# Managed Security Services

CYBANETIX

Secure your business, people and network.

Cybanetix Limited
cybanetix.com

Registered at:
The Coade
Level 9
98 Vauxhall Walk
London
SE11 5EL

Company Registration: 10558582
VAT Number: GB 262502430

# ABOUT US

**Key Partnerships:**

- SentinelOne Technical Partner of the year 2024
- Member of SentinelOne Paladins (highest level of technical expertise)
- Exabeam EMEA MSSP of the year 2021-2023
- Founding member of Exabeam Emerald Club
- Microsoft Partner (Cloud Solutions) 2023

**Our Certifications:**

- ISO27001 – Information Security Management
- ISO9001 – Quality Management
- ISO14001 – Environmental Management
- PCI-DSS – Payment Card Data Security
- Cyber Essentials – UK government-backed

## COMPANY BACKGROUND

CYBANETIX

- Founded in 2017 by industry experts
- UK based cybersecurity specialist, offering comprehensive protection across all attack surfaces.
- Providing managed security services to a diverse array of sectors, including Retail, Manufacturing, Media, Entertainment, Education, and Travel.
- Experienced MSSP to highly regulated industries such as Critical Infrastructure, Financial Services, and Utilities.
- Clients include Blue-chip/FTSE 250 firms and globally recognised brands

## MANAGED SECURITY SERVICES

Specialist in providing high quality Managed Security Services that are tailored specifically to customer needs and target outcomes, including:

- 24/7/365 Security Operations Centre
- Managed Detection & Response (MDR/MEDR)
- Full Security Outsourcing
- Extended, Detection & Response (XDR)
- Security Orchestration, Automation, Response (SOAR)
- External Threat Management & Brand Protection
- Security Posture and Vulnerability Management
- Managed Firewall, Email, and Mobile Services

exabeam Services Partner of the Year 2023

SentinelOne Technical Partner of the Year 2024

Microsoft

# MANAGED SERVICE DIFFERENTIATORS

**All Inclusive Service:**

- ✓ No hidden costs
- ✓ Fixed, predictable service cost
- ✓ UK based, SC Cleared SOC
- ✓ Built-in threat intelligence and automation
- ✓ Vulnerability Management Service

**Outcome Focused:**

Managed Services tailored specifically to our customers' security needs and requirements.

**Service Agility:**

Agile service that adapts to evolving customer security needs, risk profiles, and technological advancements

**Service Quality:**

We prioritise high-quality service across all industries, ensuring security and customer satisfaction through aligned Service, Technical, and Project representatives

## Security Experts

SOC and SecDevOps teams with advanced analytical and technical expertise, spanning multiple technologies and vendors.

## Streamlined Security Workflows

We utilise pre-built and custom automations to optimise security workflows, drive service consistency, and to accelerate threat detection and response.

## Industry Leading Response

The Cybanetix SOC guarantees an industry-leading <15-minute response time to all detected threats, regardless of type, vector, or severity.

## Continuous Security Improvement

We leverage SOC telemetry and reporting data to drive continuous improvements to both our service and our customers security posture.

# MANAGED SERVICES OVERVIEW

# MANAGED SERVICE OVERVIEW

CYBANETIX

## SERVICE HIGHLIGHTS

24/7/365 UK SOC, with guaranteed **<15-minute** response SLA, regardless of severity

**Human monitoring** of customer systems providing real-time security **alerts** with detailed **investigation** and forensic analysis

Built in **threat intelligence** and **automation** (SOAR), enhancing SOC workflows across detection, enrichment, investigation and response

**Dynamic reporting portal** for on-demand access to security metrics, trend data and tailored reports

## KEY BENEFITS AND OUTCOMES

**Holistic visibility** of your security posture, spanning cloud, on-premise and hybrid environments

**Rapid detection and response** to malicious and suspicious events, including auto-containment

Investigation and Response workflows **fully aligned with customer** teams, ITSM toolsets, and existing incident managed processes

Reduce overall business risk by enabling **early detection** and response to security threats

# MANAGED SERVICE - CORE DELIVERABLES

The Cybanetix MDR Service is offered as an all-inclusive package, providing fully managed onboarding, core technology management, 24/7 security monitoring, and comprehensive service delivery.

