e2e assure

**SOC as a Service**

Service Definition Document

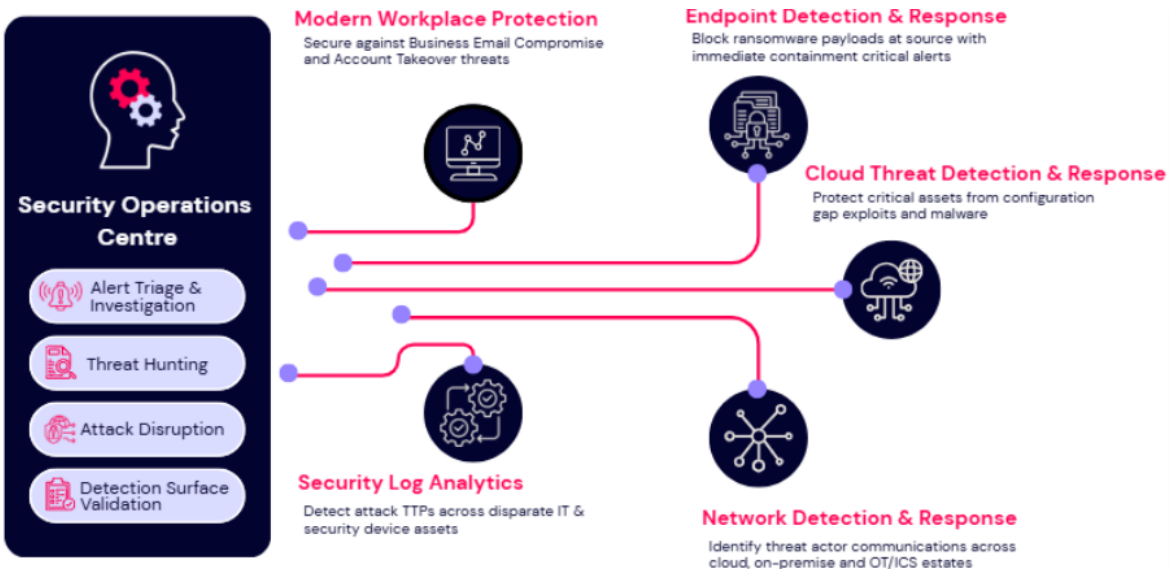
# SOC AS A SERVICE

## Service Definition Document – G-Cloud 15

CONTENTS

Services Used to Provide the Solution ..... 2
Security Operations Service ..... 2
Modern Workplace Protection ..... 3
Endpoint Detection and Response ..... 5
Cloud Threat Detection ..... 6
Network Detection and Response ..... 7
Security Log Analytics ..... 8
OT SOC Monitoring ..... 9
PRECON Dark Web Monitoring ..... 11
External Perimeter Monitoring ..... 12

## SERVICES USED TO PROVIDE THE SOLUTION




### Security Operations Service

The e2e-assure Security Operations Service is the foundation of our Threat Detection & Response portfolio. Delivered exclusively from our UK-sovereign, SC-cleared SOC, it blends specialist human expertise with our in-house platform, Cumulo, to provide 24/7 detection, investigation and response across your environment.

Our boutique operating model means every customer benefits from analysts who understand your sector, your threat landscape, and your normal patterns of activity. Cumulo leverages a catalogue of local AI Local Language Models (LLM) which inter-operate directly with your existing security tooling to unify telemetry, enrich signals, and orchestrate automated and analyst-led actions with precision.

