CRITICALSTART Cybersecurity Consulting for Microsoft Security Solutions

SERVICES CATALOG

CRITICALSTART

They're good. We're better.

TABLE OF CONTENTS

About the Catalog

This catalog details the Cybersecurity Consulting for Microsoft Security solutions offered by CRITICAL**START**. It provides you with the scope of each service, objective, goal it fulfills, use cases, and benefits you will derive, so you can select the services that fit your unique requirements.

Service Delivery

These services are delivered by highly trained and certified cybersecurity specialists who will customize the delivery to include your business use cases and environment.

THREAT LANDSCAPE

The threat landscape today has become increasingly complex and is continuously changing. Attacker techniques have shifted from mass distribution methods to targeted attacks on specific organizations.

The digital infrastructure of organizations that include cloud native to hybrid to on-premise applications further adds to this complexity.

Security professionals now need to focus on:

- ✓ Securing their security perimeter
- ✓ Implementing a modern security infrastructure
- ✓ Safeguarding the security credentials of every cloud application

CRITICAL**START** offers four categories of consulting services:

EDUCATE

ASSESS

DESIGN

IMPLEMENT

Our experts deliver all of our services using a hands-on, business scenario-based approach.

Cybersecurity Consulting Services

Following is more detail about each of our four distinct categories of services for Microsoft Security:

✓ **Educational Workshops** train you on the Microsoft Security stack and the best practices and guidelines you should follow when adopting these solutions.

✓ **Assessments** evaluate your unique business environment and threat landscape and review your current security posture to identify any gaps. Assessments address both Azure and M365 environments.

✓ **Design Services** help you design your modern security posture based on the evolution of your business environment and threat landscape. Your design is based on risk analysis and threat modeling conducted in your environment to ensure it is relevant and actionable. This offering includes Microsoft Security Consulting Services and covers all Microsoft Security products. In addition, we offer Demos to help you visualize your business environment and the value of Microsoft Security solutions to your business.

✓ **Implementation Services** help you deploy the Microsoft Security solutions required for your business environment.

In addition, our Proof of Concept (POC) Workshops guide you on how to correctly adopt new Microsoft Security products and best practices.

The following pages detail each of the above solutions. ➡

CISO IMPERATIVES

The cloud and hybrid infrastructure environment in most enterprises today brings with it a split operational and shared security responsibility model.

Key CISO imperatives include:

- ✓ Establishing a modern perimeter with identity controls and policy to protect users, devices and data
- ✓ Enabling end-to-end visibility of security policies and compliance management
- ✓ Ensuring that every cloud application included is reviewed for security
- ✓ Adding security controls to Cloud DevOps and the cloud infrastructure

Educational Workshops:

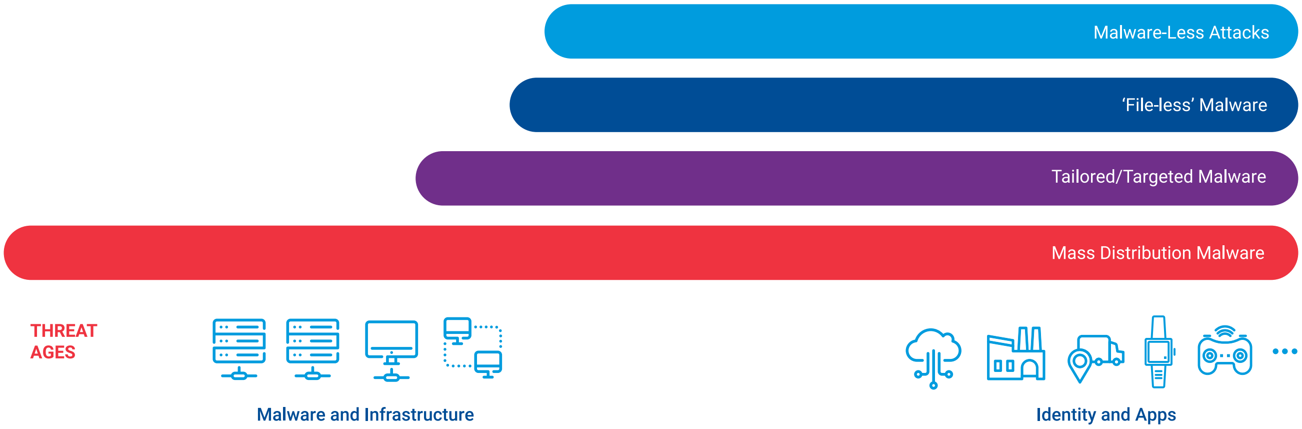
Objective: These workshops are designed to provide you with a working knowledge of the following topics:

- ✓ The modern threat landscape
- ✓ Microsoft solutions that provide the corresponding prevention, detection, and response capabilities
- ✓ Strategies for on-premises workloads and hybrid or cloud workloads
- ✓ Business scenarios showing actual cyberattack use cases and the corresponding Microsoft-recommended approach

DELIVERY METHODOLOGY

Our in-depth workshops are delivered by highly trained security consultants who understand the Microsoft Security stack. The workshop curriculum includes:

- ✓ **Modern Threat Landscape**
  This section of the workshop focuses on the current threat evolution within the enterprise and examines the key CISO imperatives to counter this threat.

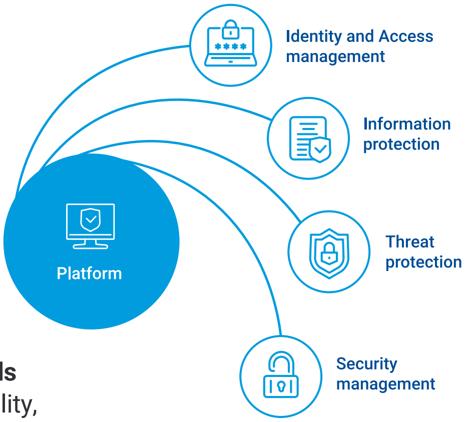

Malware-Less Attacks
'File-less' Malware
Tailored/Targeted Malware
Mass Distribution Malware
THREAT AGES
Malware and Infrastructure
Identity and Apps

Microsoft Solutions

Microsoft security solutions address most of the CISO imperatives listed above and include the following:

1. Identity and Access Management solutions that provide identity-based security and access controls
2. Threat Protection through the Microsoft 365 Defender family of solutions. These solutions protect your endpoints (Microsoft Defender for Endpoints), data (Microsoft Defender for Office 365) and cloud applications (Microsoft Cloud App Security)
3. Security and Compliance Management solution with Azure Sentinel. This provides end to end visibility of your business

Our experts use a shared responsibility model that highlights the importance of implementing security controls to protect your environment, even when the operational models are split with your cloud service providers.



Microsoft Solutions that Protect your Environment

In this service, we detail the Microsoft Security stack, including four strategic areas: Identity and Access Management, Information Protection, Threat Protection, and Security Management.

- ✓ **Strategies for on-premises workloads and hybrid or cloud workloads**
  This service covers the different architectures that help enable visibility, security and control in a multi-platform, cloud and hybrid environment. We cover strategies to modernize your on-premises security stack, while also implementing modern cloud security solutions.
- ✓ **Business scenarios showing actual cyberattack use cases and the corresponding Microsoft-recommended approach**

Business outcome: These workshops will give you and your security organization a better understanding of the critical areas mentioned above.

Assessments (Azure and M365)

Objective: Azure and M365 assessments are designed to review your threat landscape and current state implementation, identify gaps in your security posture, and define a prioritized roadmap for implementing the security controls.

DELIVERY METHODOLOGY

These assessments are delivered by highly trained cybersecurity consultants who:

- ✓ Work with you to understand your unique security objectives
- ✓ Leverage interviews and assessment scripts to understand your current security state implementation
- ✓ Use security guidelines such as National Institute of Standards and Technology (NIST)-800, Center for Internet Security (CIS) and Microsoft
- ✓ Recommend security best practices to identify security gaps
- ✓ Draw up a security strategy/roadmap and work with you to prioritize your implementation

Business outcome: These assessments will provide you with an understanding of your security posture based on Microsoft Security Best Practices.

Demos

Objective: The objective of our Demo services is to showcase the value of the solutions in the Microsoft Security stack in the context of your unique security requirements.