## TECHNOLOGY ONBOARDING

- SIEM & EDR roll-out/take on
- Setup/integration of core technologies
- Review/on-board log sources
- Configure new connectors
- Setup:
  - SIEM Dashboards
  - Detection & Alerting rules
  - Role Based Access
  - Data models
- Define retention policies
- Alert testing and verification

## SIEM & EDR PLATFORM MANAGEMENT

- Day to day platform configuration
- On-boarding of new log sources
- Move/Adds/Changes
  - Security Policies
  - Dashboards
  - Alerts and detection rules
  - Incident Management playbooks
- Ensure alignment to relevant compliance schemes
- Optimise log ingestion

## SERVICE DELIVERY & OPERATIONS

- 24/7 15-minute response
- Agree communications and escalation plans
- Track Service Level Agreements
- Manage Service Change controls
- Incident investigations:
  - Critical alerts from defined security vendors
  - High and medium severity threats
  - Customer raised/ad-hoc forensic investigations
- Containment of threats for mutually agreed IR playbooks
- Support and/or orchestration of Major incident response
- Service Reporting

## ALIGNED RESOURCES

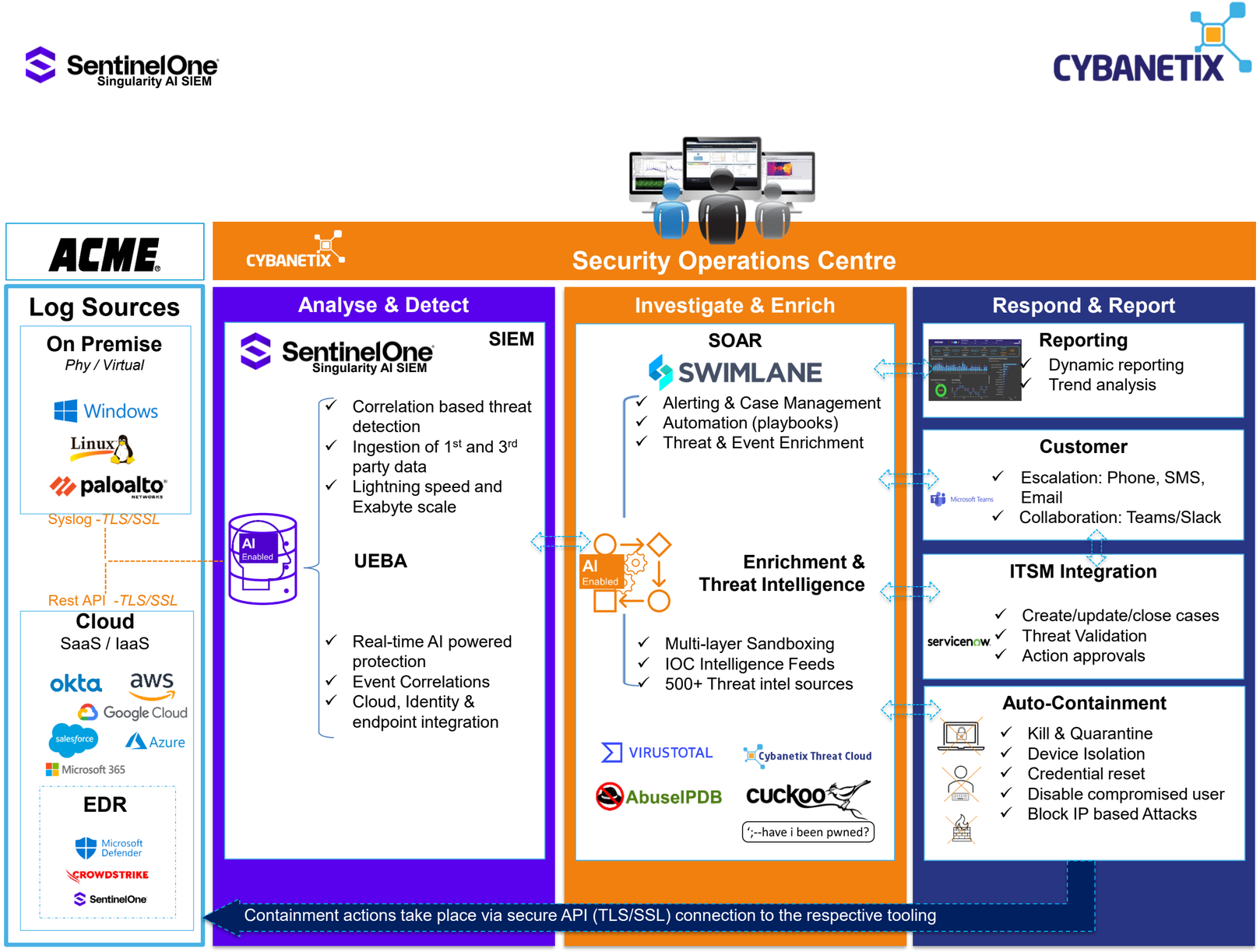
- Key resources aligned for both project and BAU:
  - Account Manager - Ultimate responsibility for contract performance
  - Project Manager - Ensures mature governance and a streamlined project management structure
  - Service Delivery Manager - Responsible for day-to-day performance management and reporting.
  - Focal Security Engineer – Ensures technical functionality is aligned to changing requirements and security needs

