XIOGUARD

360° CYBERSECURITY

THE ULTIMATE MANAGED SECURITY SERVICE FOR 360 DEGREE CYBERSECURITY COVERAGE

TURN THE TABLES ON RANSOMWARE TODAY!

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

AUTOMATED THREAT HUNTING (ATH)

NETWORK TRAFFIC ANALYSIS (NTA)

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING POWERED EVENT COORDINATION

PRECISION AUTOMATED RESPONSE

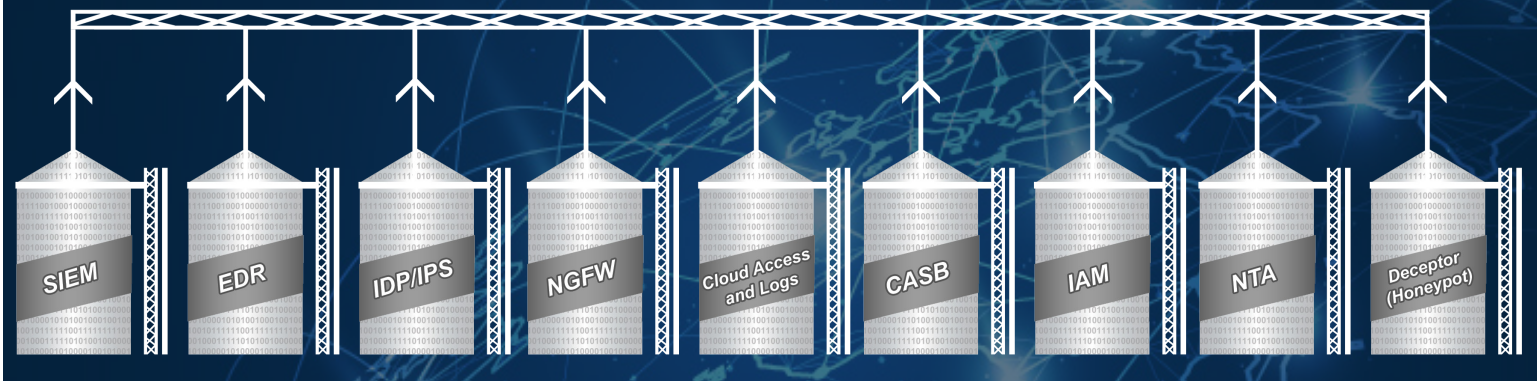
INTEGRATED SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

XioGuard employs an open XDR Next-Generation SIEM platform for 360-degree detection and response by ingesting data from all tools, correlating data across the entire attack surface, delivering high-fidelity detections, and responding to threats automatically through AI/ML. The unified platform ingests data from existing security tools to deliver 360-degree visibility and response capabilities across the entire attack surface. This AI-powered platform also learns as it works over time to become faster and more sophisticated at detecting, correlating, and responding to incidents.

Advanced Capabilities Include:

- Automatic Threat Hunting
- AIML Powered Event Coordination
- In-Depth Network Threat Detection and Anomalous Activity Monitoring
- Network Traffic Analysis
- Comprehensive Extensible Analytics
- Prioritized, Valid Security Incidents with Correlated Raw Data
- Log Management
- Compliance and Standards-Based Reports
- Real-Time and Long-Term Search with Web-Like Query and Iterative Filtering
- Event Alerting
- Precision Automated Response
- Event Log and Network Flow Data Consolidation
- Incident Analysis Assistance
- User and Entity Behavior Analytics
- Network Virtualization and Application Intelligence
- File and Registry Access Monitoring
- Real-Time and Historical Cross Correlation
- Integrated Security Orchestration, Automation and Response

Bridging Silos to Get Visualization into the Entire Attack Surface



info@xiologix.com | 888.492.6843 | www.xiologix.com

XIOGUARD

360° CYBERSECURITY

THE ULTIMATE MANAGED SECURITY SERVICE FOR 360 DEGREE CYBERSECURITY COVERAGE

Often, indicators of compromise (IOCs) go unnoticed or unresolved in your systems environment. XioGuard helps identify and resolve these IOCs quickly before it's too late:

- Suspicious entries in system or network accounting, or logs
- Discrepancies between logs
- Repetitive unsuccessful login attempts within a short time interval
- Unexplained new user accounts
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial/disruption of service or inability of one or more users to log in to an account
- System crashes
- Poor system performance of dedicated servers
- Operation of a program or sniffer device used to capture network traffic
- Unusual time of usage (e.g., user login during unusual times)
- Unusual system resource consumption. (High CPU usage)
- Last login (or usage) for a user account does not correspond to the actual last time the user used the account
- Unusual usage patterns (e.g., a user account associated with a user in Finance is being used to log into an HR database)
- Unauthorized changes to user permission or access

WHAT DOES XIOGUARD COST?

$1000 per month (up to 10 GBs of logs per day)

Package can be upgraded to include:

- Intrusion, Detection to Malware Command and Control Detection/Analysis
- Sandboxing
- Deceptor

info@xiologix.com | 888.492.6843 | www.xiologix.com