



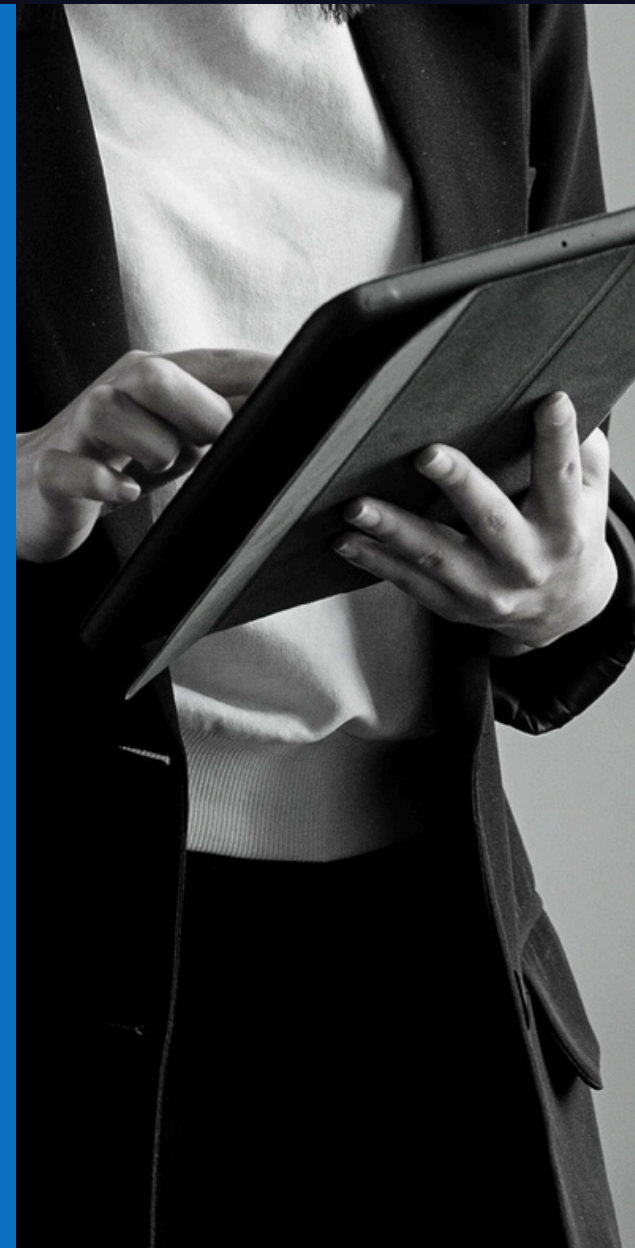
Modernize your SOC with Microsoft Sentinel Whitepaper

Date
June 2025

Created by
Black Cell SOC
Black Cell Cloud Security¹

Content

- About Black Cell SOC
- Introduction
- Solution
- Challenges
- Roadmap
- Benefits
- Success in Action



About Black Cell SOC

Since 2010, Black Cell’s Security Operations Center (SOC) has delivered expert-driven, around-the-clock cybersecurity services designed to protect and strengthen our customers’ digital infrastructure. Acting as an extension of internal teams, our SOC integrates seamlessly with each customer’s IT environment to monitor, detect, analyze, and respond to threats in real time.

By collecting and correlating telemetry from the entire monitored infrastructure, the SOC provides centralized visibility and rapid threat response. Our services include advanced threat hunting, vulnerability management, phishing investigation, and end-to-end incident handling, all executed by experienced cybersecurity professionals.

With a focus on both proactive and reactive defense, Black Cell SOC enhances our customers’ security posture through continuous monitoring, detailed reporting, and actionable remediation guidance. Transparent communication and close collaboration ensure that organizations remain agile, informed, and resilient in the face of evolving cyber threats.



