Managed Detection & Response

Organizations of all sizes are under attack and are looking for modern, and effective cybersecurity monitoring, threat detection, and incident response solutions. For over a decade, Vertek's Security Operations Center team has provided world-class monitoring and detection services that adhere to rigorous federal, state, and industry regulations.

Managed Detection & Response

Our U.S. based, 24x7 Security Operations Center team actively monitors client's networks for possible hacking attempts and system intrusions, providing up-to-date cybersecurity threat alerts and the remediation guidance needed to deflect them.

Vertek provides clients with the hardware, software, and sensors needed to analyze and monitor threats within on premise, collocated, or cloud-based networks and environments. We provide up-to-date cyber threat information and automating response actions where applicable and provides critical threat and attack remediation guidance and support to clients as they execute against the suggested remediation guidance.

Service	MDR - Managed Detection & Response Functionality
Description	Detect and respond to threats on premise, in the cloud or in cloud applications
Remote Deployment of Unified Security Management (USM) Solution	• Physical or virtual appliance deployment • Inventory scanning and asset registration • Network and endpoint monitoring • Baseline vulnerability environment scanning • Event correlation, tuning and alarm trimming • Basic USM dashboard and MDR report creation
Alarm Monitoring	• 24x7 Coverage for Severity Level 1 • 12x5 Coverage for Severity Levels 2 • 9x5 Coverage for Severity Levels 3-4
SIEM Tuning	• Continuous
Ticket Creation	• Included
Threat Analysis	• 24x7 Coverage for Severity Level 1 • 12x5 Coverage for Severity Levels 2 • 9x5 Coverage for Severity Levels 3-4
Remediation Guidance	• Included
Automated Threat Response	• Based on USM integration capabilities with Client technology
Client Portal	• Service notifications • Incident response contact and escalation documentation • Request alarm or USM support • View and respond to tickets • Industry feeds and advisories • Track USM filtering and suppression • 2 portal accounts come standard
Unified Security Management (USM) console access	Read-only Appliance access (clients can access views and search but cannot make system changes that impact other users.). Actions Read-only can take: • Create dashboard and dashboard views • View alarms page and alarm details • View events page and event details • View asset page and assets details • View vulnerabilities page and vulnerabilities details • View environment configuration issues and environment users • View the saved reports page
Lifecycle Management	• Platform updates, signature updates, platform maintenance • Verification of Data Backup; configuration and job status • Health monitoring of Service Software and Appliance
Service Reporting	• Monthly MDR report emailed to Client contacts (e.g., incident response activities, alarm analytics, change notifications, alarms flagged for review, overall alarm deflection, etc.)
Service Review	• Quarterly Technical Account Manager guided service review to discuss performance, discuss Client roadmap, obtain service feedback, set high-level goals and objectives

Managed Threat Intelligence

Without visibility into attacks, threats and risks, it's impossible to measure, control and mitigate risk, capture a return on investment, and continuously improve your security or risk program to drive positive business outcomes.

Vertek's Managed Threat Intelligence (MTI) service expands the basic Managed Detection and Response service by providing a greater level of incident response and threat support, and access to dashboards and advanced analytics helping clients to advance their cyber-maturity, realize business value, and proactively reduce risk.

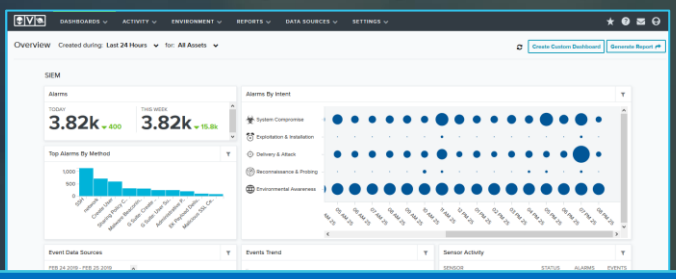
Service	MTI - Managed Threat Intelligence Functionality
Description	MDR + Advanced analytics and Client security operations oversight
Security Action Dashboard	• Monthly incident and action dashboard creation • Monthly SIEM, SOC report creation and review • Security concerns, questions and noteworthy items • Monthly report repository
Advanced Analytics Platform	• Client SAML authentication provider required • Detect, protect and respond dashboards • Access to 35+ security visualizations and user guides • Ability to customize report visualizations and create dashboards
Service Reporting	• Ability to export reports from Vertek's Client Portal or from the Advanced Analytics Platform
Service Review	• Monthly Security Analyst guided alarm review, report review, and tuning discussion (e.g., discuss outstanding and important alarms and vulnerabilities, help prioritize and set remediation activities, discuss standard and custom reports and document action items that carry forward month to month.)

