LOGIQ.AI

SECURE

Edge Protection

INTRODUCTION

LOGIQ.AI is a system that can directly ingest security event logs from agents compatible with OSSEC (Open Source Security), which is a powerful open-source host-based intrusion detection system.

OSSEC is a host-based intrusion detection system (HIDS) that can be used on a variety of platforms. It has an advanced correlation and analysis engine with log examination, file integrity monitoring, Windows registry monitoring, centralized policy enforcement, rootkit scanning, and real-time alerting/active response. It supports most operating systems including Linux, OpenBSD FreeBSD), Mac OS X Solaris), as well as Windows.

OSSEC is composed of three main components: the manager, the agent, and the local OSSEC server.

The manager oversees the agents, which monitor system activity and report back, the manager then compiles the agent reports, combines them with its own rules and tests, and alerts if there are any security issues.

The agents detect changes or anomalies in the data flow that could signify a malicious attack such as worms, viruses, hacking tools, and more.

The local OSSEC server is responsible for analyzing the data from the agents and taking appropriate action depending on the type of attack detected.

LOGIQ.AI takes over the functions of the manager and the local OSSEC server, making it easy to bring together security-related events into your data fabric for instant consumption.

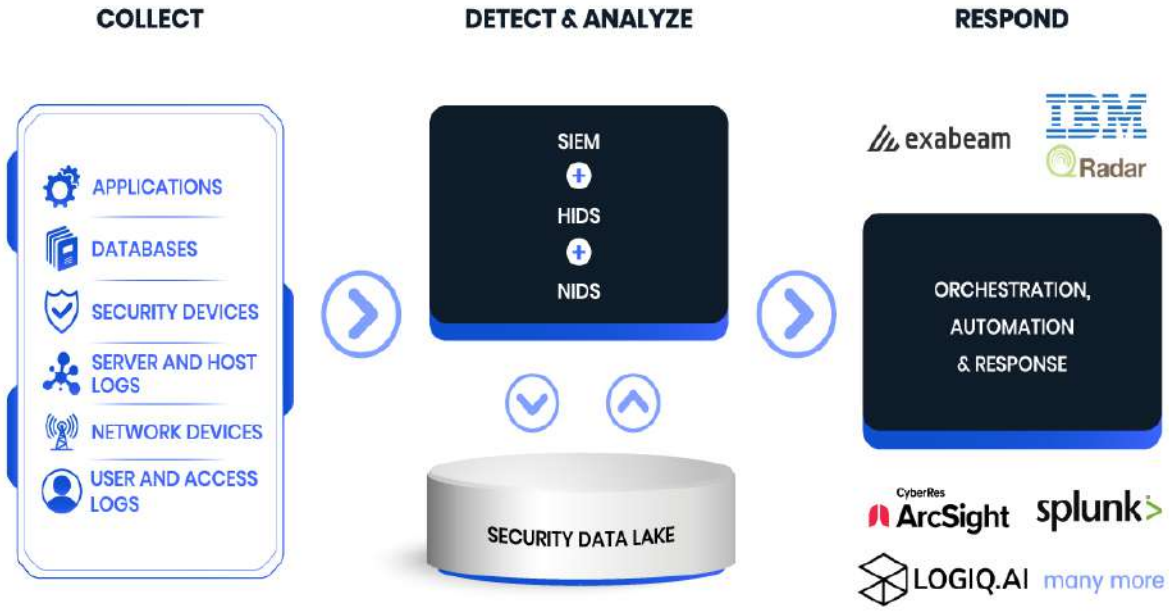
HIGHLIGHTS

- LOGIQ.AI can ingest security event logs from OSSEC, an open source host-based intrusion detection system (HIDS) compatible with multiple operating systems.
- OSSEC consists of three main components: the manager, agent and local server which are responsible for monitoring system activity and alerting in case of any anomalies or malicious attacks.
- LOGIQ takes over the functions of manager & local server to bring together security events into a data fabric for instant consumption.
- LOGIQ.AI takes over the functions of the manager and local OSSEC server, bringing security-related events into a data fabric for instant consumption.
- LOGIQ utilizes OSSEC capabilities in Intrusion Detection & Prevention; File Integrity Monitoring; Log Management; Compliance Management; Real Time Alerts; Centralized Management across cloud platforms.
- LOGIQ takes over the functions of manager & local server to bring together security events into a data fabric for instant consumption.

