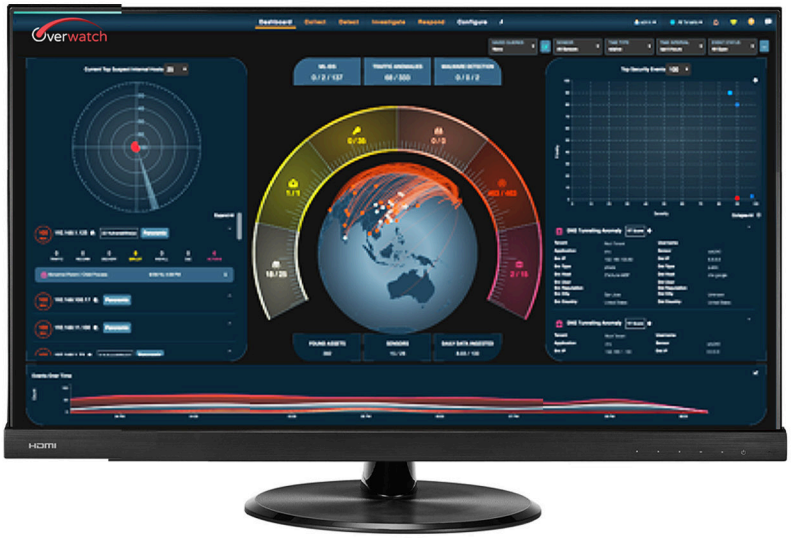
Overwatch
BY HIGH WIRE NETWORKS

Overwatch 24/7

Your Early Warning System

Security Information and Event Management (SIEM) is the foundation of any comprehensive enterprise cybersecurity strategy. That's because it helps to centralize enterprise-wide security management, but a traditional SIEM solution alone is not enough.



A Better Approach

The cornerstone of the Overwatch Managed Security Platform-as-a-Service, combines AI-powered X Detection & Response (XDR) technology with the Overwatch 24/7 Security Operation Center (SOC) to effectively cut through the noise and drill down on real threats.

How Overwatch 24/7 Works

1. Sensors and agents capture data from multiple sources in one
2. Advanced machine-learning algorithms weed out false alarms.
3. High-fidelity threats are handled automatically.
4. Our analysts have time to proactively inspect or hunt for threats.

Bottom Line

Overwatch 24/7 is your early warning system. It allows security teams to efficiently respond to threats and identify critical events before data is stolen or damage is done.

Overwatch
BY HIGH WIRE NETWORKS

Overwatch 24/7
Your Early Warning System

Overwatch 24/7: Simplified Yet Sophisticated

Unlike traditional SIEM solutions, Overwatch 24/7 relies on comprehensive, pervasive data collection, big-data processing and artificial intelligence to uncover relevant, actionable data for effective threat detection and response.

Critical Features

- Comprehensive, automatic sensor-based data collection
- Physical (on-premises) and cloud visibility
- Integrated IDS/IPS paired with AI to reduce false positives
- 50,000+ detections for known and unknown behaviors, mapped to the cybersecurity kill chain
- Simple, easy-to-use GUI dashboards
- Advanced analytics and data-lake mining
- Built-in integration with other Overwatch solutions
- Integration with other systems, for GRC and more
- APIs for data export
- Built-in event-response and case-management capabilities:
  - Create a trouble ticket
  - Trigger email, Slack and restful API alerts
  - Automatically send out PDF reports
  - Signal firewalls to take appropriate action

Defense in Depth

The Overwatch platform, managed by our 24/7 security operations center, offers organizations end-to-end protections for network, perimeter, end points, users, networks, applications, and cloud.