Modern AI SOC Services

AMICIS GROUP

Introduction

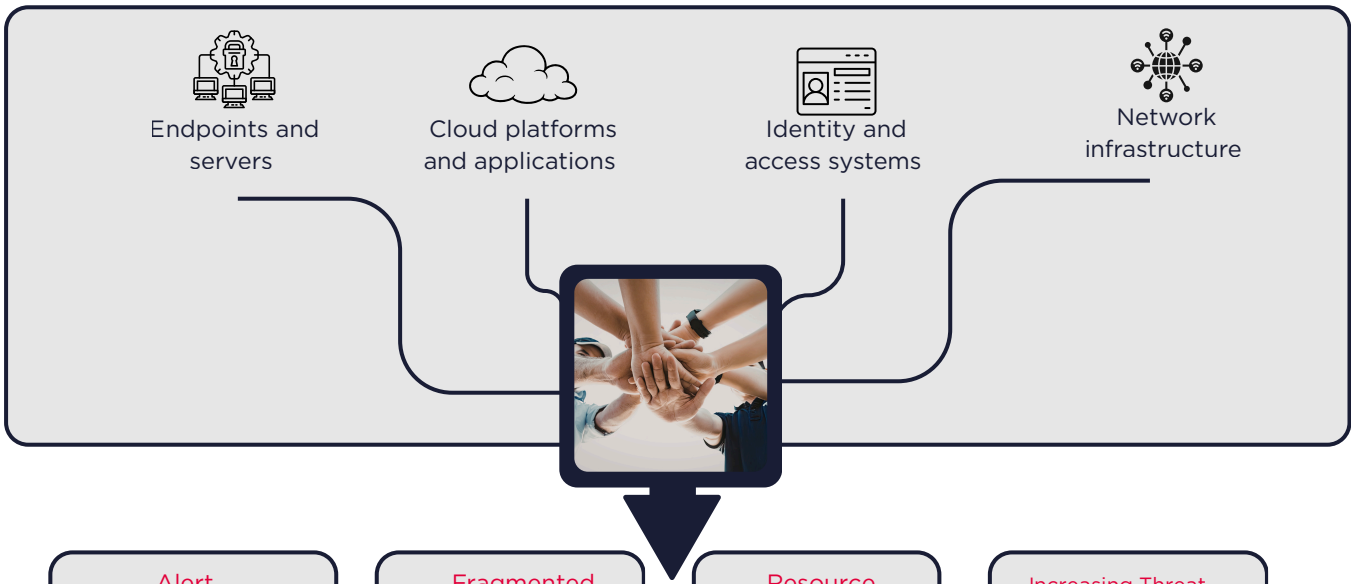
Security operations have become more complex, not just more important.

As organisations adopt cloud platforms, remote working and identity driven access, the volume of security data has increased significantly. At the same time, attackers are moving faster and operating across multiple parts of the environment.

For mid-market organisations, the challenge is clear. You need strong detection and response capability, but building and running an internal Security Operations Centre is rarely practical. Modern SOC services provide a more effective and achievable approach.

The Reality of Modern Security Operations

Security teams are expected to monitor activity across:



Alert Overload

Security tools generate vast volumes of alerts, many without sufficient context. In many environments, a significant proportion of alerts are false positives, while others are never fully investigated.

Fragmented Visibility

Different tools operate in isolation, limiting the ability to track threats as they move across identity, endpoint and cloud environments.

Resource Pressure

Internal teams are stretched, often balancing IT operations with security responsibilities, making consistent monitoring and response difficult.

Increasing Threat Sophistication

Modern Threat Actors rarely target one system. They're adapting quickly and moving laterally across identity, endpoint, network and cloud environments, making it difficult to identify without strong detection and threat intelligence.

The Hidden Challenge: Investigation at Scale

Most organisations have invested in detection. The real challenge is what happens next.

Security tools are effective at identifying potential threats, but investigation remains largely manual. This creates a bottleneck where large volumes of alerts must be validated, enriched and assessed before action can be taken.

