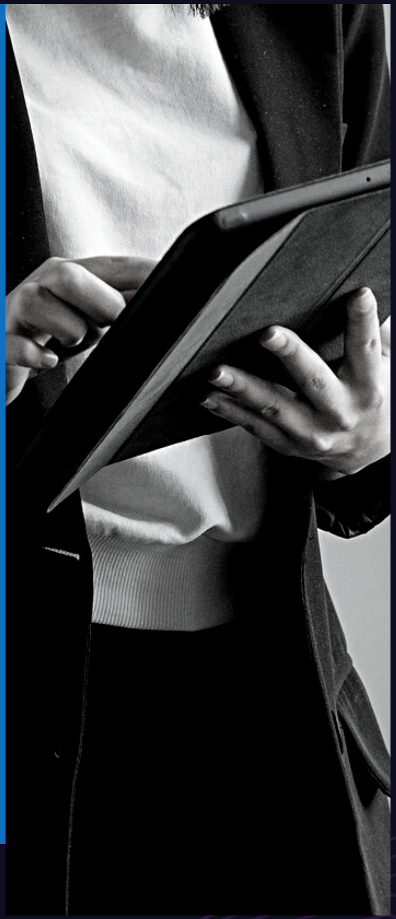
Microsoft **Security Services**

Created by
Black Cell Magyarország Ltd.

Content

- Introduction
- Solution
- Managed Security Services
- On-Demand Security Services
- Contact



Who **We Are ?**

Black Cell is a professional cybersecurity company providing end-to-end cybersecurity assurance within its Fusion Center, Integration, Offensive Security and Compliance solution areas, as well Cloud Security and ICS/OT Security specializations.

Black Cell is a pioneer in its niche market, provisioning high quality services to every single client, regardless of the size of the business or the size of the individual deal. We act fast, are dedicated to solve complex problems and work flexibly to meet the most rigorous expectations.

2010
Company was founded

005
Offices around the world

40
Employees

100+
Happy clients

Our Mission

Our goal is not only advising to the best of our knowledge, **but creating bespoke & resilient cybersecurity ecosystems.**

The goal of our leadership team is to provide clear direction, foster collaboration and innovation in order to help our clients' organization towards sustained growth and success.

Solution

Managed
Detection & Response

Black Cell's Managed Detection and Response [MDR] is a cybersecurity service that provides organizations with a team of Microsoft Security experts who monitor your Microsoft Extended Detection and Response [XDR] solutions and respond to cyberthreats 24/7 or 8/5. Black Cell leverages its expertise, processes, and Microsoft security technology to reduce risk, stop attacks and improve the effectiveness of your security operations. MDR is focusing on both reactive and proactive activities, such as advanced threat hunting and vulnerability management backed by exploit probability [EPSS] that are done real time by Black Cell's Microsoft experts. MDR provides alert and IoC triage, and includes investigation, response, detailed vulnerability reporting and remediation with recommendations.

Solution **Values**

- Increased security maturity
- Faster time to value for your security investment.
- Reduced MTTD [mean time to detect] and MTTR [mean time to respond]
- Resource augmentation with 24/7 or 8/5
- Guided response and managed remediation
- Proactive defense

Increased Security Maturity

Rapid ROI

Reduced MTTD & MTTR

Resource Augmentation

Response & Remediation

Proactive Defense

Managed Security Services on Microsoft 365 Defender

Security monitoring

Creates less chance of a successful attack and provides the ability to better understand attack techniques and respond appropriately.

Vulnerability management

Delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.

Advanced Threat Hunting

Has powerful hunting search and query tools to hunt for security threats across the organisation’s data sources.

Phishing Investigation

Provides insights into threats and related response actions that are available in the Microsoft 365 Defender portal.

Learn more about the key features and benefits of each service.

Security Monitoring

MDR Security monitoring is a fully managed security monitoring powered by Microsoft 365 Defender suite that creates less chance of a successful attack and provides the ability to better understand attack techniques and respond appropriately. Black Cell's Microsoft security and compliance experts coordinate detection, prevention, investigation, and response across endpoint, identities, email, and applications by leveraging Microsoft 365 Defender solutions to provide integrated protection against sophisticated attacks.

