Panoptic Cyberdefense

Panoptic Cyberdefense is a SOC professional service involving high-level consulting, monitoring, data collection, analysis, security management, and reporting.

Service Features

NIDS Sensor Automated Threat Detection
NIDS Sensor Automated Compliance Detection
MultiGig NIDS Sensor Included
1TB Lookback Packet Capture
Continuously Learning Malware Detection

Proprietary Signature Updates
Banking Signature Updates
Community Signature Updates
Off-site Packet Captures
Off-site Log Retention
One Year SIEM, Log and PCAP Retention
Application Detection and Filtering
Attachment Detection and Sandboxing
Firewall Hardware Included
Firewall Redundancy
NIDS Redundancy
NIDS 10Gb Sensor Ports
Additional Lookback Storage
SSL Traffic Decryption
Web Content Filtering
Application Micro-segmentation
Support for Cloud Infrastructure

Security Management

Security Event Correlation
Log Correlation
Network Behavior Analysis
24/7 Sensor Tuning
24/7 Professional Analysis

24/7 Threat-level Alerting
Log Analysis
Alert Rules Management
Customized Signature Design
Firewall Management
Firewall Configuration Change Control
Policy Configuration Management
Unified Threat Management
VPN Tunnel Management
Client VPN Management

Consulting

Monthly Security Briefing
Reporting to IT Committee

Service Operation

Online Ticketing
24/7 Phone Support
E-mail Alerting
Emergency Dispatch
2 Hour Emergency Response
Hardware Replacements / Upgrades
Software Upgrades
Firmware Upgrades

Optional Service Level
15 Minute Priority Response

Security Reporting

Monthly Summary
SIEM Daily
SIEM Weekly
SIEM Monthly
SIEM Yearly

Firewall Daily
Firewall Monthly
FW Configuration Differential
FW Full Configuration
FW Policy Object
Uptime and Bandwidth Monitoring
Uptime and Bandwidth Graphing
Incident Report
Post-Mortem
Root Cause Analysis
Reason for Outage

Optional Reporting
Current Whitelist
Data Archive DVD
Custom Reports