

Managed Detection & Response (MDR)



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

MDR SERVICE OVERVIEW



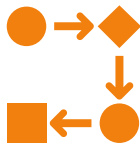
SERVICE HIGHLIGHTS



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



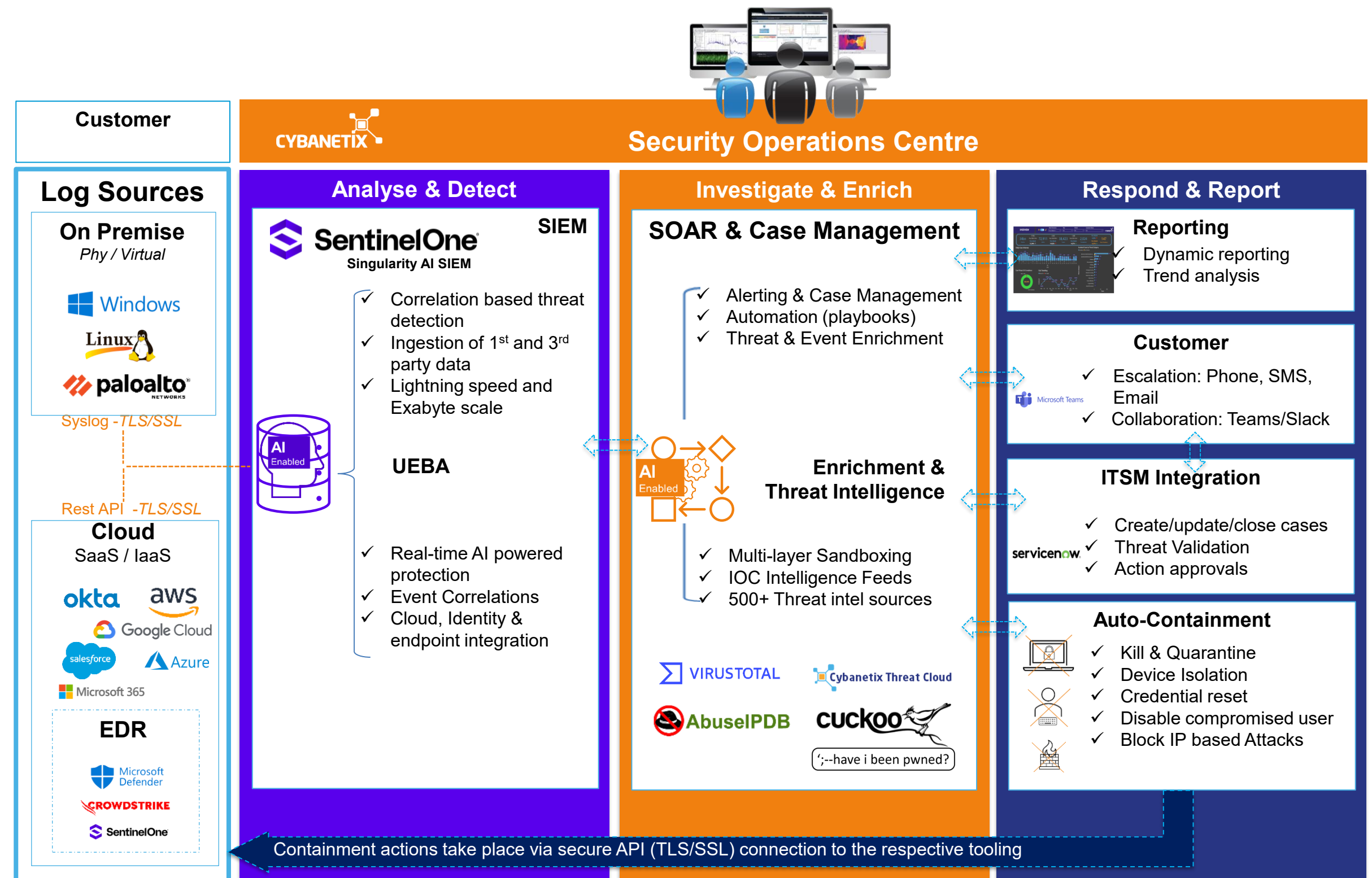
Reduce overall business risk by enabling **early detection** and response to security threats

