SENTINEL ASSESSMENT & OPTIMIZATION

Optimize existing Microsoft Sentinel deployment to improve detections, reduce noise and control SIEM costs without losing visibility.

Gain visibility. Reduce risk. Strengthen defense.

Microsoft Sentinel | Log Analytics | MITRE | Content Hub | Logic Apps | Defender XDR

CUSTOMER PROBLEM

Sentinel environments can become expensive and noisy when connectors, analytics rules, retention, automation and data ingestion are not optimized.

The result: high SIEM cost, alert fatigue, missed threats and inefficient SOC operations.

HOW WE SOLVE IT

INNOVATE assesses Sentinel architecture, data connectors, ingestion patterns, analytics rules, incidents, workbooks, UEBA, watchlists, SOAR playbooks and cost drivers.

We use Microsoft Sentinel, Log Analytics, MITRE Coverage, Content Hub, Logic Apps and Defender XDR integrations to tune detections, reduce ingestion cost and improve SOC effectiveness.

YOUR OUTCOME

- Lower SIEM cost through smarter ingestion and retention
- Higher-fidelity detections and less alert fatigue
- Prioritized optimization backlog for SOC operations

SENTINEL ASSESSMENT

Understand your Sentinel environment and uncover optimization opportunities.

ASSESSMENT FOCUS

- Architecture & Data Flow
- Data Connectors
- Ingestion & Retention
- Analytics Rules
- Incidents & Alerts
- Workbooks & Dashboards
- UEBA & Watchlists
- SOAR Playbooks
- Cost Drivers

YOU GET

- Current State Assessment
- Data Ingestion Analysis
- Rule Efficiency Review
- Alert Volume Analysis
- Content & Coverage Review
- Cost & Usage Report
- Gap Analysis
- Recommendations
- Executive Presentation

ASSESSMENT SCORE

Developing

Clear visibility of gaps and opportunities to optimize Sentinel.

VS

SENTINEL OPTIMIZATION

Tune, optimize and reduce costs while improving detections and SOC effectiveness.

FOCUS AREAS

- Ingestion & Retention Tuning
- Analytics Rule Optimization
- Incident Noise Reduction
- UEBA & Watchlist Tuning
- SOAR Playbook Efficiency
- Content Hub Optimization
- MITRE Coverage Enhancement
- Automation & Response
- Cost Optimization

YOU GET

- Optimized Data Ingestion
- Better Detection Accuracy
- Reduced Alert Fatigue
- Improved SOC Efficiency
- Optimized Playbooks
- Enhanced Visibility
- Lower SIEM Cost
- Operational Runbook
- Executive Reporting

OPTIMIZATION IMPACT

Optimized

Lower SIEM cost, higher-fidelity detections and improved SOC effectiveness.

IDEAL FOR

Organizations seeking visibility into their current Sentinel deployment and a prioritized optimization roadmap.

IDEAL FOR

Organizations with existing Sentinel deployments looking to reduce cost, improve detections and maximize SOC impact.

SENTINEL OPTIMIZATION JOURNEY

ASSESS
Evaluate environment, cost & performance

ANALYZE
Identify gaps, noise and cost drivers

PRIORITIZE
Define optimization opportunities

OPTIMIZE
Tune rules, connectors, retention & playbooks

VALIDATE
Measure improvements and cost savings

CONTINUOUSLY IMPROVE
Continuously monitor, adapt and optimize

WHAT YOU RECEIVE

- Executive Assessment Report
- Cost & Usage Analysis
- Analytics Rules Review
- Incident & Alert Analysis
- Optimization Roadmap
- Tuning Recommendations & Runbook
- Cost Savings Report
- Dashboard & Workbook Enhancements

INNOVATE
AXAITRA GROUP MEMBER

Member of Microsoft Intelligent Security Association

Microsoft Security | Microsoft Verified Managed XDR Solution

Let's start the conversation.

Contact us to turn security challenges into strategic opportunities through actionable insights and expert guidance

contact@innovate-security.ai
www.innovate-security.ai