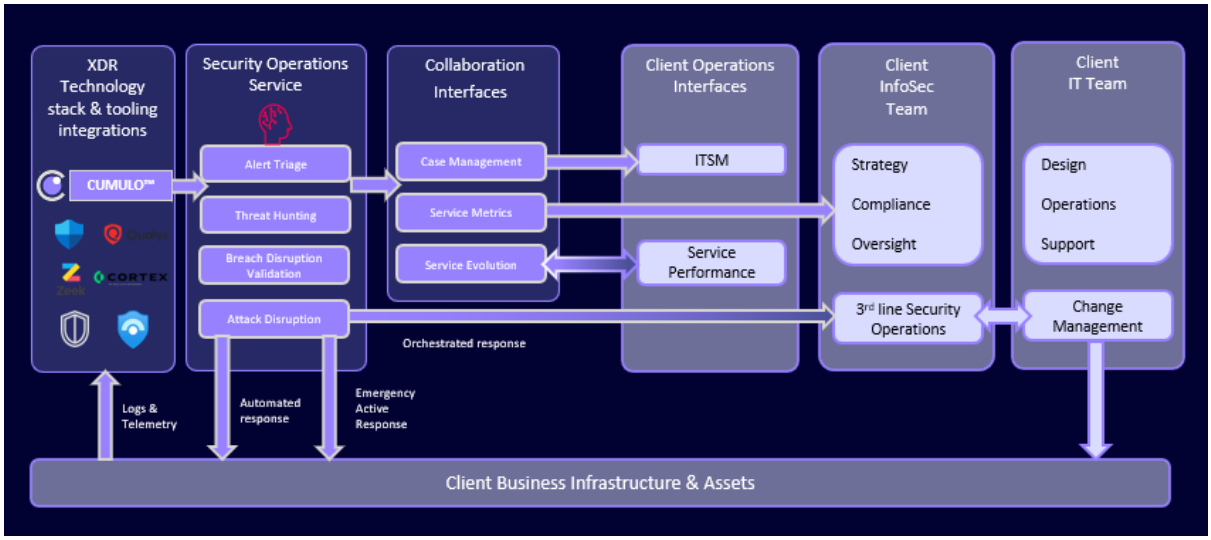
We operate against explicit, aggressive SLAs to minimise business impact:

- Critical Incidents: MTTD 15 minutes, MTTR 30 minutes
- High Incidents: MTTD 30 minutes, MTTR 1 hour
- Medium Incidents: MTTD 2 hours, MTTR 4 hours
- Low Incidents: MTTD 8 hours

Continual threat hunting sweeps driven by intelligent AI agents are combined with additional ad-hoc human hunts triggered by new intelligence or emerging threats, optional hypothesis-driven deep dives are a feature of our specialist approach. Where appropriate, we deliver automated, orchestrated or active analyst-led containment to disrupt attacks before they propagate.

To ensure continuous improvement, we offer quarterly Detection Surface Validation, combining analytics review, telemetry assurance, and attack simulation to verify that coverage aligns to MITRE ATT&CK and your evolving risk profile.

All activity, evidence and response actions are captured in Cumulo, providing a real-time view of posture, incidents, reporting dashboards and compliance-ready audit trails. Monthly reporting and structured service management ensure that your threat visibility, maturity, and resilience keep improving quarter-on-quarter.




## Modern Workplace Protection

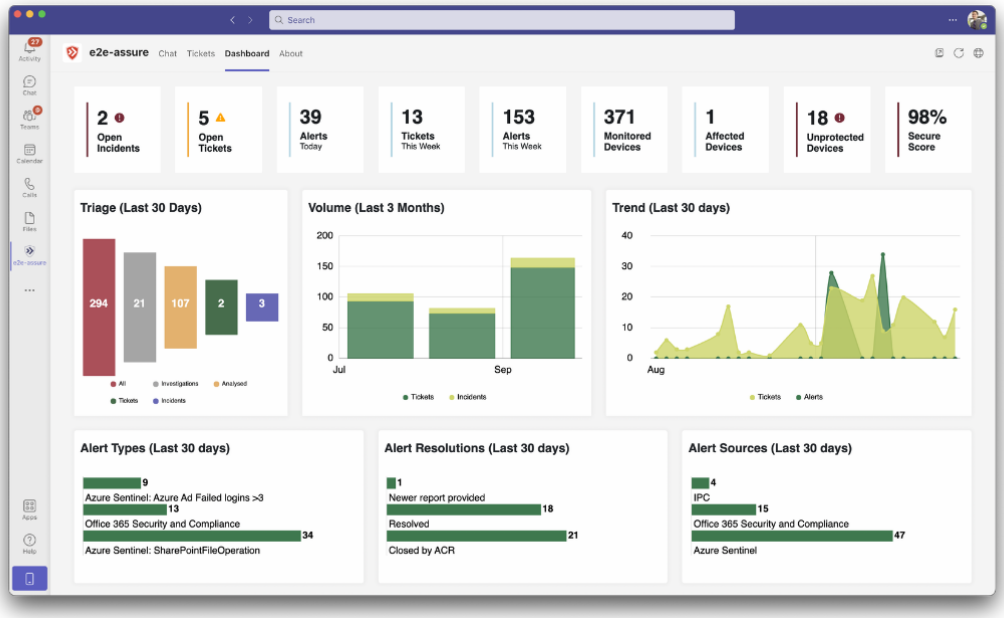
Modern Workplace Protection safeguards your environment against the most prevalent enterprise attack vectors: Account Takeover (ATO), Business Email Compromise (BEC), credential abuse and identity-led infiltration. Delivered through our UK-sovereign, SC-cleared Security Operations Centre and powered by the e2e-assure Cumulo platform, the service provides continuous monitoring and automated response to suspicious behaviour across identities, authentication events and privilege activity.