CORE TECHNOLOGY OPTIONS

MDR SERVICE TECHNOLOGIES

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

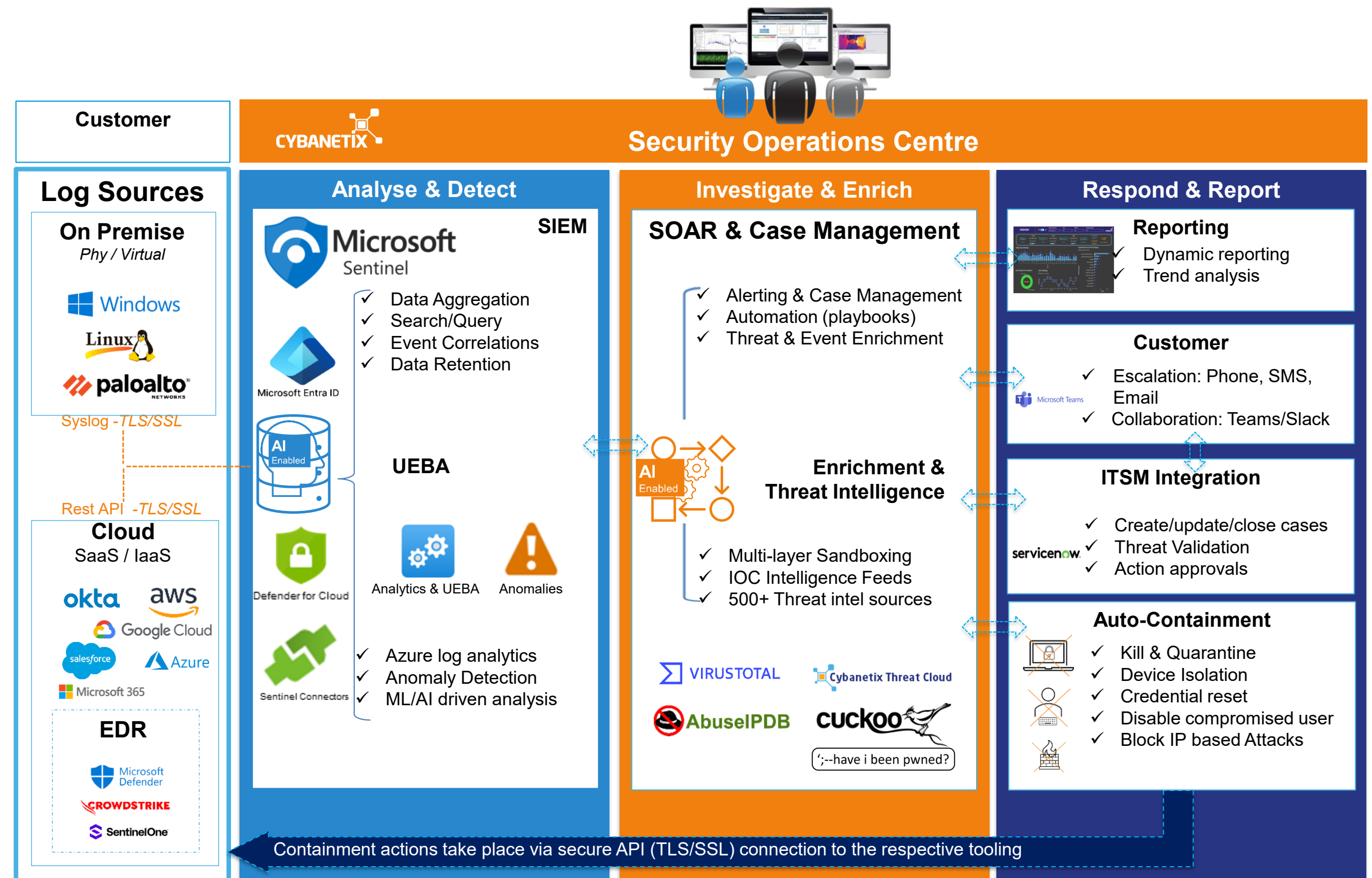
- ✓ Collect security data from a wide array of sources, providing a comprehensive view of the security landscape, enabling accurate threat detection.
- ✓ Built on a scalable, cloud-native infrastructure that can handle increasing data volumes and complexity.
- ✓ Consolidate SIEM and EDR into a single, 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