Key features & benefits

- Extended security monitoring via Microsoft Defender suites
- 24/7 or 8/5 service managed by certified Microsoft professionals working from an EU-based onshore Security Operations Centre.
- Full incident analysis with actionable remediation guidance
- Regular review and recommendations
- Bridging the gap between IT operational teams and cyber security
- Security monitoring service provides comprehensive visibility via Microsoft 365 Defender suite

Vulnerability management

MDR Vulnerability management is a fully managed service powered by Microsoft Defender Vulnerability Management that delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Leveraging Exploit Prediction Scoring System [EPSS], Microsoft Threat intelligence, business contexts, and devices assessments, Black Cell's Microsoft experts rapidly and continuously prioritize the biggest vulnerabilities on your most critical assets and provides security recommendations and management service to mitigate risk.

Key features & benefits

- Continuous discovery & monitoring
- Detailed weekly reporting
- Risk-based intelligent prioritization powered by EPSS to estimate the probability of exploitation activity.
- Remediation & tracking

Advanced Threat Hunting

MDR Threat Hunting is a fully managed service powered by Microsoft 365 Defender suites that has powerful hunting search and query tools to hunt for security threats across the organisation's data sources. Black Cell predefined hunting queries guide our Microsoft experts towards asking the right questions when looking for potential security issues in the metrics already present in your XDR solution. Advanced hunting is a query-based threat hunting tool that lets Black Cell Microsoft experts explore up to 30 days of raw data. We can proactively inspect events in your network to locate threat indicators and entities. The flexible access to data enables unconstrained hunting for both known and potential threats. Black Cell Threat Hunters rapidly investigate, support containment and close threats when an automated response is not possible.

Key features & benefits

- Continuous discovery & monitoring
- Detailed weekly reporting
- Channelling the validated incidents into the Security Incident Management Process
- Predefined hunting queries mapped to MITRE ATT&CK Framework
- Reduced dwell time of attacks
- Identifying unknown threats
- Defense against advanced persistent threats [ATPs]

Phishing Investigation

MDR Phishing Investigation and Response is a fully managed service powered by Microsoft Defender for Office 365 that provides insights into threats and related response actions that are available in the Microsoft 365 Defender portal. This service can help your organization's security team protect users from email- or file-based attacks. The capabilities help monitor signals and gather data from multiple sources, such as user activity, authentication, email, compromised PCs, and security incidents.

Key features & benefits

- Continuous discovery & monitoring via Microsoft Defender for Office 365
- Detailed weekly reporting
- Channelling the validated True Positive cases into the Security Incident Management Process
- Full email analysis, response and communication with actionable remediation guidance regarding emails reported by end-users

On-Demand Services
on Microsoft 365 Defender

Implementation

Consulting
and Configuration

Hardening

Training

Learn more about each service
we provide.

Implementation

Microsoft 365 Defender is a powerful and comprehensive cybersecurity suite, however to truly get the most out of your investment, you need to get the foundations right. Once you define your desired outcomes and build a plan to create value with Microsoft 365 Defender, Black Cell helps you to select the licensing and deployment path that is the best fit for your organization. Black Cell collaborates with your internal team and advises on key areas of your implementation to achieve targeted business outcomes and future-proof your investment.

Service scope:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Entra Identity Protection
- Microsoft Defender for Cloud Apps
- SIEM Integration [Microsoft Sentinel, Splunk Enterprise and IBM QRadar]

Key features & benefits

- Focus on security requirements and issues.
- Milestone and key deliverables managed through project plans.
- Anticipation and reduction of implementation risks.
- Provides the ability to define, prioritize and manage project scope.
- Measures budget to scope performance.
- Greater project visibility through consistent communications, management of expectations, and project predictability

Consulting & Configuration

Black Cell's Microsoft Consulting and Configuration services identify problems, evaluate security issues, assess risk, and implement solutions to defend against threats to companies' networks and computer systems. Our experts deal with many variables when evaluating security systems and craft layers of protection in a fast-changing IT security landscape in a zero-trust approach. Cyber is not just a technology challenge; the cyber security program must capture people, processes, and technology elements to succeed. Because of this, Black Cell experts have developed services focusing on risk management, cost efficiency, operational and technological architecture, and solution accountability on Microsoft 365 Defender suite.