Deep integration with Microsoft Graph enables high-fidelity alerting against behavioural anomalies such as impossible travel, malicious sign-ins, MFA manipulation, privilege escalation attempts, and high-risk configuration changes. Incidents are raised automatically and triaged against our explicit SLAs.

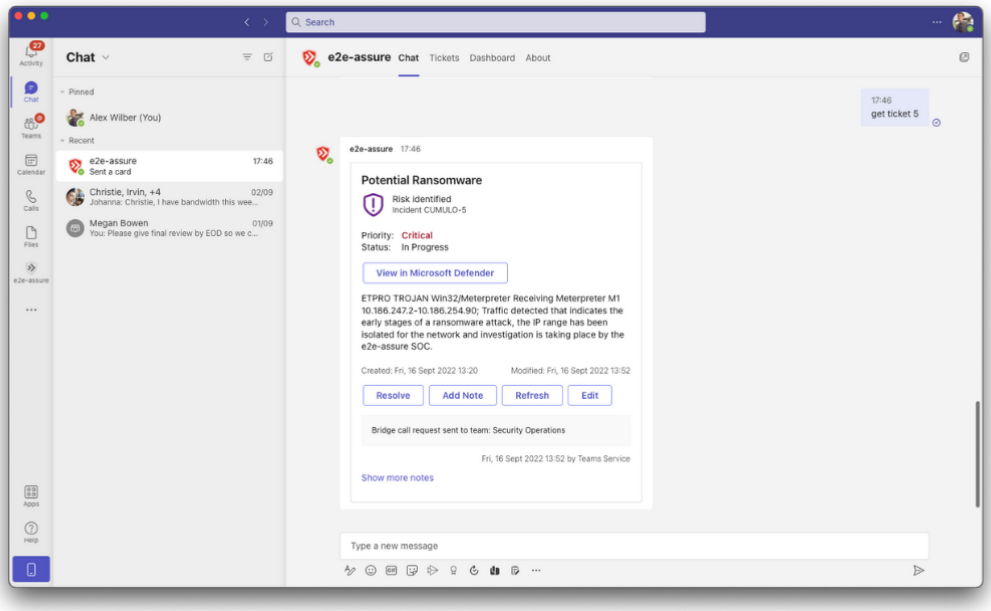
Where predefined and pre-agreed rules are met, Cumulo orchestrates automated containment, including user isolation and account suspension. Customers can also be notified through the integrated SOC App for Microsoft Teams, with the option to approve, cancel or collaborate on response actions in real time.

Behavioural trends, identity risk scoring, and policy deviations are continuously analysed by our SOC analysts leveraging integrated threat intelligence to proactively tune alert logic and improve detection quality. When combined with additional detection surfaces such as EDR, NDR or Security Log Analytics, the service forms a multi-layered defence that correlates identity compromise with endpoint or network-level attacker behaviour.

Posture dashboards, policy recommendations, and real-time alerts are delivered through Cumulo and the SOC Teams App, with monthly reporting to track improvement in identity hygiene, Secure Score, MFA compliance and risk exposure.




