# ANLYZ SIEM - CYBERAL

PRODUCT SHEET

## Empower your SOC with cloud native, next-gen cognitive SIEM

Enable your SOC team to navigate today's dynamic threat landscape with Cyberal – Anlyz's cognitive SIEM. Cyberal collects logs from disparate sources, seamlessly normalizes and runs them through advanced correlations, and sends the alerts to an Incident Response or SOAR platform.

The unlimited data lake enhances the ability to correlate more alerts and identify more threats at no additional cost. The AI- ML engine provides contextual analysis, proactive insights, and enhanced correlation; reducing redundancy and increasing efficiency of alerts.

Cyberal is also one of the very few SIEM's which supports multi-tenancy – enabling your security team to manage multiple tenants/customers/ BUs out of a single console. Powered by machine learning & UEBA, it proactively alerts SOC teams about security incidents that deviate from standard behaviour.

### KEY BUSINESS CHALLENGES

**ALERT OVERLOAD -** Security analysts are often overwhelmed by overload of alerts, which hampers decision-making

**TALENT SHORTAGE -** Limited Skilled Resources impact efficient management of security incidents

**INVESTIGATION -** An average Root Cause Analysis(RCA) of a cybersecurity incident takes about 4 Days, meaning more time required to remediate the point of breach

**SECURITY IN SILOS -** Large enterprises house multiple security solutions working in silos, which prevents SOC teams from building an investigative roadmap of threats

**HIGHER MTTD/MTTR -** More time to detect & respond for security teams leads to elongated risk exposure

# KEY FEATURES

## Data Enrichment, Contextual Analysis and Real Time Insights

Anlyz SIEM contains an in-built Knowledge Base with details regarding customer's critical assets, priority users, approved applications, and internal IPs/Subnets. This data set is leveraged to enrich the alerts coming from multiple sources providing more information to analysts to make faster decisions.

The Cyberal platform's data ingestion is architected in a high performance pipeline that performs Data Enrichment when the data gets ingested. This helps in having multiple contextual mapping and tagging done (example – MITRE, Custom asset) when the data is getting stored.

Analytics and Alerting using context enrichment, Machine learning, 150+ qualitative, complex OOB Correlation rules and scoring risk across identities and devices thus ensuring high fidelity alerts.

## Centralized view with interactive dashboards

Easily customizable interactive dashboards that are role-based, location-based, and device-based, providing better visibility & holistic view of the network.

## Integrated, custom connections

Anlyz SIEM's simplistic build supports ingestion of data from most industry standard devices. With ready support for standard formats like syslog, CEF, and LEEF format logs, Cyberal also provides customized connections, with the Anlyz team providing extended support in building the new custom connectors easily and swiftly.

## Scalable, cloud SIEM

Get top performance without bleeding costs with a scalable SIEM which can be deployed on-prem or on the cloud. With this hybrid approach, Cyberal offers unparalleled scalability with high cost optimization, empowering your security team to ingest high volume of data without any hassle.

## Threat Intelligence Integration

Anlyz SIEM connects with multiple threat intel platforms with an additional option to import feeds over STIX/TAXI. This integration helps SOC teams recognize and act upon indicators of attack(IOA) and compromise scenarios in a timely manner. You are now empowered to get curated results about threats specific to your environment and also look beyond to see where else it may exist thus forming a proactive defense.

