



SANERNOW

INCIDENT DETECTION & RESPONSE SOLUTION

Part of Industry's First Integrated and Automated
SanerNow Cyberhygiene Platform



www.secpod.com

Identify, detect, and act against known or unknown threats using SanerNow's Incident Detection and Response Solution

Research states that more than 76% of security professionals find threat detection and response a challenging task, reporting that it is getting worse by the day. Why do organizations see this as a challenging task? A key contributor is the maze of disconnected and independent multi-point tools. These multiple tools reduce efficiency in threat detection and response by creating siloed views that do not track interdependencies, thereby exposing the organization to threats.

Organizations need 24x7 protection against known and unknown threats, including relevant indicators and threat actors, exploit and vulnerability priorities

or preferences, and any known or historical data on their attack patterns to ensure timely and preventive hardening of endpoints to ensure security. It is important to note that even a small oversight of known or unknown threats can lead to significant security incidents.

Leveraging threat intelligence will only provide you a partially secured landscape of known threat detection. What is required is actionable intelligence with detailed remediation suggestions based on all these threat detection factors to detect and identify new or unknown threats with measures for speedy resolution.

SecPod SanerNow's effective solution for incident detection and response

SanerNow Incident Detection and Response (IDR) provides you with one of the fastest and easiest ways to efficiently analyze your security ecosystem in its entirety to detect and identify any threat actors, threat priority, unknown threat detection with a pattern of known threat detection across your endpoint network.

SanerNow helps you prioritize threat information using its smart multi-function agents across your endpoints to boost your endpoint security against any threat actors or groups.

SanerNow's detailed incident response features will provide you with a robust out-of-the-box solution to avoid any future or detecting existing known and unknown threats. This platform takes prompt action against any threats with its effective threat response enactments. Its single-pane-of-glass view keeps your systems cyber healthy with its integrated cyber hygiene solutions.



Actively thwart cyber-attacks with SanerNow Incident Detection and Response



Improve security and resilience with real-time and on-demand threat hunting

Detect, identify, and take down threat vectors swiftly with SanerNow's real-time and on-demand threat hunting.



Discover imminent threats with ongoing system behavior tracking

Monitor deviations in your endpoint behavior, including settings or configurations to detect and respond to attack indicators in real-time.



Trigger speedy and zero-downtime responses to threats

Close the gap between threat detection and response. Respond instantly to incidents of breach or compromise to prevent and contain the spread of attacks and secure your business.



Gain seamless visibility and control to secure your globally distributed endpoints

Get a single-pane-of-glass view across your endpoints mapping all potential threats and historic responses with SanerNow's centralized cloud-based console.

Rapidly detect, analyze, and respond to cyber-attacks in real-time



Indicators of attacks (IOA) for immediate detection of an attack

Set indicators of attack using our pre-made and customizable IOA kits. SanerNow constantly scans for these indicators in your networks and instantly raises a red flag whenever the attack conditions are triggered.



Indicators of compromise (IOC) for quickly isolating affected devices

Apart from identifying new or impending threats or attacks, SanerNow also detects devices that have been compromised by ransomware like WannaCry, CryptoLocker, Fantom, EternalRocks Worm, BadRabbit, and much more. Rapidly scan and isolate any affected endpoints to prevent attacks from spreading.



Additional control with customizable checks

Go beyond pre-defined checks for threat detection to include additional detection events to gain better control based on your internally designed incident response plans.



Zero-day response to threats with comprehensive coverage

Use SanerNow to trigger incident responses to secure your network instantly. Proactively mitigate threats and evade attacks by sealing off security gaps.



Auditable, detailed incident summaries of all detection and response activities

View detailed information of all detections and responses performed by SanerNow – when indicators were triggered, affected devices, risk level, response status, and much more to get an overview of all your incident detection and response activities.



Extensive reporting and audit logs

Get auto-generated reports based on detection and response metrics like detected attacks, monitored devices, threat responses, and more. A detailed audit log keeps a record of all admin actions performed in a network, allowing you to track data related to users and actions on the SanerNow console.

About **SecPod**

SecPod is leading provider of endpoint security and management solutions. SecPod (Security Podium, incarnated as SecPod) has created revolutionary SanerNow platform and tools that are used by MSPs and enterprises worldwide. SecPod also licenses security technology to top security vendors through its SCAP Content Professional Feed.

The SanerNow **Platform**

SecPod SanerNow is a Unified Endpoint Security (UES) and management solution that ensures cyberhygiene by automating and orchestrating measures to safeguard your enterprise endpoints from cyber attacks. The major features of SanerNow include,

- Patch Management,
- Vulnerability Management,
- Asset Management,
- Endpoint Management,
- Compliance Management
- Endpoint Threat Detection & Response



Talk to **Sales**

For enquiries on pricing

Email us on: info@secpod.com

Call us at: India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023