*SOC Teams App Dashboard*




*SOC Teams App Chat*

## Endpoint Detection and Response

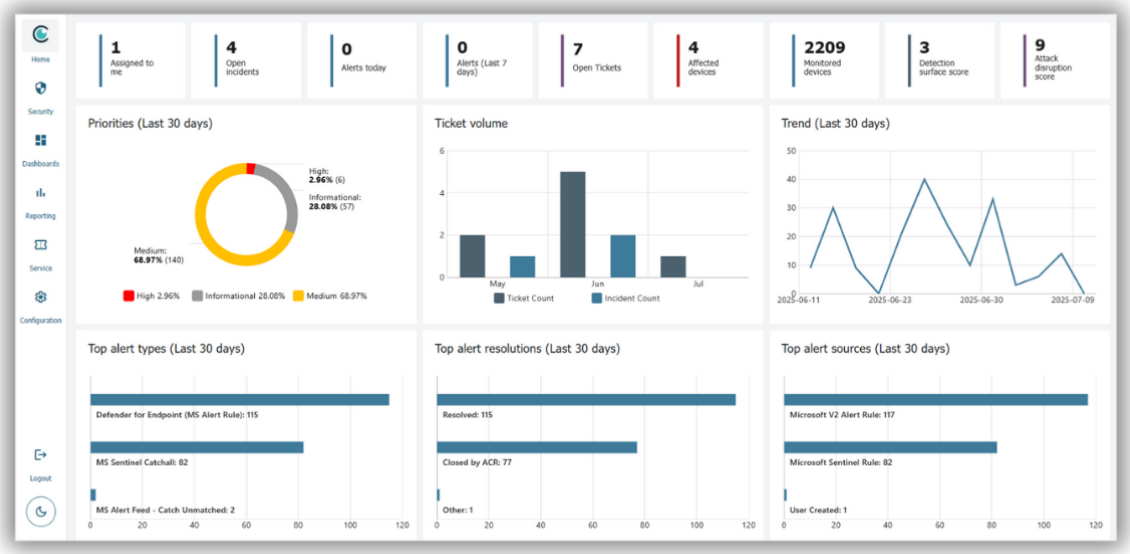
Endpoint Detection and Response delivers continuous monitoring and rapid containment of malicious activity on managed devices. The service integrates directly with the customer's chosen XDR technology and the Cumulo platform to deliver high-fidelity alerting, investigation, and endpoint level response.

Endpoint agents generate rich telemetry covering process activity, registry changes, network connections and behavioural patterns. During onboarding and throughout the service lifecycle, our analysts tune and optimise alert rules, baseline behavioural indicators and validate the configuration of deployed agents. This ensures that detections remain aligned to the latest threat intelligence and that noise levels are reduced while true positive accuracy improves over time.

Incidents may be triggered automatically by XDR analytics or escalated following analyst investigation. When a confirmed threat is identified, Cumulo coordinates a containment workflow appropriate to the customer's pre-agreed response model. This may include isolating an endpoint from the network, restricting application execution, removing or quarantining files, or initiating targeted scans. For more complex cases, orchestrated or analyst-led containment is initiated in collaboration with customer contacts.

Continuous telemetry analysis enables the service to detect early signs of attacker presence including lateral movement attempts, credential misuse, suspicious persistence mechanisms and ransomware precursors. Regular threat sweeps and trend analysis across endpoint data supports early discovery of stealthy or low volume attacks that may evade automated rules.

Quarterly validation exercises assess endpoint agent health, coverage, rule performance and containment workflows to ensure that the detection surface remains effective and aligned to the customer's environment and risk profile. Cumulo provides full case documentation including evidence, investigation steps and endpoint activity timelines, supported by regular service reporting that tracks posture improvements and key learning from recent incidents.




*Cumulo Dashboard*

## Cloud Threat Detection

Cloud Threat Detection provides continuous monitoring, analysis and response across cloud platforms to identify suspicious activity, configuration risk and attacker behaviours that may threaten workloads or data. The service integrates with native cloud security tooling such as Microsoft Defender for Cloud, AWS Security Hub, GuardDuty, and GCP Security Command CENTRE, and consolidates these signals into Cumulo for investigation and response.

During onboarding and throughout the contract, analysts tune and refine alerting policies, posture rules and analytics to ensure the service focuses on high-fidelity detections that align with the customer's environment. This includes validating baseline configuration, reviewing cloud resource deployments, and adjusting rules to reduce unnecessary noise while improving coverage of emerging threats.