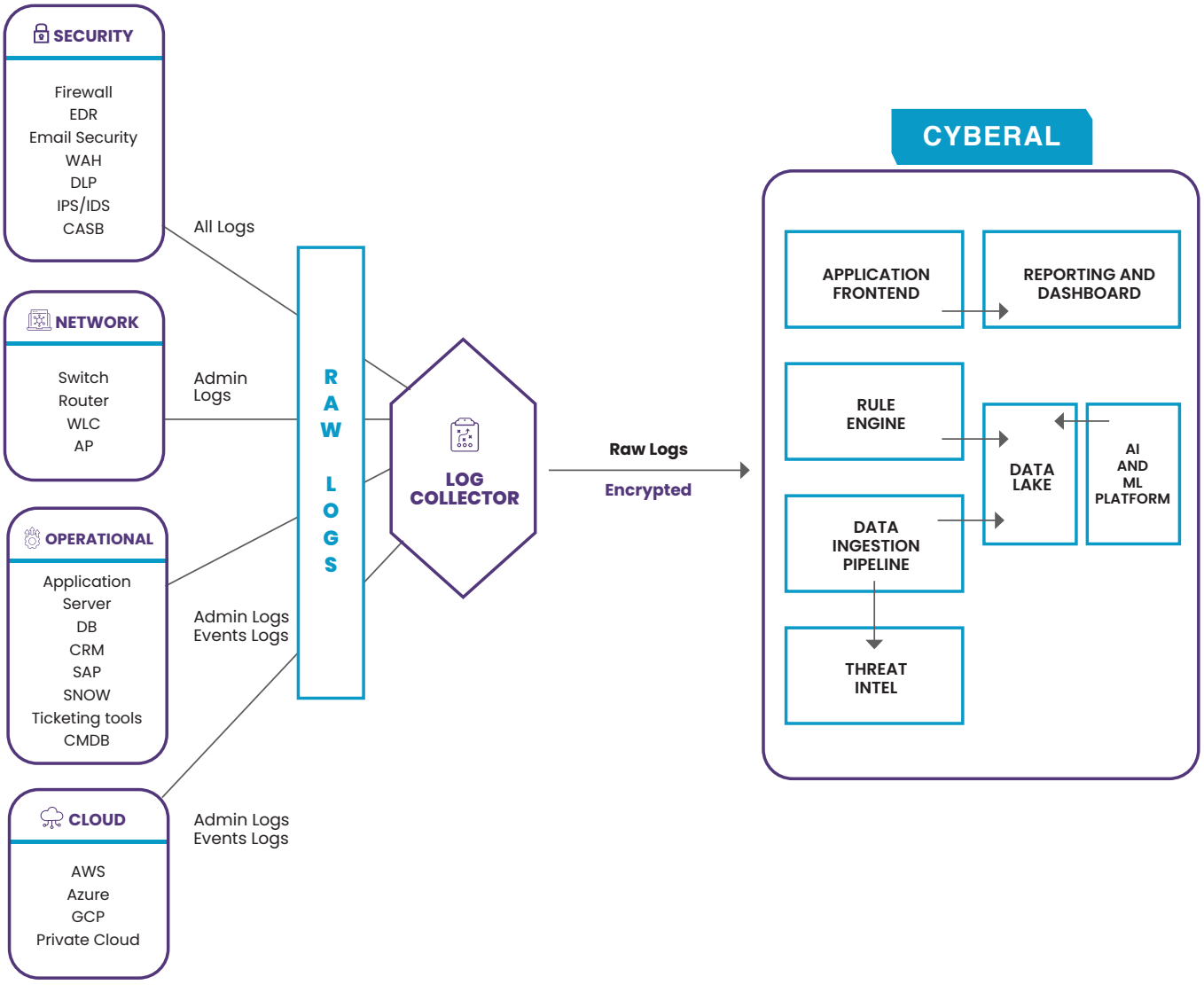
## UEBA

Powered by Machine Learning and UEBA, Cyberal can detect security incidents that deviate from standard behaviour. Cyberal goes beyond the confines of traditional SIEM features by providing advanced threat detection which can identify insider threats, hidden malware infections, and much more. This proactive way of monitoring user and entity behaviour provides an additional layer of threat detection to SIEM that help to find complicated threat with reduced noise.

## Multi-Tenancy

In a large enterprise environment and for MSSPs, it becomes imperative to have separation of data, reporting, compliance across multiple entities/ tenants. Anlyz SIEM platform is multi-tenant, that ensures a large corporation or a MSSP is easily able to manage varied requirements across multiple tenants from a single platform thereby ensuring economies of scale, ease of management, scalability of new services, without compromising on the threat detection.

# HIGH LEVEL ARCHITECTURE



## KEY BENEFITS

### 1. SCALABILITY

Cyberal can be adopted both on the cloud and on-premises, ensuring exceptional scalability for the enterprise according to changing demands

### 2. EFFICIENCY AND GREATER ECONOMIES OF SCALE

Cyberal supports multi-tenancy, which helps large enterprises as well as MSSP's to create segregated tenants from a single environment. This helps organizations to manage SIEM efficiently and derive greater economies of scale

### 3. COMPLIANCE

Meet all your compliance requirements with Cyberal's compliance management module, which enables data retention and regulatory report automation for security teams for the purposes of governance and compliance

### 4. REDUCED MTTD, MTTR

Advanced correlation capabilities with powerful machine learning & threat intel helps effectively identify and isolate security events. Furthermore, Cyberal's UEBA feature detects security incidents that deviate from standard behaviour, resulting in high fidelity alerts for SOC teams


Contact us at

contact@anlyz.co

www.anlyz.co