MDR SERVICE TECHNOLOGIES

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

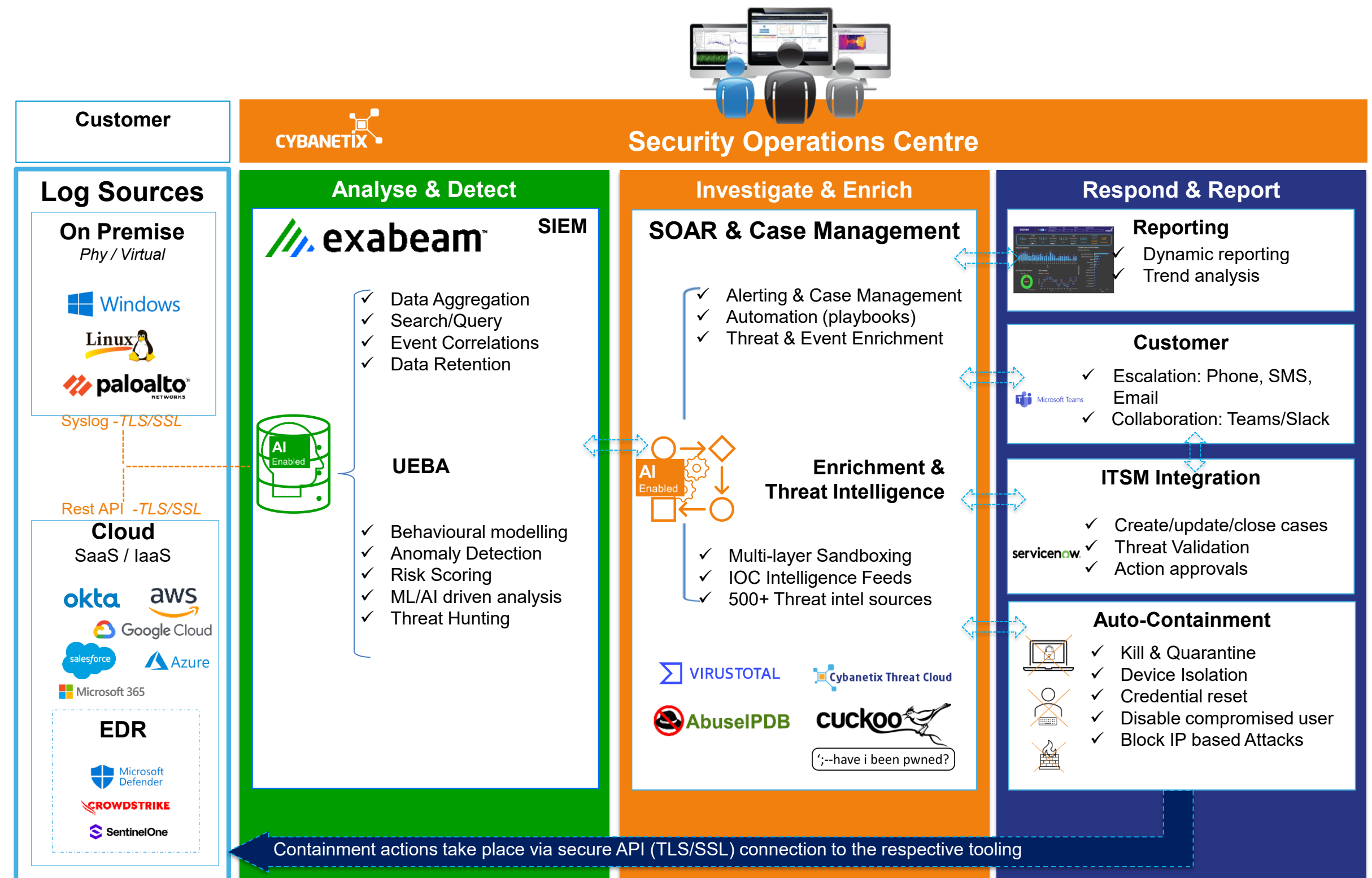
- ✓ Augment existing SIEM and EDR platforms with advanced security automation and threat intelligence.
- ✓ Maintain continuous protection and operational stability, avoiding complex SIEM technology migrations.
- ✓ Avoid security coverage gaps that could arise during technology transitions, ensuring comprehensive 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



MDR 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



SERVICE DELIVERY

ONBOARDING 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.