CAPABILITIES

Following are some of the critical OSSEc features:

- LIDs (log-based intrusion detection) actively monitor and assess data from several log data points in real time.
- Analysis at the process and file level to find malicious software and rootkit.
- Respond in real-time to attacks and modifications to the system using a variety of mechanisms, such as firewall rules, integration with 3rd parties like CDNs and support portals, as well as self-healing activities.
- Application and system-level audits for compliancewith numerous widely used standards, including PCI-DSS and CIS benchmarks.
- File Integrity Monitoring (FIM) keeps a forensic duplicate of the data as it changes over time in addition to detecting changes to the system for both files and windows registry settings.
- Integration with SIEMs and EDR solutions to provide extra context and better visibility into the environment.
- Automated patching of both critical system



components and application packages in order to quickly address vulnerabilities.

- Implementation of segmentation techniques, such as VLANs and private networks, to ensure data is isolated from public networks.
- Regular testing of security controls to ensure that they remain effective, and updated when necessary.
- Implementation of processes to regularly evaluate risks associated with new technologies or changes in the environment.
- A comprehensive security strategy must include all these elements in order to protect an organization from threats and data breaches.

HIDS

Monitor and track suspicious activity on your hosts

A host-based intrusion detection system (HIDS) is a security tool that monitors and analyzes the system and network activity on a single host to detect any suspicious behavior that could indicate an attempted cyber-attack.

The HIDS monitors various aspects of the host, such as system logs,system and application files, and network traffic, to identify any anomalies or deviations from normal activity.

When the HIDS detects suspicious activity, it generates an alert that is logged in the system's security event logs.

The HIDS may also trigger other security measures, such as blocking suspicious activity or isolating the affected system from the network, to prevent the attack from spreading.

Some common types of suspicious activity that a HIDS might monitor include:

- Unauthorized access or attempts to access restricted resources
- Modification of system or application files
- Unusual system or network activity, such as a sudden increase in network traffic or unexpected changes in system configurations

BENEFITS

The Key Benefits of SECURE include:

- Logiq provides advanced correlation and analysis engine for log examination, file integrity monitoring, Windows registry monitoring, centralized policy enforcement, and rootkit scanning
- Logiq Can detect and prevent unauthorized access to cloud infrastructure using a rule-based system to monitor network traffic and identify malicious activity
- Logiq can monitor the integrity of files on a cloud platform to detect any changes that may indicate a security breach
- Logiq can collect and analyze log data from cloud infrastructure to identify security threats and correlate log data from multiple sources
- Logiq can help organizations comply with security standards such as PCI-DSS, HIPAA and SOC2
- Logiq can provide real-time alerts for security breaches and suspicious activity, allowing organizations to quickly respond to potential threats
- Logiq can be used to manage and monitor multiple cloud platforms from a single console, providing a centralized view of security across an organization's cloud environment
- Logiq supports most operating systems including Linux, OpenBSD FreeBSD, Mac OS X Solaris, as well as Windows.

- Unauthorized network connections or traffic

To effectively track suspicious activity on your hosts, it is important to regularly review the security event logs and respond to any alerts generated by the HIDS. This can help you identify and mitigate any potential threats to your systems and networks.

SIEM

Detect, analyze and respond to security threats

Security Information and Event Management (SIEM) is a security management system that combines the functions of a security information system (SIS) and a security event management (SEM) system. It provides real-time analysis of security alerts generated by network hardware and applications. SIEM systems are designed to detect, analyze, and respond to security threats and compliance violations.

SIEM systems typically include a central console that allows security analysts to view and analyze security alerts and events in real-time. The system also includes a database that stores security-related data and a set of tools for analyzing and reporting on that data.

One of the main benefits of SIEM is its ability to detect security threats and anomalies in real-time.
This is achieved through the use of security analytics, which uses machine learning algorithms to analyze security data and identify patterns that may indicate a security threat.