# TECHNOLOGY ARCHITECTURE

# MANAGED SERVICE TECHNOLOGIES

SentinelOne's AI SIEM, delivered as part of the Singularity cyber security platform.

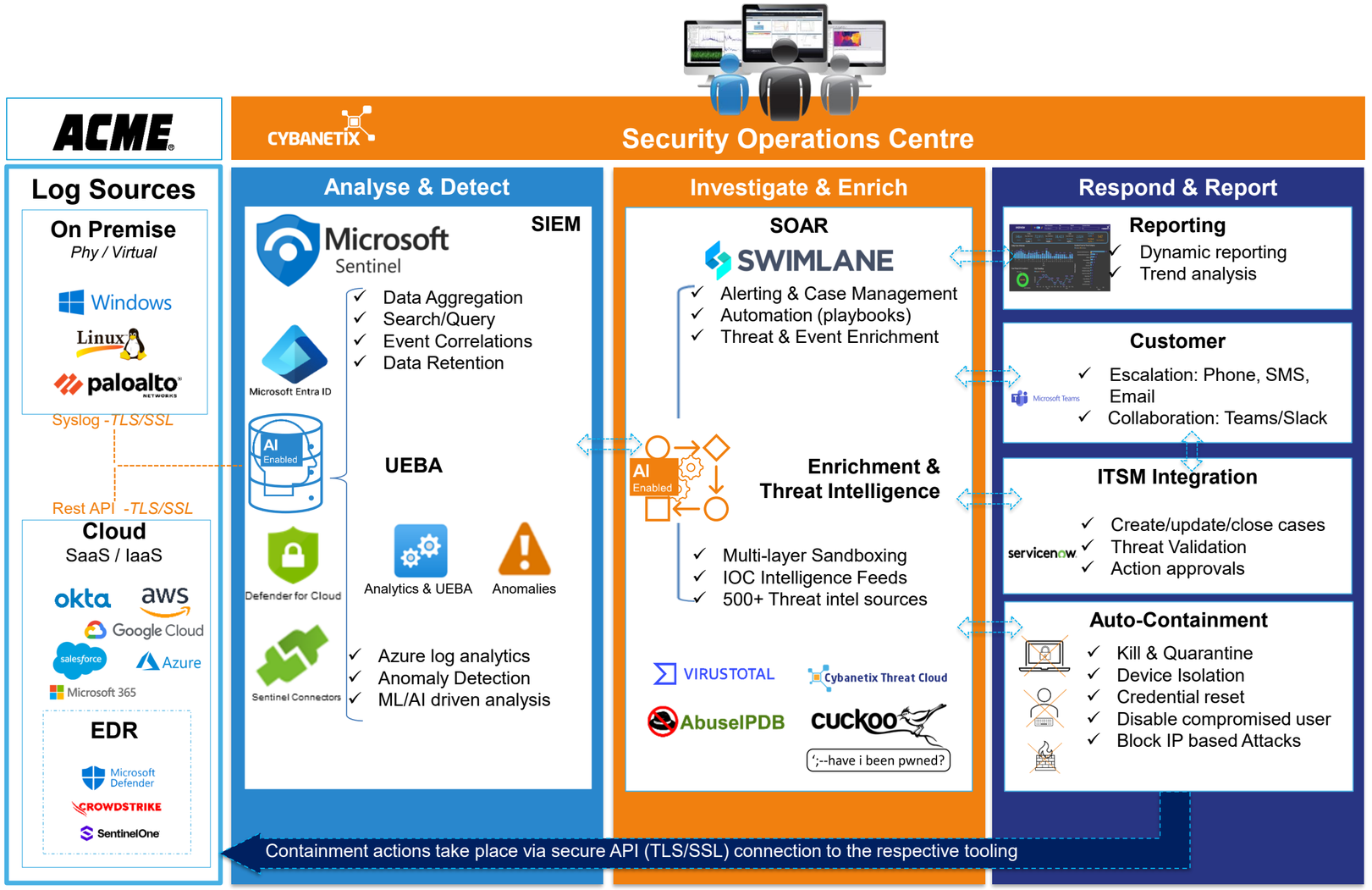
- ✓ Collect security data from a wide array of sources, providing a comprehensive view of the security landscape, enabling accurate threat detection.
- ✓ Built on a scalable, cloud-native infrastructure that can handle increasing data volumes and complexity.
- ✓ Consolidate SIEM and EDR into a single, unified security ecosystem that simplifies operations and enhances interoperability.
- ✓ Continuous service improvement program to enhance security posture and response:
  - Increase security automation
  - Expand detections and use cases
  - Identify and onboard new Log sources