The service monitors a wide range of cloud events including privilege escalation attempts, anomalous resource creation, access policy deviations, suspicious API usage, container runtime anomalies and storage access irregularities. Alerts are enriched with contextual data from cloud audit logs and posture assessments to accelerate investigation and decision-making.

When a confirmed threat is identified, Cumulo supports coordinated containment actions through the customer's cloud tooling. This may include account or role restriction, revocation of access keys, quarantine of affected workloads, removal of suspicious resources or enforcement of policy corrections. Actions may be automated where pre-agreed or executed collaboratively with customer contacts.

Continuous behavioural analysis and regular threat SWEEPS across cloud telemetry help identify stealthy techniques such as privilege drift, misconfiguration drift, dormant persistence and lateral movement through identity, network or automation constructs.

Quarterly validation exercises CAN assess the effectiveness of cloud security configurations, alerting rules, and available telemetry. This includes reviewing posture recommendations, validating agent and sensor coverage, and exercising containment workflows. Findings feed into a structured improvement plan that strengthens cloud resilience over time.

Cumulo provides full incident audit trails INCLUDED resource metadata, investigation notes and recommended remediations. Monthly reporting gives visibility into posture trends, emerging risks and opportunities to enhance cloud security configuration.

## Network Detection and Response

Network Detection and Response provides deep visibility into network traffic to identify attacker activity that may not be detectable through endpoint or log-based telemetry alone. The service uses a dedicated network appliance that captures and analyses traffic using tools such as Zeek and Snort, along with integrated threat intelligence, to surface indicators of compromise, lateral movement, command and control communication and suspicious protocol behaviour.

During onboarding, the appliance is tuned to the customer's environment by reviewing typical traffic patterns, key communication flows and known operational baselines. Analysts continuously refine analytic rules, signatures and behavioural thresholds to ensure the service focuses on meaningful signals while reducing unnecessary noise. This tuning is repeated throughout the contract to reflect changes in the customer's infrastructure, new applications or evolving attacker techniques.

Captured telemetry allows analysts to reconstruct events, review packet-level detail and identify anomalies across protocols and services. This is particularly effective in environments where endpoint agents cannot be deployed or where legacy systems generate limited logs. Asset discovery features also help maintain an accurate view of devices present on the network, which supports both incident investigation and posture improvement.

When suspicious activity is confirmed, Cumulo coordinates response actions based on the customer's predefined operating model. These actions may include generating containment signals for other detection surfaces, requesting network segmentation changes, issuing shun commands through integrated security devices or escalating directly to customer teams for urgent action. NDR can play a significant signalling role in broader attack disruption by enriching identity or endpoint alerts with network context.

Threat hunting across stored traffic and historical alerts can help to identify low volume or intermittent communication patterns, dormant persistence, lateral pivoting and protocol misuse. Quarterly validation exercises confirm the appliance is correctly positioned, that analytic signatures remain relevant and that detection coverage aligns to the customer's risk profile.

Cumulo provides complete case records containing network logs, reconstructed traffic, investigation notes and recommendations. Monthly reporting summarises detection trends, tuning outcomes, asset discovery changes and opportunities to enhance network security architecture.

## Security Log Analytics

Security Log Analytics provides a centralised and optimised approach to collecting, normalising and analysing logs from diverse on-premises, cloud and legacy environments. The service integrates customer log sources with either the Cumulo platform or a supported XDR or SIEM such as Microsoft Sentinel, enabling a consistent, high quality detection surface that supports accelerated triage and investigation.

During onboarding, log sources are assessed for availability, format, volume and relevance. Analysts work with customer teams to configure log forwarding, standardise formats, and remove unnecessary verbosity so that analytics are focused on high value security events. Tuning and optimisation continue throughout the service lifecycle as new systems are onboarded, infrastructure evolves or attacker techniques change.

The service applies alert rules, correlation logic and enrichment data to identify indicators of account misuse, privilege escalation, policy violations, network anomalies, error conditions, and attacker techniques that may not be visible through endpoint or cloud telemetry alone. In environments where endpoint agents cannot be deployed, logs often provide one of the only viable detection mechanisms, making completeness and tuning critical.

Log analytics also support investigations by providing historical context, event timelines and cross-domain evidence. Analysts construct queries to test hypotheses, identify lateral movement and correlate events between systems that would otherwise remain siloed. When deeper patterns suggest emerging risk, additional rules or custom analytics are created to reduce future detection time.