Once a potential threat has been detected,
SIEM systems can alert security analysts and provide them with the necessary information to investigate and respond to the threat. This includes identifying the source of the threat, determining the extent of the damage, and taking steps to mitigate the risk.

SIEM systems can also be used to monitor compliance with security policies and regulations. They can provide reports and alerts when security policies are not being followed and can help organizations to maintain compliance with industry regulations and standards.

Logiq provides Crowdsourced SIEM Rules with Sigma:

- Import Sigma signatures for detecting malicious signatures in logs and save yourself from vendor lock-in
- Extend your Sigma rule database with custom SIEM rules
- using our built-in rule wizard
- Use the free logiqctl CLI to batch import/export rules
- and share them across multiple environments

SOAR

Orchestrate, Automate, and respond faster to threats

Security, Operations, and Response (SOAR) is a security management approach that combines the functions of a security operations center (SOC) and an incident response team (IRT). SOAR systems are designed to detect, analyze, and respond to security threats and compliance violations.

Like SIEM systems, SOAR systems are used to orchestrate and automate the response to threats. Orchestration refers to the coordination of multiple security tools and processes to respond to a threat. This can include things like activating firewalls, blocking malicious traffic, and quarantining infected systems. SOAR systems can be configured to automatically trigger these responses when a threat is detected, allowing organizations to respond to threats more quickly and effectively.

Automation is another key feature of SOAR systems. Automation can help organizations to reduce the time and effort required to respond to threats, and can also help to reduce the risk of errors. For example, SOAR systems can be configured to automatically update security policies, apply patches, or run security scans in response to a threat.

SOAR systems can also be used to monitor and manage the response to a security incident. This can include things like tracking the progress of incident response, coordinating communication between different teams, and providing reports and analysis on the incident.

By orchestrating and automating the response to threats, SOAR systems can help organizations to respond more quickly and effectively to security threats and compliance violations. This can help to minimize the impact of a security incident, and can also help to protect against future threats.

LOGIQ's cloud-native architecture enables rapid scalability to handle the accumulation and analysis of logs from all your application and infrastructure data sources during times of high ingestion.

Use Logiq's built-in webhooks to connect to ANY SOAR platform and trigger remediation workflows on detected events.

The logiq platform utilizes OSSEC capabilities in the following ways:

Intrusion Detection and Prevention: OSSEC includes an Intrusion Detection System (IDS) that can detect and prevent unauthorized access to cloud infrastructure. It uses a rule-based system to monitor network traffic and identify malicious activity.

File Integrity Monitoring: OSSEC can monitor the integrity of files on a cloud platform to detect any changes that may indicate a security breach. It can detect modifications to system files, configuration files, and application files.

Log Management: OSSEC can collect and analyze log data from cloud infrastructure to identify security threats. It can correlate log data from multiple sources and generate alerts for suspicious activity.

Compliance Management: OSSEC can help organizations comply with security standards such as PCI-DSS, HIPAA and SOC2.

Real-time Alerts: OSSEC can provide real-time alerts for security breaches and suspicious activity, allowing organizations to quickly respond to potential threats.

Centralized Management: OSSEC can be used to manage and monitor multiple cloud platforms from a single console, providing a centralized view of security across an organization's cloud environment.

At Logiq.ai, we recognize the need for comprehensive security measures that protect our clients and their sensitive data from potential cyber attacks.

By leveraging OSSEC's intrusion detection capabilities, Logiq.ai ensures a secure environment for our customers' data and applications, providing peace of mind and confidence in our services.

SUMMARY

LOGIQ can directly ingest security event logs from agents compatible with OSSEC (Open Source Security), which is a host-based intrusion detection system (HIDS) that can be used on a variety of platforms.

OSSEC provides a number of capabilities to help secure cloud platforms, including log examination, file integrity monitoring, Windows registry monitoring, centralized policy enforcement, rootkit scanning, and real-time alerting/active response.

LOGIQ.AI takes over the functions of the manager and the local OSSEC server, making it easy to bring together security-related events into your data fabric for instant consumption.

OSSEC can be used for intrusion detection and prevention, file integrity monitoring, log management, compliance management, real-time alerts, and centralized management.