105.000+

Security Alert
Triage



3.000+

Incidents
Investigated



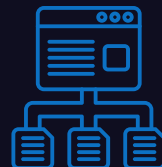
130+

Mass Phishing
Cases Handled



7

APT Cases
Managed



150+

New DaC Use
Cases



~35%

SOC Customer
Growth

Our Achievements & Skills

Explore our SOC team



Specialist
Identity and Access
Management
Information Protection and
Governance
Threat Protection

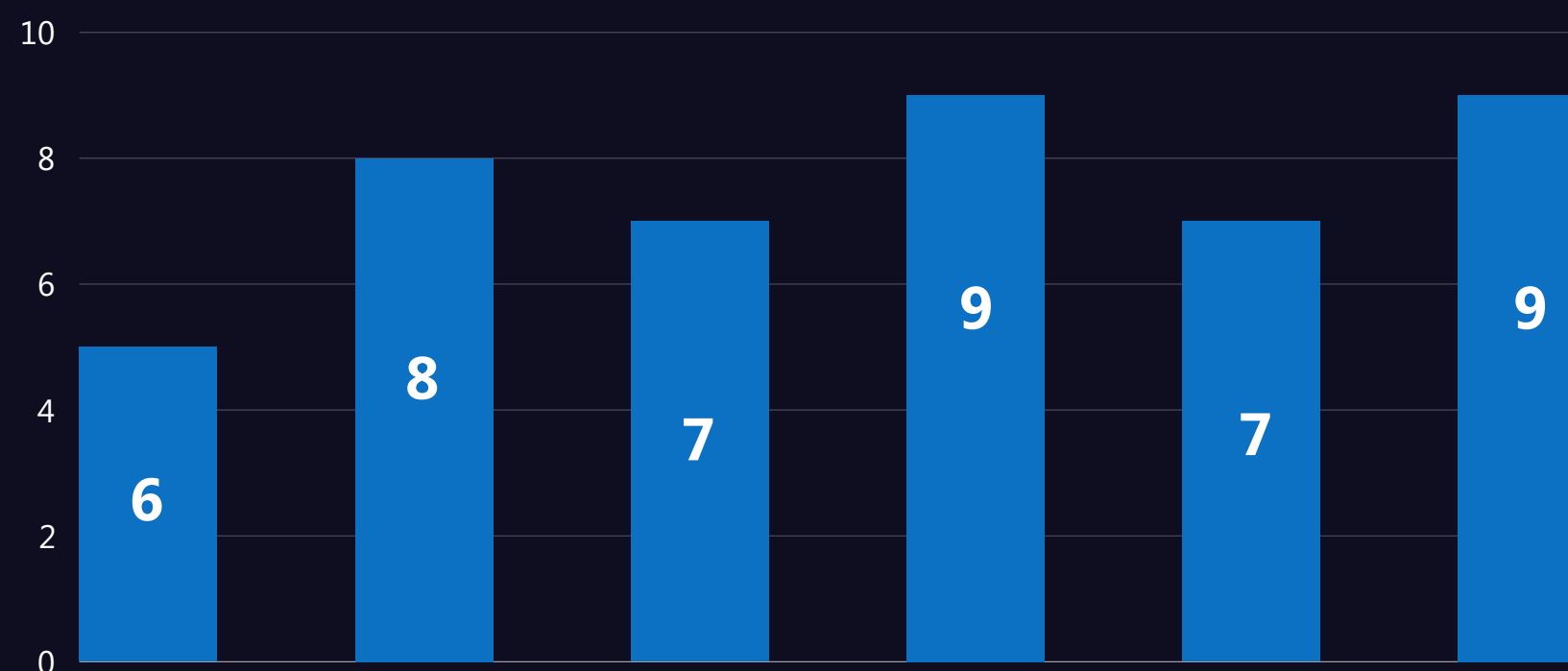


Member of
Microsoft Intelligent
Security Association


Black Cell has earned the Solutions Partner designation in the Security solution area, as well as the Identity & Access Management, Threat Protection and Information Protection and Governance Specialization. These certifications demonstrate the breadth of Black Cell's capabilities in delivering customer success based on Microsoft cloud security technologies.