"The detail within Vertek's platform is unmatched. The information is both comprehensive and able to be distilled down to an actionable level."

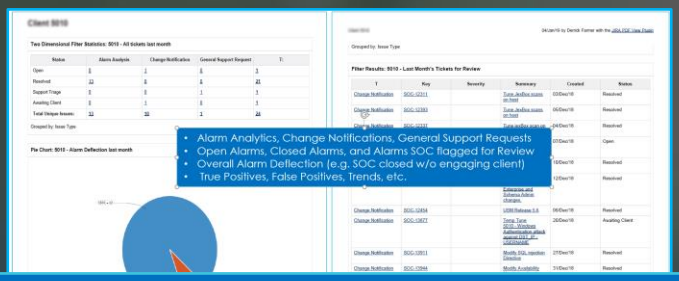
- Vertek MSP Customer

MDR & MTI Summary

Unified Security Management Reports



Security Operations Reports



MDR: Designed for smaller, early stage, cost conscious organizations just looking to get started with logging, monitoring for security or compliance reasons.

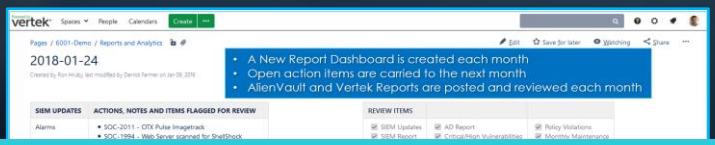
SIEM Health and Real-Time Security Metrics

- Asset Reports
- Alarm Reports
- Threat Reports
- Policy Reports
- Event Reports
- Security Reports
- Vulnerability Reports

Monthly Alarm Status Reports

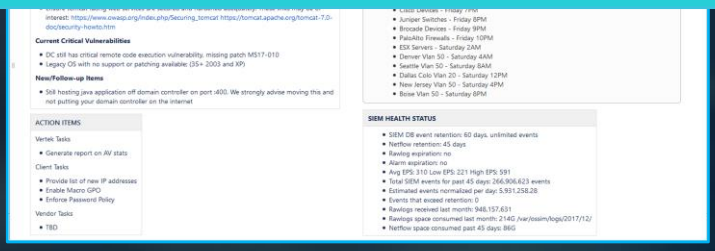
- Active Alarms, Assignment and Status
- Total Alarms (SOC Deflected vs. Client Interaction)
- True Positive Alarms sorted by severity
- False Positive Alarms

Detailed Portal Driven Service Reviews



Business Intelligence Dashboards

MTI: Designed for more advanced, mature, value focused organizations looking to rapidly evolve security, risk, or compliance programs, capabilities, and posture.



Protect, Detect and Respond

Monthly Incident and Action Dashboard

- Deployment Status & Environmental Changes
- Outstanding and Important Alarms, Vulnerabilities
- Service Tuning and Maintenance Tickets
- SIEM Total Events and Statistics
- Document Network Changes | Critical Vulnerabilities
- Generate and Track Client & Vertek Action Items
- Critical Prioritization and Remediation Guidance
- Track Client Signoff on SIEM Filtering and Suppression

Security Operations Management Visibility

Answer key questions stakeholders are asking:

- How secure is our organization?
- Are our security investments paying off?
- Are cybersecurity services delivered in a fashion that meet the business needs?
- Are our IR capabilities adequately managing the impact of incidents to the organization?