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



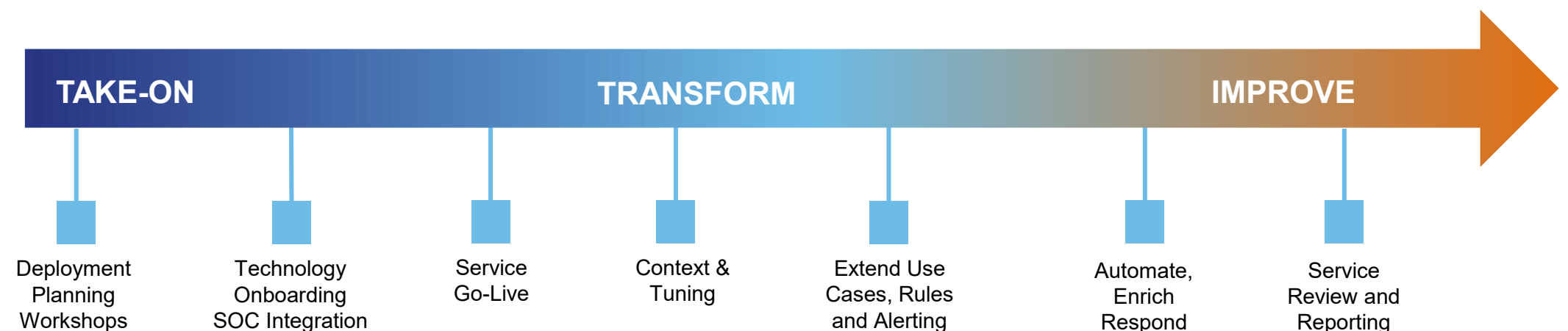
Transformation

- 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.



MDR SERVICE OPERATING MODEL

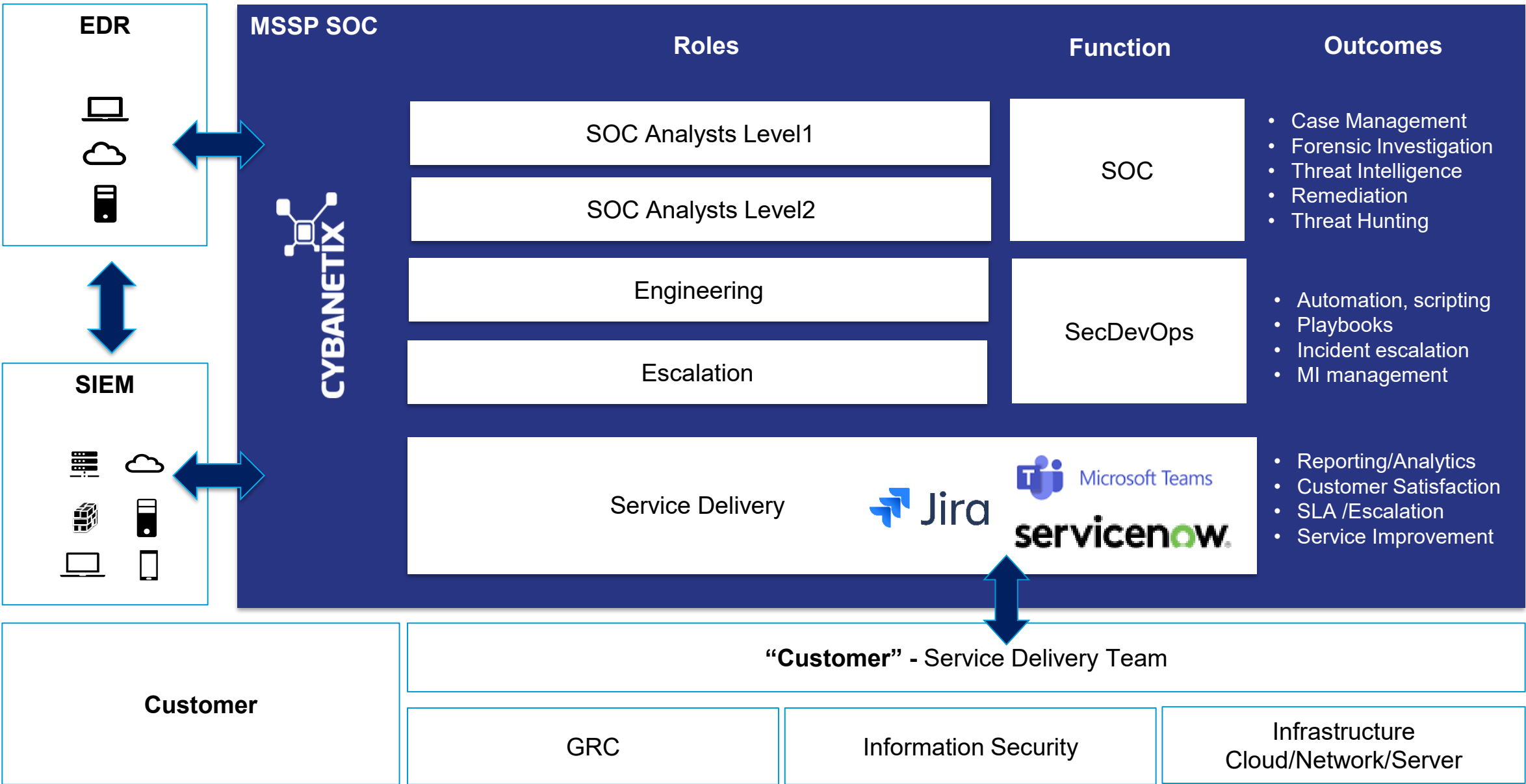
SOC Operations: Level 1/2 Analysts handling high velocity alerts. A triage point from L1 to L2 allows forensic analysis of alerts and where appropriate escalation to customer security teams. SOC Analysts are supported by senior level escalation contacts.

