illumio | Microsoft

INTEGRATION BRIEF

Microsoft Sentinel Solution

Enhance security operations in Sentinel with Illumio Zero Trust Segmentation

Empowering security teams with visibility and improved context

Security teams are increasingly leveraging Sentinel, Microsoft's cloud-based SIEM and SOAR platform, as a central tool for collecting telemetry from multiple sources across their hybrid data center infrastructure.

Sentinel collects logs from critical workloads and security appliances, such as firewalls, IDS systems, switches, and gateways, looking for actionable data. It then consolidates that data across the infrastructure for monitoring, troubleshooting, threat detection, threat hunting, security containment, and remediation.

As the volume and frequency of threats continues to rise, so too does the pressure on security operations teams. Security operation centers receive tens or hundreds of thousands of security alerts each day which is more than most security teams can effectively manage. This often leads to information overload and alert fatigue. What is often missing from this data is detailed telemetry of lateral network behavior between all workloads across east-west traffic.

The Illumio Zero Trust Segmentation Platform serves as the source of truth for all application dependencies on all workloads across your hybrid environment. With the Illumio Sentinel Solution, critical events and traffic flow logs from Illumio are now readily available in Sentinel. This provides new levels of visibility and collaboration and empowers security teams to better understand what's happening in their network so they can stop cyber incidents from becoming disasters.

Illumio Sentinel Solution: How it works

Available on the Microsoft Azure Marketplace, the Illumio Sentinel Solution includes a data connector that pulls in audit events and traffic flow logs into Sentinel.

Illumio data then gets put into Sentinel's Advanced Security Information Model format. This ensures the data structure aligns with other security products for better SecOps efficiency.

From there, Illumio uses three Sentinel workbooks that deliver out-of-the-box analytics ready to use immediately.

These workbooks give you a powerful set of data from your Illumio environment. Use the information to enrich your existing security operations. You can also create your own custom workbooks and queries to consolidate information from other security event data Sentinel is ingesting for deeper insights.

Key benefits

Enhanced SecOps efficiency
View your auditable events and traffic flow logs as readable, usable data directly in your Sentinel console. Centralize your security monitoring and achieve more efficient operations.

Greater visibility into workloads
Prioritize security efforts using data on tampering events, auditable events, ports scan events. See blocked traffic and the most trafficked workloads and services.

Faster incident response with ASIM
Correlate Illumio traffic flow logs from workloads with other security event data. Get deeper insights that help you identify and respond to threats.

The power of Illumio ZTS in Microsoft Sentinel

Security admins can now import Illumio log data into Sentinel. This means you can create security queries on Illumio flow log and audits, view analytics in out-of-the box dashboards (workbooks), and receive alerts on security events.

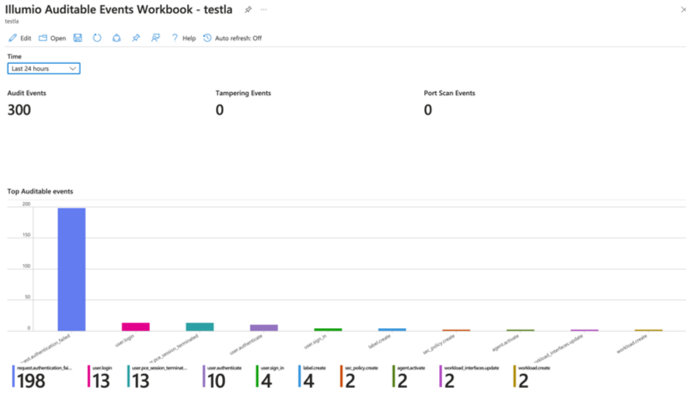
The Illumio Sentinel Solution brings these three Illumio workbooks directly into Sentinel. Network and security teams can centralize security operations, use enriched data for troubleshooting, and meet audit and compliance needs with enhanced data from their Illumio workloads and corresponding traffic flows.

Auditable events workbook
Use your SIEM to archive and retrieve long-term audit and compliance data, providing:

- Counts of audit events, tampering events, and port scan events
- Change monitoring of workloads affected by policy changes and changes by resource type and user
- Data on all authentication events filtered by severity and status

Flow data workbook
Analyze workload and traffic data for troubleshooting, including:

- Workloads with most traffic (inbound/outbound)
- Services (port/protocol) that are most active
- System traffic flow levels during time intervals (allowed, blocked, potentially blocked, and unknown)


Illumio Auditable Events Workbook - testla

testla

Time: Last 24 hours

Audit Events: 300

Tampering Events: 0

Port Scan Events: 0

Top Auditable events

request.authentication_fai... 198

user.login 13

user.pce_session_terminat... 13

user.authenticate 10

user.sign_in 4

label.create 4

sec_policy.create 2

agent.activate 2

workload_interfaces.update 2

workload.create 2

Workload stats workbook
See information about your Illumio VEN statistics, including:

- Workloads by VEN version, type, and status
- Counts of managed and unmanaged workloads by OS and enforcement state

Out-of-the-box analytics rules

The Illumio Sentinel Solution's analytics rules automatically create alerts and incidents based on events such as firewall tampering, enforcement changes, and detected issues with the Illumio VEN. When an alert is trigged, an incident gets created with full details, including the number of corresponding events and logs, timestamp, creator, status, hostname, IP address, and more.

SOCs are being modernized with Microsoft Sentinel. With the Illumio Sentinel Solution, network and security teams can strengthen cyber resilience and compliance with better visibility and protection.

Member of
Microsoft Intelligent
Security Association
Microsoft Security

Illumio's Sentinel Solution is now available on the Azure Marketplace

Access the solution on the Azure Marketplace or learn more about our partnership with Microsoft Sentinel.

About Illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Zero Trust Segmentation Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.