# MANAGED SERVICE TECHNOLOGIES

Cybanetix will integrate and manage the existing Microsoft Sentinel SIEM and Defender EDR platforms into our MDR Service:

- ✓ Augment existing SIEM and EDR platforms with advanced security automation and threat intelligence.
- ✓ Maintain continuous protection and operational stability, avoiding complex SIEM technology migrations.
- ✓ Avoid security coverage gaps that could arise during technology transitions, ensuring comprehensive protection.
- ✓ Continuous service improvement to enhance security posture and response:
  - Increase security automation
  - Expand detections and use cases
  - Identify and onboard new Log sources
  - Optimise log ingestion



# MANAGED SERVICE TECHNOLOGIES

Exabeam SIEM and UEBA provides enhanced detection, investigation, and response capabilities through the application of advanced AI and machine learning behavioural analysis.

- ✓ Uses machine learning to identify anomalous behavior patterns, enabling the detection of sophisticated threats and insider attacks that traditional security tools might miss
- ✓ Reduced False Positives by focusing on behavior rather than predefined signatures
- ✓ Effective threat detection across even the most diverse and complex IT environments
- ✓ Continuous service improvement program to enhance security posture and response:
  - Increase security automation
  - Expand detections and use cases
  - Identify and onboard new Log sources

exabeam

CYBANETIX

ACME

CYBANETIX

## Security Operations Centre

### Log Sources

**On Premise**
*Phy / Virtual*

Windows
Linux
paloalto NETWORKS

Syslog - *TLS/SSL*

Rest API - *TLS/SSL*

**Cloud**
SaaS / IaaS

okta
aws
Google Cloud
salesforce
Azure
Microsoft 365

**EDR**

Microsoft Defender
CROWDSTRIKE
SentinelOne

### Analyse & Detect

exabeam **SIEM**

- ✓ Data Aggregation
- ✓ Search/Query
- ✓ Event Correlations
- ✓ Data Retention

AI Enabled

**UEBA**

- ✓ Behavioural modelling
- ✓ Anomaly Detection
- ✓ Risk Scoring
- ✓ ML/AI driven analysis
- ✓ Threat Hunting

### Investigate & Enrich

**SOAR**

SWIMLANE

- ✓ Alerting & Case Management
- ✓ Automation (playbooks)
- ✓ Threat & Event Enrichment

AI Enabled

**Enrichment & Threat Intelligence**

- ✓ Multi-layer Sandboxing
- ✓ IOC Intelligence Feeds
- ✓ 500+ Threat intel sources

VIRUSTOTAL
Cybanetix Threat Cloud
AbuseIPDB
cuckoo
';--have i been pwned?