As alert volumes increase, this gap between detection and response becomes more pronounced. The result is:

- Delayed response times
- Increased risk of missed threats
- Analyst fatigue and inefficiency

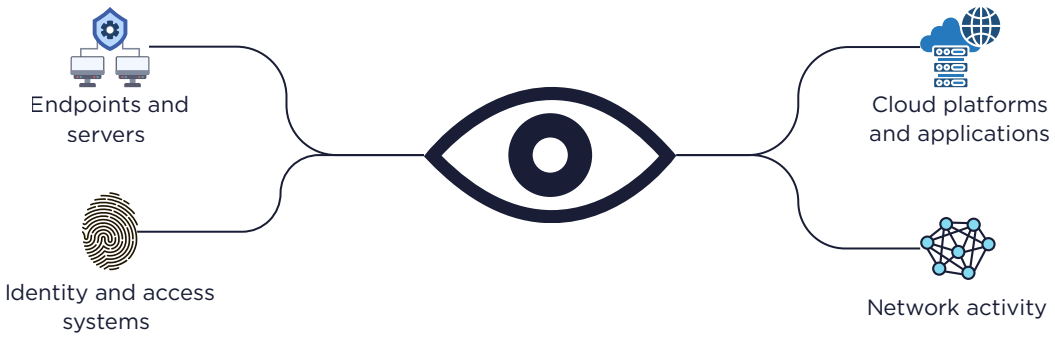
Modern SOC services address this challenge directly by improving how alerts are investigated, prioritised and acted upon.

Why Traditional Approaches Fall Short

This creates a gap between visibility and action. Data is collected but not always translated into effective response.

Detection Across the Modern Environment

Effective threat detection today relies on visibility across multiple parts of the environment, not just a single system. Modern SOC services bring together telemetry from:



Technologies such as Endpoint Detection and Response and Extended Detection and Response support this by providing deeper visibility and helping correlate activity across these areas. This allows security teams to identify threats that move across systems, rather than viewing events in isolation.

Within a modern SOC, these capabilities are combined with intelligent investigation and analyst oversight to ensure that alerts are prioritised correctly and translated into effective action.

The Role of AI in Security Operations

AI is increasingly used to support the investigation and triage of security alerts. It enables:

- Faster enrichment of alerts with relevant context
- Identification of patterns across large data sets
- Reduction in manual investigation effort
- More consistent analysis across large volumes of alerts

In many environments, this allows organisations to significantly reduce the volume of alerts that require manual review, enabling teams to focus on genuine threats.
However, AI is most effective when combined with human expertise. A balanced approach ensures efficiency improves without losing control or clarity in decision making.

Creating a Unified Security View

One of the most important capabilities of a SOC is the ability to bring multiple data sources together into a single, coherent view. Without this, threats can remain hidden as they move between systems.

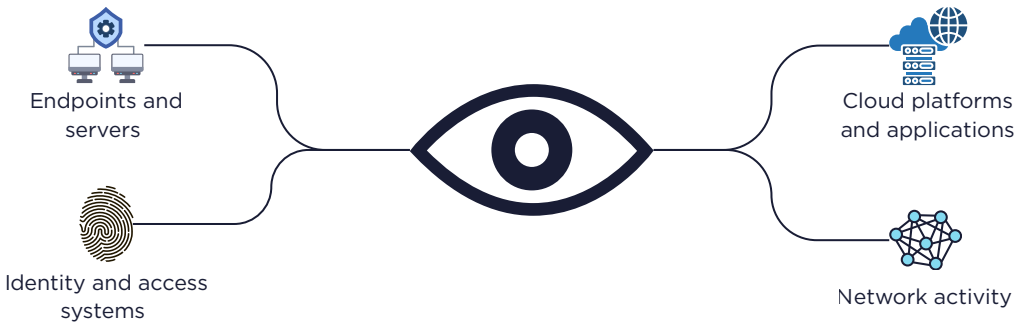
A modern SOC provides:

- Centralised visibility
- Correlated activity across environments
- Clear prioritisation of risk
- Actionable insight for response

This unified view is essential for identifying complex, multi-stage attacks and responding effectively.

