MD5/SHA)
- Path/Name/Version Whitelisting
- Offline/Air-Gap Operation Support
- 2FA & Granular RBAC
- Remote Agent Activation/Deactivation
- Syslog Output for SIEM Integration

positive technologies

PT NAD

EARLYDETECTION OFTHREATSAND TARGETED ATTACKS IN NETWORKTRAFFIC

ML-Driven Traffic Analysis

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

PT NAD brings visibility to the network layer, analyzing both North-South and East-West traffic. It utilizes Supervised and Unsupervised Machine Learning to profile traffic and detect deviations from the baseline. Crucially, it can detect attacks hidden within Encrypted Traffic (TLS) without needing to decrypt everything, by analyzing handshake metadata and cipher weaknesses. It identifies botnets, "fileless" malware operating at the network level, and zero-day exploits.

Forensics and Threat Hunting

For investigators, PT NAD is a time machine. It stores raw packets and session metadata, allowing analysts to reconstruct the attack timeline and identify "Patient Zero." Threat hunting is supported via multiple vectors: Similarity matching, Hash/IoC matching, and Detection Category. The system also extracts files transferred over the network (SMB, HTTP, FTP, etc.) for local scanning, ensuring no data needs to be sent to the cloud.

Network security policy monitoring

Configuration errors and violations of security policies (e.g., unfinished sessions, weak passwords, remote access tool usage, or tools for concealing network activity) are identified to enhance network security.

Suspect 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

Rapid deployment

Agentless architecture: **1 hour** to deploy and **1 hour** to get first detects

Attack investigation

Metadata is collected and analyzed to support timely decisions and recommend effective responses.

Features and Specification

Supports complex installations, like :

20 Gbps of analyzed traffic
100 000 flows per hour
SPAN mirroring support
Air-gapped Infrastructure

Supported protocols:

TCP, UDP, ICMP, HTTP, HTTPS (TLS Analysis), SMB, CIFS, NFS (File Sharing), SMTP, POP3, IMAP (Email), SSH, FTP, TFTP, DNS, DHCP, SNMP, RDP (Remote Desktop), SQL (Database Traffic), Industrial/SCADA

Basic security

- Identifies security policy non-compliance
- Detects new devices/ shadow IT on the network
- Manages network assets
- Exposes malware activity
- Uncovers the use of hacking tools

Advanced Security

- Analyzes traffic and user behavior for anomalies
- Identifies attacker evasion techniques
- Tracks lateral movement within the network
- ATT&CK MITRE mapping widget
- Continuously monitors for signs of previously undetected attacks
- Detects masked malicious traffic with FP rate ~0.00001%
- Uproots threats hidden in encrypted traffic
- Detects vulnerabllity exploits
- 8500+ unique IoA out of the box
- Provides expert monitoring as an ongoing service
- Inline Blocking via NGFW API Integration
- Full Packet Analysis (Not just flow data)
- On-Premise Learning (False Positive Reduction)
- Scheduled & On-Demand Reporting (PDF/CSV)
- REST API for Automation

What you get

Knowledge and experience

PT research center monitors 40+ hacking groups worldwide, providing IoA, IoC, and reputational lists to PT NAD twice a week

Technologies

On-premise analysis and anti-evasion techniques, utilizing self-learning AI to profile the behavior of all network devices

Expert support

PT Expert Security Center team remotely conducts retrospective analysis to identify any security issues that the internal team might have missed