### Respond & Report

**Reporting**

- ✓ Dynamic reporting
- ✓ Trend analysis

**Customer**

Microsoft Teams

- ✓ Escalation: Phone, SMS, Email
- ✓ Collaboration: Teams/Slack

**ITSM Integration**

servicenow

- ✓ Create/update/close cases
- ✓ Threat Validation
- ✓ Action approvals

**Auto-Containment**

- ✓ Kill & Quarantine
- ✓ Device Isolation
- ✓ Credential reset
- ✓ Disable compromised user
- ✓ Block IP based Attacks

Containment actions take place via secure API (TLS/SSL) connection to the respective tooling

# SERVICE DELIVERY

# APPROACH METHODOLOGY

Cybanetix have a proven methodology for transitioning customers to our MDR

Service, including the migration of pre-existing customer technologies.

The methodology proposed includes 3 workstreams: Take on, Transform and Improve.

CYBANETIX

## Take On / Onboard

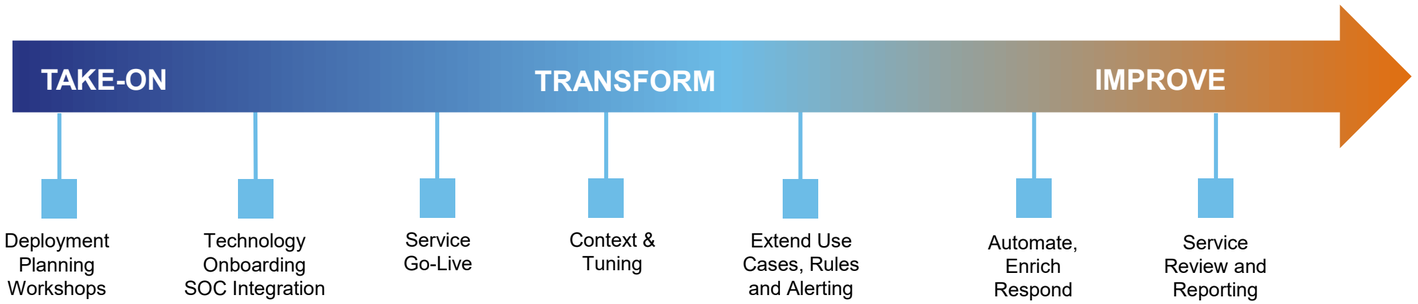
- Integrate core SIEM and EDR technologies into the Cybanetix SOC and Case management platform
- Review/validate existing SIEM log sources, use cases and rules, EDR coverage and policy configurations
- Apply standard SOC playbooks (automation) for SOC incident management (alerting, triage, investigation)
- Activate initial 24/7/365 security monitoring, based on existing security use cases and detections

## Transformation

- Tune existing SIEM & EDR rules and event correlations to improve detection and reduce false positives
- Apply Cybanetix SOC security use case and detection library (over and above pre-existing)
- Identify options to develop/apply advanced playbook automations, i.e. enrichment, faster containment
- Normalise data across security operations for improved and consistent security reporting

## Improve

- Analyse SOC telemetry to identify potential weakness and/or gaps in security posture
- Use reporting data to help inform and support customer security strategy and focused initiatives
- Continuous review, tuning and optimisation of SIEM detection rules and EDR policy.
- Continuously explore technical roadmaps, service enhancements to drive down security risk profile.