Black Cell's Microsoft Defender Configuration service helps organisations take their ability to protect, detect and respond to advanced threats to the next level. We aim to assist in the understanding, usage, and optimisation of our clients' Microsoft 365 Defender solutions through a combination of technical support and best practice advice.

Key features & benefits

- License planning and management.
- Maturity roadmap planning
- Solution assessments and Proof of Concepts
- Professional support and configuration

Hardening

Black Cell Hardening services are based on Microsoft Secure Score, a native measurement tool to continuously evaluate and improve your organization's security posture, across the identity, data, apps and device domains, with a higher value indicating more resilient cybersecurity posture. Following the Secure Score recommendations, you can protect your organization from threats. Black Cell professionals determine the cybersecurity maturity based on the current score and provide you with detailed action plan to improve the overall security and remediate the vulnerabilities. You can also get an all-up view of the total score, historical trend of your secure score with benchmark comparisons, and prioritized improvement actions that can be taken to improve your score.

The Centre for Internet Security (CIS) has published benchmarks for Microsoft products and services including Microsoft 365 Foundations Benchmark. The document provides prescriptive guidance for establishing a secure baseline configuration for Azure.

Key features & benefits

- Black Cell Microsoft experts conduct gap assessment to compare the organisation's current cybersecurity maturity to the baseline configurations defined by CIS and identify the gaps or shortcomings.
- Based on the findings, Black Cell defines achievable goals with maturity levels backed by a detailed implementation plan.

Training

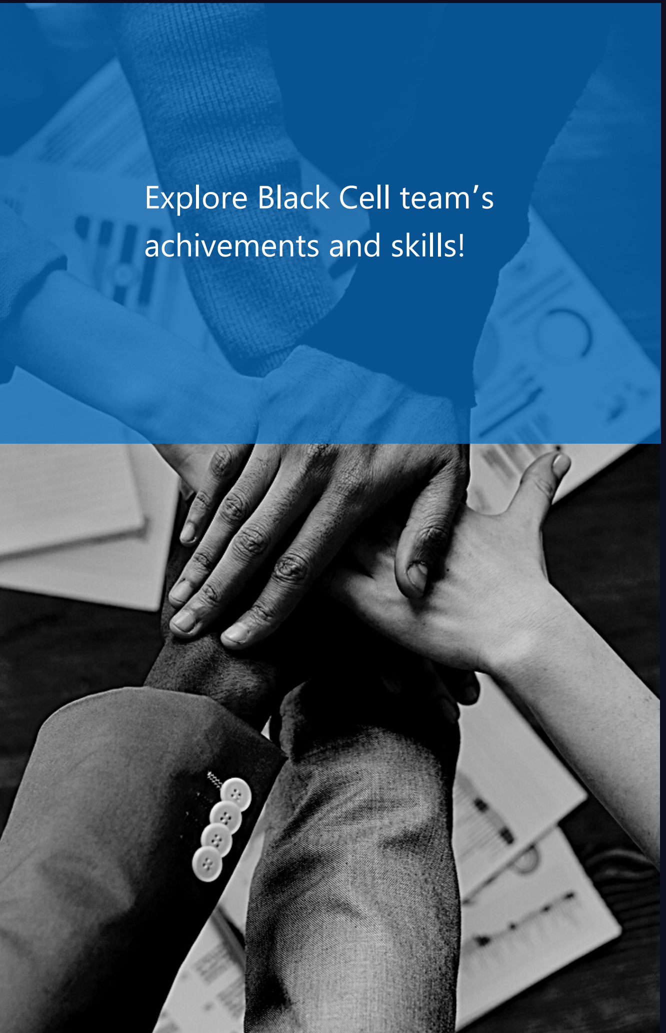
Microsoft 365 Defender is a modular cloud-based cybersecurity solution. Standalone modules can be purchased and implemented as „add-on" products on top of various Microsoft licenses. We often identify demands, that our customers would need a fully tailored training package focusing on specific Microsoft products (e.g., Defender for Endpoint). Demands are usually driven by planned and scheduled IT Security developments, which often involve cloud migration. In this case, transitions are gradual and roadmap like processes, so the project moves from function to function, that determines the modular nature of the internal training plan. The modular training package designed by Black Cell's Microsoft architects offers an adequate solution to the needs described above.