23+ SOC employees

● FTE



Tech Stack

The tools behind the build

DEFENDER XDR

Advanced threat detection for enterprises. Can be used as an alternative "SIEM" for a "mini-SOC".

LIGHTHOUSE

Used for cross tenant permission management.

TEAMS

Used for internal alert notifications and inter-org war rooms.



SPLUNK

Used as our centralized SOAR system for 24/7 monitoring.

TWILIO

Used for alerting analysts outside of working hours.

JIRA

Used as a ticketing system to interface with our customers.

Core Services & Supported SIEM Systems

Built-in capabilities and trusted integrations



24/7/365
Security Monitoring



Advanced
Threat Hunting



Phishing
I&R



Splunk Enterprise &
Cloud



Microsoft
Sentinel



Elastic

Black Cell's Certificates



NATO AQAP 2110:2016
Quality Management
System



ISO/IEC 27001:2022
Information Security
Management System



ISO 9001:2015
Quality Management
System



Family-friendly
workplace



OUR EMPLOYEES' VENDOR-SPECIFIC CERTIFICATIONS

Microsoft | Palo Alto Networks | Sophos | IBM |
Splunk | Rapid7 | OPSWAT | Snyk



OUR EMPLOYEES' INDEPENDENT CERTIFICATIONS

CISSP | CISA | CISM | CEH | OSCP | OSED | PMP |
ISO/IEC 27001:2022 Certified Lead Auditor | ISO
9001:2015 Certified Lead Auditor | ITIL 4
Foundation, Managing Professional

Executive summary

In an era defined by rapid digital transformation and increasingly sophisticated cyber threats, organizations face daunting challenges in achieving comprehensive security oversight. Disparate security tools, overwhelming alert volumes, and evolving attack vectors all conspire to create risks that are difficult to mitigate without a unified strategy. Black Cell's managed security services based on Microsoft Sentinel are designed to address these challenges through an integrated solution that leverages the cloud-native SIEM and SOAR capabilities of Microsoft Sentinel with Defender XDR and Defender for Cloud. This service suit empowers Security Operations Centers (SOCs) with timely insights, automated responses, and proactive threat hunting capabilities that are crucial for modern enterprises.



Enterprises today operate in a complex, hybrid digital ecosystem that includes on-premises infrastructures, cloud workloads, endpoints, and increasingly, Internet of Things (IoT) devices. This digital expansion necessitates a security framework that not only unifies disparate data streams but also correlates and analyzes them in real time. Microsoft Sentinel is at the heart of our solution, functioning as the central hub for data aggregation, threat detection, and incident response. By effectively integrating Defender XDR – which provides extended detection and response across endpoints, identities, and applications – and Defender for Cloud, which focuses on workload protection and cloud security posture management, we deliver an end-to-end security solution. This document outlines how our service integrates these technologies, addresses the prevalent challenges, and augments SOC capabilities, ultimately reducing risk and ensuring operational continuity.

Microsoft Sentinel

The Centralized Security Hub

ABOUT MICROSOFT SENTINEL

Microsoft Sentinel is a cloud-native SIEM and SOAR platform that revolutionizes security operations. It ingests telemetry data from various sources, including network devices, endpoints, applications, and cloud services, and employs advanced machine learning and analytics to detect anomalies and emerging threats. Sentinel's ability to correlate a vast array of log data into actionable insights transforms how SOC's prioritize incidents and deploy resources.

LEVERAGING DEFENDER XDR

Defender XDR (Extended Detection and Response) enhances Sentinel by providing deep threat visibility and protection across a myriad of endpoints and identity systems.