# MANAGED SERVICE ARCHITECTURE

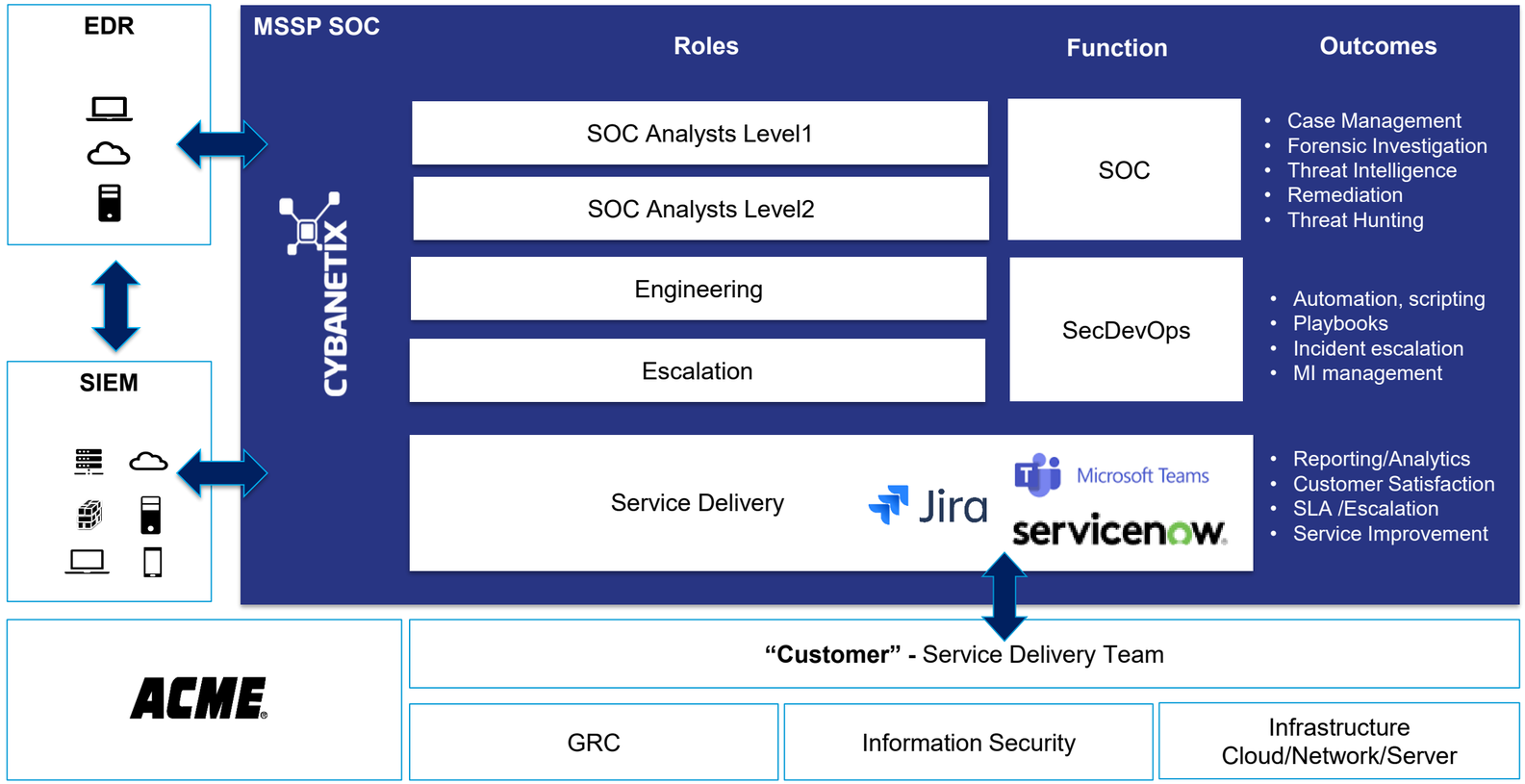
**SOC Operations:** Level 1/2 Analysts handling high velocity alerts. A triage point from L1 to L2 allows forensic analysis of alerts and where appropriate escalation to customer security teams. SOC Analysts are supported by senior level escalation contacts.

**Account & Service Delivery:** The following resources will be aligned:

- **Account Manger** - holds ultimate responsibility for contract.
- **Service Delivery Manager (SDM)** - responsible for performance management and reporting.
- **Lead Engineer** - technical authority working closely to implement technical and service changes, and drive security posture improvements.

**Customer Engineering:** Responsible for continuous development of our technology and security service capabilities.

**Service Integration:** Day to day collaboration between Cybanetix aligned resources and customer internal teams via preferred communications platforms, e.g. Teams, ServiceNow and Jira.