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.



MDR 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 Service down/unavailable/ e.g. no ingestion of logs		RESPOND WITHIN 30 MINUTES
Technology platform faults - P2 reduced service/performance		RESPOND WITHIN 2 HOURS
Technology platform faults- P3 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 (during standard hours only)		RESPOND WITHIN 8 HOURS

MDR SERVICE REPORTING



Reporting is provided via the Cybanetix Reporting Engine (CRE), 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.

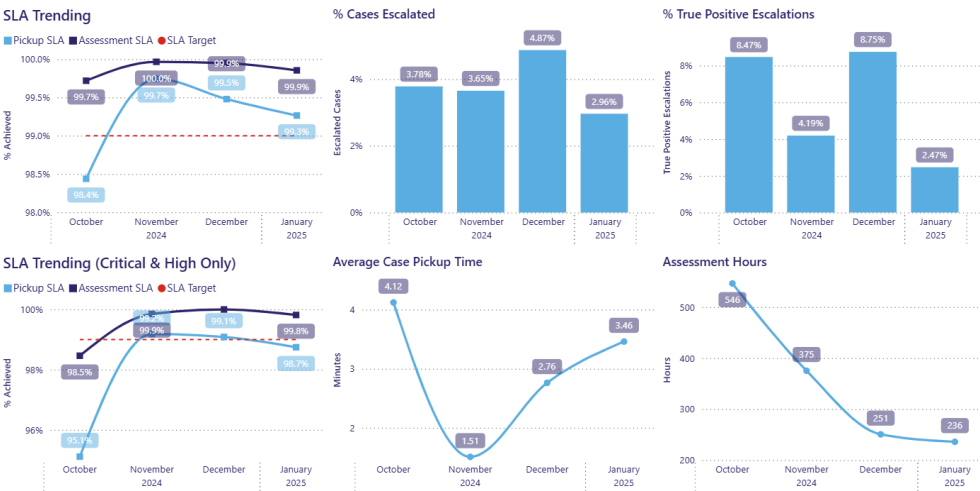
The portal has a dedicated report builder, allowing customers to build tailored reports covering all aspects of the service.

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 every 4 hours, 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.



MDR SERVICE

Value Proposition

All Inclusive Service:

- ✓ No hidden costs
- ✓ Fixed, predictable service cost
- ✓ UK BASED; SC Cleared SOC
- ✓ Built-in threat intelligence and automation

Outcome Focused:

MDR Service 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

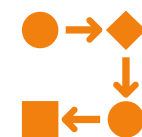
Service Quality:

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



Security Expertise

SOC and Engineering 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

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.