Detection Across the Modern Environment

Effective threat detection today relies on visibility across multiple parts of the environment, not just a single system. Modern SOC services bring together telemetry from:



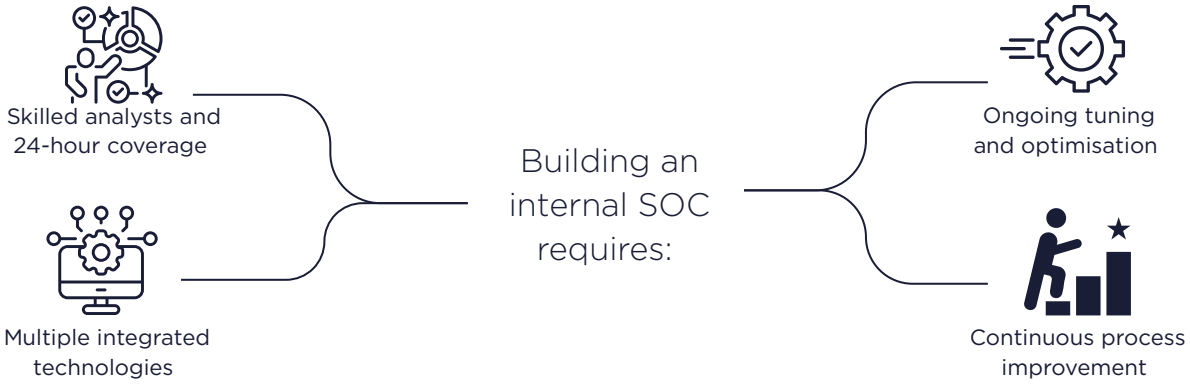
Technologies such as Endpoint Detection and Response and Extended Detection and Response support this by providing deeper visibility and helping correlate activity across these areas. This allows security teams to identify threats that move across systems, rather than viewing events in isolation.

Within a modern SOC, these capabilities are combined with intelligent investigation and analyst oversight to ensure that alerts are prioritised correctly and translated into effective action.

SOC and MDR: Understanding the Difference

MDR focus primary on endpoints. A SOC provides a broader security operations capability combining detections, investigation and incident response across endpoint, identity, cloud and network environments. MDR is an effective starting point, however as environments grow more complex, a SOC becomes an increasingly important to identify advanced and coordinated threats.

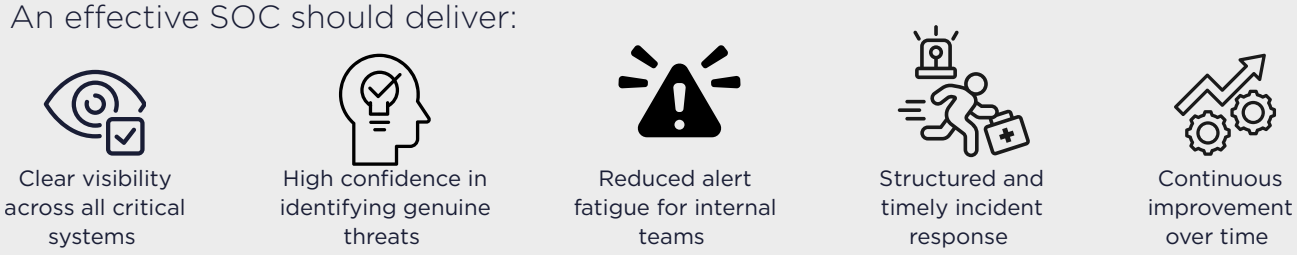
The Operational and Financial Reality



It also requires the ability to handle large volumes of alerts efficiently, something that is increasingly difficult without automation and specialist tooling.
For mid-market organisations, this creates both cost and complexity. A managed SOC provides an alternative that delivers capability without the same operational burden.

What Good Looks Like

An effective SOC should deliver:



It should reduce complexity, not add to it.

Why Organisations Choose Managed SOC

Organisations adopt managed SOC services to:

Increasingly, they are also looking for solutions that can scale with growing data volumes without increasing internal workload.

Why Amicis Group

Amicis Group delivers modern SOC services designed specifically for mid-market organisations. We combine experienced analysts with leading technologies across endpoint, identity, cloud and network environments to provide a unified and effective security capability.

The Operational and Financial Reality

We incorporate advanced detection and AI assisted investigation where appropriate, helping reduce noise, improve prioritisation and accelerate response.
Most importantly, we bring clarity and confidence to an area that is often complex.

We deliver peace of mind in a digital world.

Amicis Group provides a modern engineering-led SOC service built for mid-market organisations. We combine experienced security professionals with leading technologies across endpoint, identity, cloud and network environments to deliver a unified and effective security capability.

Our approach is:

We use AI and automation to support alert triage, enrichment and investigation, while keeping human judgement and incident response at the centre of the service.
For our customers, this means access to a mature security operation that is easier to adopt, easier to scale and focused on real operational needs.