Where appropriate, log analysis can provide signals that support containment workflows in other service components. Examples include identifying network segments requiring isolation, highlighting devices requiring direct investigation or surfacing privileged activity that warrants identity controls.

Quarterly validation checks confirm that log sources are functioning, correctly formatted and providing the intended coverage. This includes verifying connectors, reviewing content relevance, refining analytics and confirming forwarding integrity. Findings feed into ongoing posture improvements and recommendations.

Cumulo provides detailed case records that include log evidence, correlation analysis, timeline reconstruction and suggested remediation steps. Monthly reporting provides customers with trends, optimisation outcomes, coverage insights and opportunities to enhance log-driven detection.

## OT SOC MONITORING

OT SOC Monitoring provides continuous visibility and threat detection across operational technology environments where legacy equipment, specialised protocols and strict availability requirements demand a tailored security approach. The service integrates OT-aware telemetry sensors with the Cumulo platform to identify abnormal behaviour, unauthorised activity and process-impacting events within industrial control systems.

The service supports two deployment models. The Sovereign Embedded option uses a pre-built onsite appliance containing the OT telemetry sensor, a local Cumulo instance, Security Log Analytics and Network Detection and Response capabilities. Appliances are sized according to site requirements and provide a consolidated OT security footprint where localised processing and resilience are important. The Sensor Relay option deploys only the OT telemetry sensor into the customer's virtual infrastructure and relays data to the central SOC platform. These approaches can be mixed across multi-site estates to match each location's scale, architecture and risk profile.

During onboarding, OT communication baselines are established by observing normal traffic patterns, device roles and process activity. Analysts tune detection logic to reflect approved engineering workflows, expected function codes and operational rhythms. As systems evolve or seasonal patterns shift, tuning is updated to maintain a high signal quality and reduce false positives.

The service monitors for events such as unexpected write attempts to controllers, unauthorised logic changes, configuration drift, anomalous protocol function codes, device impersonation, and the emergence of undocumented assets. Alerts are enriched with operational context and escalated through agreed pathways to the customer's OT Security Office or appropriate operational teams.

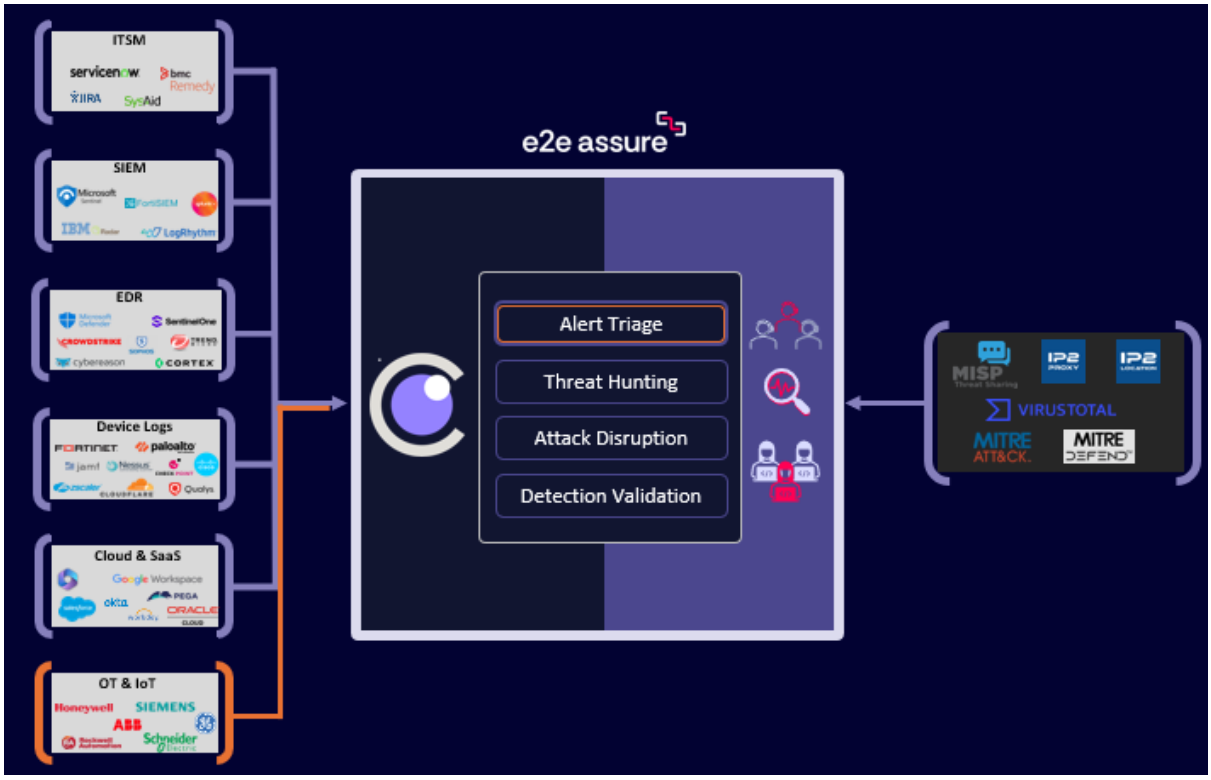
Correlation with IT telemetry highlights cross-domain activity including movement from business networks into control zones or attempts to access engineering workstations using compromised identities. Weekly threat hunting activities review lower-priority OT alerts and network patterns to identify reconnaissance behaviour or slow, intermittent anomalies that automated rules may not surface.