# SERVICE LEVELS

Industry leading SLA, guaranteeing 15-minute human-led response to all alerts

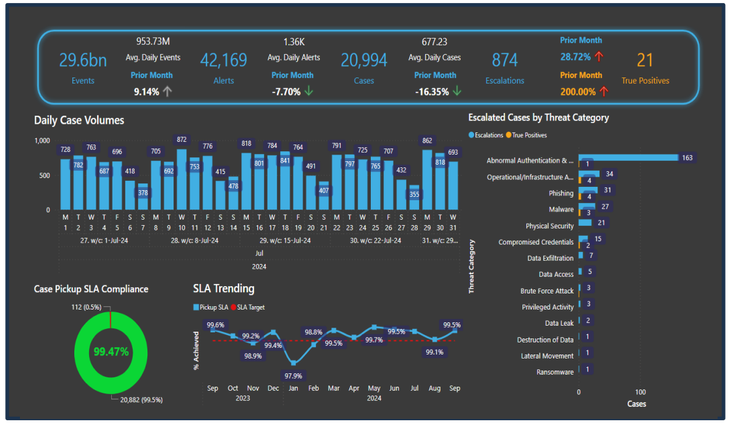
| | |
|---|---|
| First triage and investigation started | LESS THAN 15 MINUTES |
| Time to complete initial investigation of an alert | LESS THAN 1 HOUR |
| Technology Platform faults - P1<br>Service down/unavailable/<br>e.g. no ingestion of logs | RESPOND WITHIN 30 MINUTES |
| Technology platform faults - P2<br>reduced service/performance | RESPOND WITHIN 2 HOURS |
| Technology platform faults- P3<br>Minor/isolated issues not affecting the main service, e.g. single Log source not working (during standard hours only) | RESPOND WITHIN 8 HOURS |
| Service requests response<br>(during standard hours only) | RESPOND WITHIN 8 HOURS |

# SERVICE REPORTING

Reporting is provided via our dynamic reporting portal, offering customers secure, on-demand access to their data

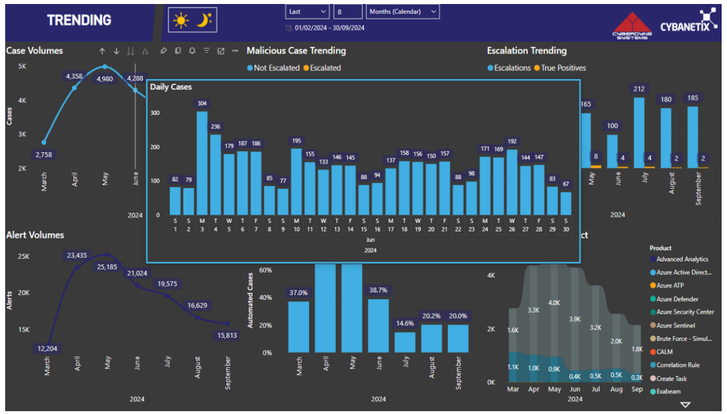
**Monthly highlight** reports contain a summary of security and service metrics for the given period, such as incident volumes and types, threat insights, and trends for the given period.

**Quarterly Service Review** is typically a face-to-face meeting where the Cybanetix Service Delivery Manager will provide a comprehensive report of the service and associated security metrics. The report will include detailed security and service-related metrics such as; number of incidents, type of incidents, time of incidents, severity of incidents, average response times, false positives, SLA performance analysis, use case statistics, technology health and performance, and configuration change management. This report is used to monitor trends within the security posture and refine the service accordingly.




**Tailored reporting**

Cybanetix provide access to the reporting portal so customers can view, extract and build reports provided as part of the service. The portal has a dedicated report builder, allowing customers to build tailored reports covering all aspects of the service. Reports can be extracted as PDF or PPT formats and the reporting data can be extracted for use in external reporting tools in CSV format.




**Real-time data**

The portal polls data on a daily basis, with reporting data no older than 24hrs. Customers will also have access to the underlying SIEM/SOAR tooling should they wish to have real-time access to the data, which will include all relevant alerts, incidents and cases. The managed service will also be integrated into the customers own ITSM ticking platforms (such as ServiceNow or Jira) to ensure case and incident data is visible in real-time with customers being given access to case notes, updates and closure details.

# END