

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.

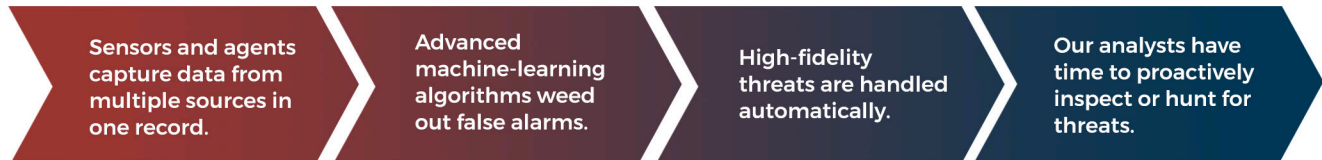
A Better Approach



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

The Overwatch 24/7 Kill Chain centralizes, normalizes and enriches security data from all security tools, across an organization's entire attack surface.

How Overwatch 24/7 Works



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 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

- | | |
|--|---|
| <ul style="list-style-type: none"> ✓ 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 | <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> • 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

Through the 24/7 Security Operation Center, Overwatch delivers defense in depth by managing best of breed solutions and offering organizations end-to-end protections and 360 visibility.