Here's how Defender XDR integrates with Sentinel:

- **Unified Telemetry Aggregation:** Defender XDR feeds critical endpoint and identity signals directly into Sentinel. This ensures that every event—whether an unusual process execution, anomalous network traffic, or suspicious authentication attempt—is recorded and correlated with other security data.
- **Automated Threat Correlation:** When Defender XDR detects a potential threat, Sentinel's advanced analytics automatically correlate the event with data from other sources. For instance, if an endpoint anomaly is detected alongside unusual identity behavior, Sentinel's intelligent playbooks can automatically elevate the incident's priority.
- **Enhanced Incident Response:** The integration empowers SOC analysts to access a holistic view of the security landscape from a single pane of glass. Enhanced dashboards, real-time alerts, and enriched threat context facilitate faster decision-making and streamlined remediation workflows.

Together, Microsoft Sentinel and Defender XDR create an environment where deep visibility is paired with automation, reducing the time to detect and respond to threats while easing the burden on overextended security teams.

Defender for Cloud

Securing the Cloud Ecosystem

As businesses increasingly move workloads to the cloud, ensuring that these environments are secure becomes paramount. Defender for Cloud is Microsoft's solution for continuous security posture management and threat protection across cloud workloads, including virtual machines, containers, databases, and serverless functions. It enforces best practices, provides insightful security recommendations, and automatically detects vulnerabilities in cloud configurations.

INTEGRATING DEFENDER FOR CLOUD WITH MICROSOFT SENTINEL

The seamless integration between Defender for Cloud and Microsoft Sentinel enhances the overall security posture by:

- **Automated Posture Assessments:** Defender for Cloud continuously assesses the configuration and security posture of cloud resources. It feeds these assessments into Sentinel, allowing SOCs to track compliance and react promptly to deviations.
- **Centralized Alert Management:** Alerts generated by Defender for Cloud—whether due to misconfigurations, suspicious cloud activity, or compliance violations—are automatically ingested by Sentinel. This centralized view helps SOC analysts manage and prioritize incidents more effectively.
- **Cross-Domain Correlation:** By correlating cloud security events with Sentinel's logs from on-premises systems and Defender XDR's endpoint data, macro-level threat patterns become visible. For example, an attempted breach in a cloud service can be linked with lateral movement detected on an endpoint, triggering an automated containment workflow.
- **Proactive Remediation:** Integrated remediation playbooks allow for automated responses across the cloud and endpoint environments. Actions such as isolating compromised resources, revoking suspicious credentials, and applying patches can be triggered automatically, ensuring a rapid and coordinated response.

The integration of Defender for Cloud with Microsoft Sentinel delivers a unified security framework that covers every aspect of an organization's digital footprint—from on-premises and remote endpoints to cloud workloads—empowering SOC teams with the granular visibility necessary to maintain a robust defensive posture.

Addressing Challenges in the Modern SOC

Modern SOC's face unprecedented challenges: an ever-expanding attack surface, false-positive-generated alert fatigue, siloed data sources, and a skill shortage that hampers prompt incident response. Traditional security tools often fail to provide a holistic view, leaving gaps that threat actors can exploit. The fundamental challenge lies in correlating signals from heterogeneous sources in a timely manner to detect sophisticated threats.

HOW MICROSOFT TECHNOLOGY OVERCOMES THESE CHALLENGES

Microsoft's security ecosystem—built around Sentinel, Defender XDR, and Defender for Cloud—addresses these challenges through:

- **Unified Data Aggregation:** By consolidating logs and telemetry from various environments into Sentinel, organizations overcome the issue of data silos. The result is a comprehensive security view where critical events are not lost in translation.
- **AI-Driven Alert Correlation:** Microsoft Sentinel's machine learning algorithms identify patterns and anomalies across vast amounts of data. This automated correlation significantly reduces false positives and alerts SOC teams only when there is clear threat evidence.
- **Automated Diversion and Remediation:** Preconfigured playbooks and automated workflows ensure that, once a threat is detected, the system responds immediately with actions such as quarantining endpoints, revoking privileges, or triggering additional forensic investigations. This automation is vital in scenarios where every minute matters.
- **Optimized SOC Workflows:** The integration streamlines routine tasks, enabling SOC analysts to shift focus from manual triaging to strategic threat hunting. Enhanced dashboards and interactive reports facilitate deep investigations, ensuring that the SOC remains agile and well-informed.
- **Scalability and Flexibility:** Microsoft's cloud-native solutions are designed to scale seamlessly with organizational needs. Whether managing traditional infrastructures, cloud workloads, or hybrid environments, the integrated platform grows with demand—without compromising on performance or security.

Through this holistic approach, Microsoft's technology not only mitigates the inherent challenges of modern security operations but also sets the foundation for enhanced operational efficiency, improved threat intelligence, and a resilient security posture across the enterprise.

Implementation Roadmap

SOC Services

Black Cell implementation service is structured to ensure a smooth transition from legacy security frameworks to a unified, automated security environment. The key phases include:

1. ASSESSMENT AND PLANNING

- **Initial Assessment:** We conduct a comprehensive review of your current security posture, data flows, and compliance requirements.
- **Stakeholder Engagement:** Working with IT and security leaders, we identify critical assets and define security objectives aligned with business goals.
- **Roadmap Development:** A detailed implementation roadmap is crafted, including resource allocation, timelines, and milestone tracking.



2. DESIGN AND ARCHITECTURE

- **Integration Blueprint:** We design an architecture that leverages Sentinel as the central aggregator, seamlessly integrating data from Defender XDR and Defender for Cloud.
- **Custom Data Connectors:** Tailor-made connectors are developed to ensure that telemetry from all sources is ingested efficiently.
- **Automation Workflows:** Incident response playbooks are customized to automate repetitive tasks and streamline SOC operations.

4. TRAINING AND TRANSITION

- **SOC Training:** Comprehensive training sessions are provided to your security team, empowering them to leverage the enhanced features of the integrated platform effectively.
- **Knowledge Transfer:** Detailed documentation and hands-on support ensure a smooth handover and continued operational success.

3. DEPLOYMENT AND INTEGRATION

- **Platform Deployment:** Microsoft Sentinel is deployed as a cloud-native service, with all critical data points integrated from endpoints, cloud services, and identity platforms.
- **Defender Integration:** We integrate Defender XDR and Defender for Cloud, ensuring that alerts, insights, and recommendations flow into Sentinel's centralized console.
- **Testing and Calibration:** Rigorous testing—including simulated threat scenarios—is conducted to calibrate detection rules, validate automated workflows, and ensure system robustness.

5. CONTINUOUS SUPPORT AND OPTIMIZATION

- **24/7 Monitoring:** Ongoing managed services ensure that your security environment is continuously monitored, with regular health checks and performance tuning.
- **Incident Response Support:** Our team remains on standby to assist with critical incident investigations and remediation efforts.
- **Regular Updates:** The solution is continuously refined based on evolving threat intelligence and emerging compliance requirements.

Business Benefits and SOC Impact

FROM A SOC PERSPECTIVE, OUR SOLUTION OFFERS PROFOUND BENEFITS



Reduced Alert Fatigue: Automated correlation and enriched analytics significantly reduce noise, allowing analysts to focus on high-risk incidents.



Faster Response Times: Automated workflows and rapid threat containment reduce Mean Time To Response (MTTR), minimizing the potential damage from breaches.



Comprehensive Visibility: A unified security view across endpoints, cloud infrastructures, and identity systems ensures that no threat goes unnoticed.



Operational Efficiency: Streamlined processes and automated playbooks free up valuable human resources, enabling your SOC to operate more strategically.



Enhanced Compliance and Reporting: Real-time security posture monitoring and automated compliance checks simplify audit processes and ensure adherence to regulatory frameworks.