In addition to the management of the given products, the training package covers the related implementation processes as well. The modules contain several product-specific submodules that provide our customers with an additional opportunity to put together a fully tailored training plan. After a brief theoretical introduction related to the selected Microsoft solution, Black Cell experts present the practical application of the services/features in Black Cell's own Microsoft demo environment via multiple live sessions.

4 main domains

- Identity and Access Management
- Threat protection
- Information protection
- Governance and compliance

Our
Achievements & Skills

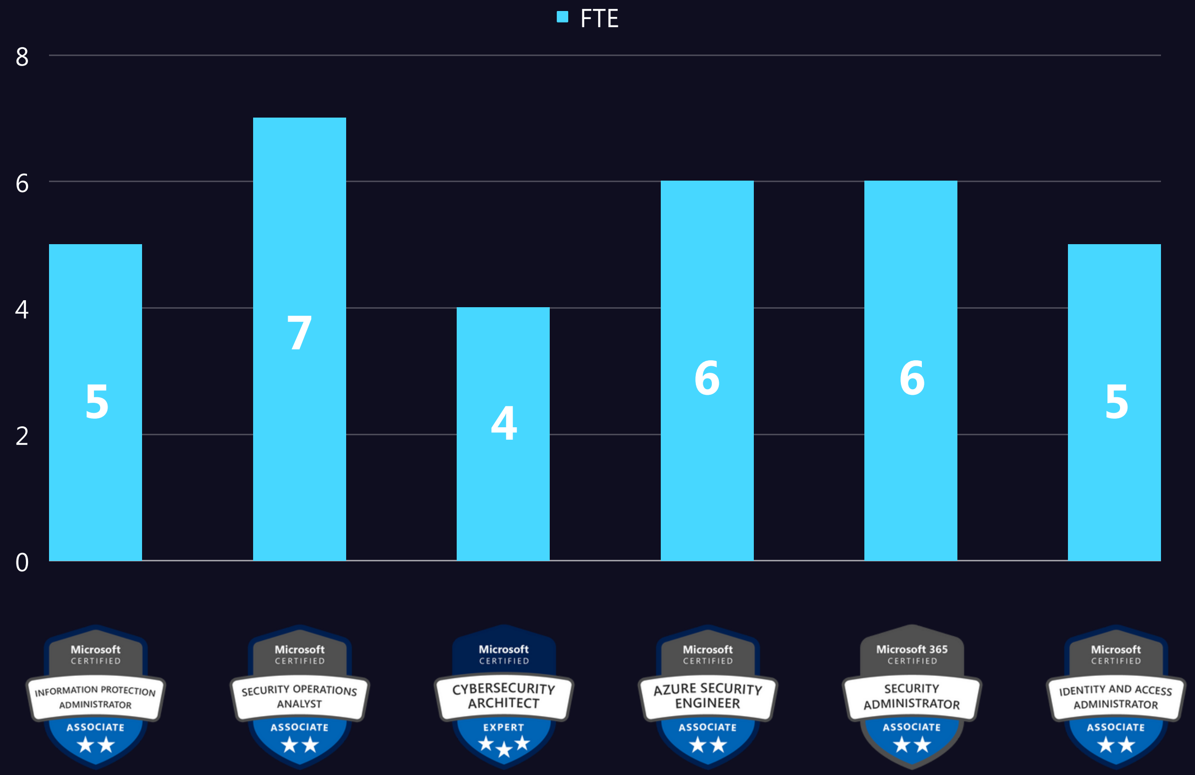


Explore Black Cell team’s achievements and skills!

Microsoft
Solutions Partner
Security

Specialist
Identity and Access Management
Threat Protection

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



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

BLACK CELL
Protecting critical infrastructures

Thanks

www.blackcell.io