TectOnaS

# LOG SLEUTH

COLLECT, CONNECT, AND PROTECT

● ● ● www.tectonas.com

## LOG SLEUTH

| | |
|---|---|
| **Customer** | Banks, Defence, Government, PSUs, Corporates |
| **Customer Requirements** | Transform your IT assets' logs into a powerful security tool, providing your teams with real-time insights to detect and respond to potential threats. |
| **LOG SLEUTH Solution** | Collect, connect, and protect: Our platform brings together logs from all sources, helping you identify and reduces security risks. |

## WHY LOG SLEUTH?

IT system logs are necessary for many businesses to maintain and review in order to identify errors, anomalous activity, or unauthorized access. The entire organization benefits from this. By using, Log Sleuth, you can save time and money by identifying issues early on.

Our tool helps IT and security teams fix issues in systems and apps by looking at logs. It also helps them check how well things are working and find areas to improve.

Our tool also helps security teams to find suspicious activities, strange behavior, or unauthorized access attempts, so they can respond quickly and reduce risks.

### THE CHALLENGE

- Gathering all kinds of logs from various sources into one place.
- Converting different logs into a standard normalize format, eventually making it easy to understand.
- Finding patterns or unusual things, like a cyber-attack, by looking at all the logs together.

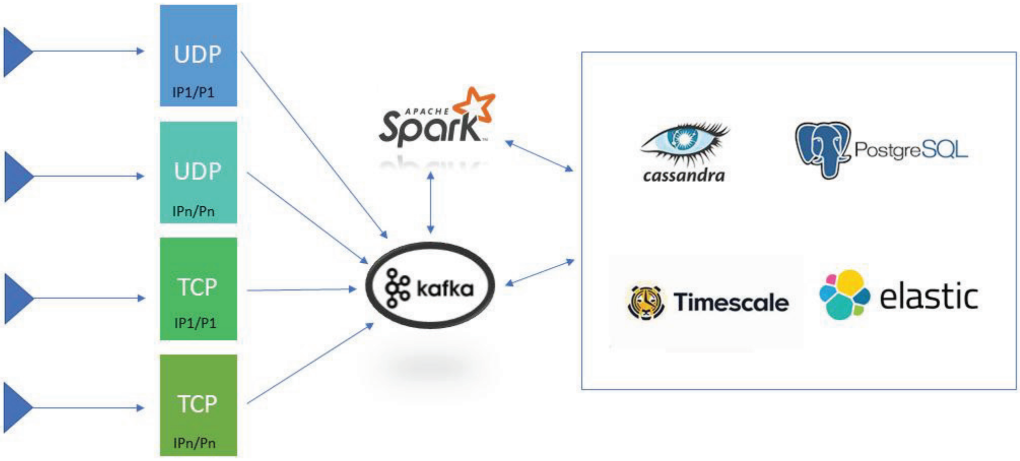
### LOG SLEUTH SOLUTION

- It gathers data from many sources quickly and easily.
- Makes sense of the data by finding patterns recognition and correlation.
- Filters normal log entries during analysis and focuses on unusual things to reveal problems.

### RESULTS & BENEFITS

- Keep an eye on all logs from various sources from centralized location.
- Get automatic alerts when something suspicious is found, so you can take action.
- Use Log Sleuth to catch illegal access attempts and check that security operations and firewalls are configured properly.

# THEORY OF OPERATION



LOG SLEUTH is a versatile and robust system that can scale with your evolving requirements. Additionally, it offers significant cost savings and can be seamlessly integrated across various environments. Plus, it can store and access data in a way that makes sense for you. LOG SLEUTH can collect data from many different sources, like system logs, network logs, application logs, SNMP, MS Event Logs and etc.

These collectors bring together logs from different sources, like network devices, servers, and firewalls, to help find connections between them. This helps reveal hidden patterns and clues that might show an attack is happening. LOG SLEUTH uses advanced AI and machine learning to find unusual patterns in the data, so you can catch problems before they become big issues.

LOG SLEUTH can work with many different types of messaging protocols and can be set up in a way that makes it very reliable and scalable. It can also be set up in a cluster to make sure it's always available and can handle a lot of data.

LOG SLEUTH deliver messages at network limited throughput using a cluster of machines with latencies. LOG SLEUTH is capable of scaling production clusters up to a thousand brokers, processing trillions of messages per day, storing huge amount of data, and managing hundreds of thousands of partitions. It safely stores data streams in a reliable and fault-tolerant system that can withstand failures.

LOG SLEUTH spreads out its resources across different locations to ensure high availability and can also connect multiple locations together.

## LOG SLEUTH BENEFITS

- Enhanced Security Posture: Log Sleuth plays an important role in securing your defenses by proactively identifying and addressing weaknesses before malicious actors can make use of them.
- Compliance Assurance: Generate detailed reports that align with regulatory requirements, ensuring Compliance with standards like GDPR, HIPAA, etc.
- Operational Efficiency: Log Sleuth helps organizations identify and fix problems quickly by analyzing logs to find errors and trends across different teams and departments.
- Risk Mitigation: Log Sleuth helps prevent costly security breaches by catching and fixing problems early.

### GLOBAL CYBERSECURITY STANDARDS RECOMMEND LOG SLEUTH :

Log Sleuth is recommended because it helps companies catch problems early, saving time and money. It also helps take quick action to prevent small issues from becoming big problems that cause downtime.

### ABOUT TECTONAS LOG SLEUTH SOLUTIONS :

Tectona offers end-to-end solutions in log monitoring, reporting, security policy compliance, audits, and regulatory compliance. It also supports security incident response and forensic investigation. Log SLEUTH enables organizations to identify more precisely the potential threats and issues in log data, uncover the root causes of problems, and initiate prompt responses to mitigate risks.

Contact us at sales@tectonas.com to get a test drive.