Customer Success Story

Freeway Entertainment's Path to ISO/IEC 27001:2022 Certification

CLIENT

Freeway Entertainment is a global leader in film and entertainment services, specializing in rights management, content localization, and distribution support. Operating across international markets, the company relies on a hybrid IT environment combining on-premises systems and Microsoft 365 cloud services. With increasing cybersecurity challenges in the media industry, Freeway Entertainment committed to achieving ISO/IEC 27001:2022 certification as part of a strategic security overhaul. This initiative reinforced their dedication to protecting client assets and ensuring operational resilience.



CHALLENGES

- Achieve ISO/IEC 27001:2022 certification through a meaningful security transformation, not superficial compliance.
- Lack of centralized visibility across a hybrid infrastructure combining on-premises systems and Microsoft 365 services.
- Inadequate endpoint, identity, and cloud activity monitoring for modern cyberattack defense.
- Custom-developed on-prem application lacked logging, creating operational blind spots.
- Need for advanced detection without alert fatigue or heavy operational overhead.

Customer Success Story

Freeway Entertainment's Path to ISO/IEC 27001:2022 Certification



SOLUTIONS

- Deployed Microsoft Sentinel for centralized, cloud-native security monitoring.
- Rolled out Microsoft Defender for Endpoint (MDE) with hardened configurations and centralized policy management.
- Enhanced the custom application's logging for Sentinel integration.
- Implemented UEBA, Logic Apps for incident response, and fine-tuned analytic rules.
- Onboarded servers with Azure Arc and optimized log ingestion to reduce noise and costs.
- Deployed Content Hub solution packs and Black Cell's proprietary detection rules.



KEY RESULTS

- Achieved unified visibility across endpoints, servers, and applications.
- Detected multiple true positives shortly after go-live.
- High detection accuracy and reduced alert noise.
- Streamlined operations through automation and integrated incident response.
- Delivered a scalable, future-ready security framework supporting ISO 27001 certification.



KEY SERVICES

- Security architecture design and implementation aligned with ISO 27001.
- SIEM and endpoint security deployment and customization.
- Development of custom detection rules, log parsers, and automation workflows.
- Integration with ticketing systems and operational process improvements.
- Delivery of comprehensive documentation and knowledge transfer.

Key Benefits

Collect and analyse data

-  Eliminate infrastructure set up and maintenance with a cloud-native SIEM
-  Flexible data ingestion and storage options
-  350+ out-of-the-box connectors
-  Single-click use case discovery and deployment

Detect evolving threats

-  Alerts automatically correlated into prioritised incidents
-  Full visibility of an attack path, even across multiple sources
-  Built-in UEBA to automatically detect anomalies
-  Automatic enrichment with Threat Intelligence backed by Microsoft Threat research

Get 24/7 EU-based monitoring

-  Round-the-clock protection backed by Microsoft Sentinel
-  Alerts and incident response within 30 minutes
-  300+ pre-built connectors and custom detection rules
-  ISO 27001-certified processes and comprehensive audit trails

Investigate incidents with full context

-  Security Copilot embedded into the experience
-  Built-in machine learning for incident correlation, SOC optimisations, automatic attack disruption, and more
-  Visual investigations of the full scope of incidents
-  Unified data model across Defender XDR and Defender for Cloud for comprehensive incident creation, and 50% faster responses

Respond across all your tools

-  Built-in security orchestration, automation, and response (SOAR)
-  Customisable automations for rapid response via logic apps
-  200+ Microsoft created solutions and 280+ community contributions

Contact

Let's Get Work Together

Get in touch with us today!
Our team of experts is ready to assist you



Szabolcs
Németh

+36 70 415 33 43

szabolcs.nemeth@blackcell.io

www.blackcell.io

Béla
Droppa

+36 70 417 62 90

bela.droppa@blackcell.io

www.blackcell.io

Márk
Fülöp

+36 70 432 13 86

mark.fulop@blackcell.io

www.blackcell.io