Quarterly validation checks confirm that sensors and appliances are positioned correctly, that detection rules remain relevant, and that baselines reflect the current OT estate. Validation also helps identify shadow assets, new protocol behaviour or architectural changes that require attention.

Cumulo provides case records containing traffic analysis, investigation notes, device context and recommended follow-up actions. Monthly service reporting summarises key alerts, tuning activities, posture changes and opportunities to enhance security across production environments.

Due the different approaches to handling confirmed true positives and incidents within operational technology environments, the service component has its own defined service targets as documented in the below table:

| Severity | Typical examples (OT) | Target MTTD | Target MTTN (notify customer OT Security Office) |
|---|---|---|---|
| **Sev 0 – Safety / Process-impacting critical** | Unauthorized PLC logic change; unsafe set-point write; ransomware on HMI/engineering station in control zone | **30 min** | **60 min** |
| **Sev 1 – High** | Confirmed intrusion in OT network, abnormal OT protocol function codes (e.g., Modbus write outside baseline), unauthorized remote access into ICS DMZ | **60 min** | **120 min** |
| **Sev 2 – Medium** | Lateral movement indicators in ICS DMZ, policy violations, suspicious but not clearly malicious command sequences | **4 hours** | **8 hours (same day)** |
| **Sev 3 – Low** | New/unknown device seen, minor config drift, low-confidence anomalies | **1 business day** | **1 business day (digest or ticket)** |
| **Informational** | Baseline changes, inventory deltas, non-actionable intel matches | **Batch (daily/weekly)** | **Weekly or monthly digest** |




*OT/IT connectivity with Cumulo*

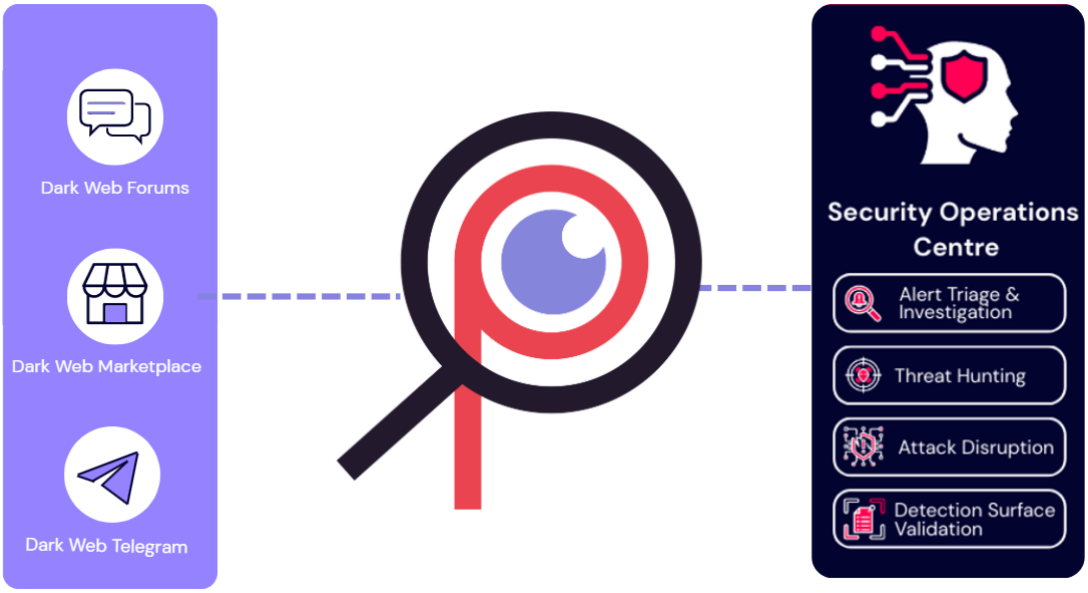
## PRECON DARK WEB MONITORING

PRECON Dark Web Monitoring provides early warning of potential threats by continuously analysing sources of cybercriminal activity, including dark web marketplaces, underground forums, stealer malware logs, leaked credential dumps and attacker coordination channels. The service identifies exposed credentials, data leaks, perimeter weaknesses and indications that a customer is being profiled or targeted by threat actors. Intelligence is processed and investigated within Cumulo to support decisions on proactive security measures.

The service begins by establishing a monitoring profile that captures customer attributes such as domains, email patterns, IP ranges, cloud storage identifiers and keywords associated with the organisation. These attributes are used to configure automated searches across multiple intelligence platforms. Profiles are reviewed and tuned throughout the contract as the customer's infrastructure or threat landscape evolves.

Alerts surface findings such as compromised credentials, leaked datasets, evidence of stealer malware infection, suspicious domain registrations, attack planning indicators, and vulnerabilities identified by third parties. Analysts validate and contextualise these discoveries and enrich them with information drawn from available telemetry and threat intelligence. When appropriate, PRECON findings are correlated with other detection surfaces to identify account misuse, device compromise or potential footholds inside the customer's environment.

Because PRECON provides early detection rather than incident containment, emphasis is placed on actionable guidance and proactive measures. Recommendations may include resetting affected credentials, enabling or strengthening MFA, tightening exposure of cloud repositories, revoking access keys, patching externally facing systems or hardening perimeter controls. Where the customer has enabled relevant automated response capabilities through other services, PRECON alerts can be used to initiate containment workflows or identity protections.



## EXTERNAL PERIMETER MONITORING

External Perimeter Monitoring provides continuous visibility of an organisation's internet-facing assets to identify vulnerabilities, misconfigurations and exposure points that threat actors could exploit. The service combines daily attack surface scanning with weekly vulnerability assessments and passive intelligence feeds to surface external risks before they lead to compromise. Findings are investigated and validated within Cumulo, with recommendations provided to help reduce or eliminate exposure.

During onboarding, the service establishes a baseline of known public assets, including domains, IP ranges, services and externally reachable systems. This baseline is refined over time as new assets are deployed, retired or modified. Analysts tune scanning scopes and detection rules to reflect the customer's infrastructure, ensuring that monitoring remains accurate while minimising irrelevant or duplicative alerts.

The service reviews scan outputs for misconfigurations such as exposed services, open ports, outdated software versions and unintended changes to internet-facing systems. Vulnerability assessments identify weaknesses that carry known exploitability characteristics, while passive intelligence sources such as Shodan, ShadowServer and sector-specific intelligence provide early warning of emerging threats or changes in the customer's external footprint.

Validated findings are triaged in Cumulo and enriched with contextual information to support clear prioritisation. Examples include identifying a newly exposed management interface, detecting a critical vulnerability on a firewall version in active exploitation, or discovering an unfamiliar external asset communicating with the environment. Analysts provide guidance on mitigation actions and, where appropriate, correlate findings with other detection surfaces to check for related internal activity.

Regular tuning ensures that the baseline of known assets remains accurate and that detection logic reflects customer architecture changes. Monthly reporting provides a consolidated view of external exposures, recurring trends and opportunities to strengthen perimeter resilience. This helps customers maintain a clear understanding of their internet-facing risk profile and supports proactive security improvement.

*Example of the scanning tools and the SOC is depicted below:*