DELIVERY METHODOLOGY

The demos are designed to show:

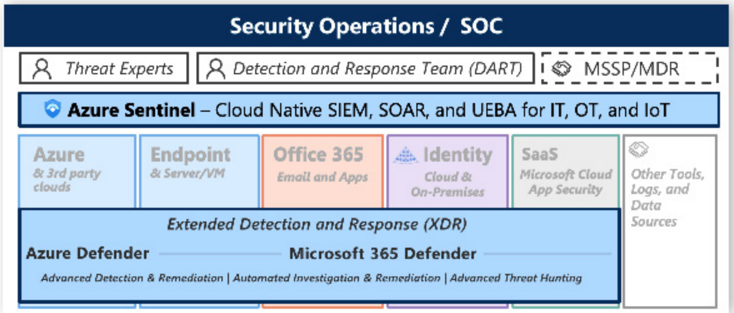
- ✓ The different product features and functionality of the Microsoft Security stack
- ✓ The use cases and business scenarios relevant to your business environment and how the Microsoft stack identifies and responds to threats in your environment
- ✓ Threat modeling in your environment and the Microsoft features that help protect you against these threats
- ✓ A day-in-the-life scenario for your Security Operations Center using the Microsoft Security solutions

Sample demos include the following real-life scenarios:

- ✓ Identity and Access Management demos

THREAT SCENARIO	MICROSOFT CAPABILITIES
Phishing and password spray attacks	Password-less authentication using biometrics (Azure Active Directory)
User account compromise	Conditional access policies in Azure Active Directory
Lateral Traversal attacks with credential threat	Privileged Access Management using Azure Active Directory Credential theft detection using Azure Identity Protection

- ✓ Security Operations Center demos


Security Operations / SOC
Threat Experts
Detection and Response Team (DART)
MSSP/MDR
Azure Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT
Azure
& 3rd party clouds
Endpoint
& Server/VM
Office 365
Email and Apps
Identity
Cloud & On-Premises
SaaS
Microsoft Cloud App Security
Other Tools, Logs, and Data Sources
Extended Detection and Response (XDR)
Azure Defender
Microsoft 365 Defender
Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

These demos address the following business requirements:

BUSINESS REQUIREMENTS	MICROSOFT CAPABILITIES
Advanced detection, investigation and remediation	Cloud-native Security Information and Event Management (SIEM), and Security Orchestration Automation and Response (SOAR) features in Microsoft Azure Sentinel.
Integrated investigation experience across all assets	Microsoft Extended Detection and Response(XDR) modules provide deep visibility into Windows, Linux, Mac desktops and servers, Office 365, Active Directory and Azure Tenants.
Extend the capabilities of the existing SOC tools	The Microsoft Graph Security API and Log Integration capabilities of the Extended Detection & Response (XDR) solution allow you to integrate existing SOC tools with the Microsoft solutions

Business outcome: These demos enable you to map your unique user scenarios and threat landscape and envision the future state with the Microsoft solution stack. The hands-on delivery of these demos makes this value more tangible.

Proof of Concept (POC) Workshops

Objective: POC Workshops are designed to help you evaluate the scope and implementation methodologies of the Microsoft Security solutions.

DELIVERY METHODOLOGY AND CURRICULUM

These hands-on, scenario-based workshops are delivered by expert security consultants. The curriculum includes the following:

- ✓ **Deployment strategies, including rapid adoption techniques**
  The adoption frameworks detail the framework for decisions, people and process maps, best practices, models and experiences. This guidance is based on real-world experiences and industry best practices.
- ✓ **Implementing business use cases and scenarios**
  In this section, we cover the various business use cases and how to implement them using the Microsoft Security stack.
- ✓ **Controls and policies tuned to meet your security needs**
  In this section we cover the controls and policies that are currently turned on and how you can change them to meet your unique needs.

Business outcome: At the end of this workshop, you will have an understanding of the Microsoft Security implementation methodologies best suited for your unique business environment.

Microsoft Security Consulting (All Microsoft Products)

Objective: Our consultants help you identify and prioritize the implementation of the appropriate Microsoft security Best Practices for your business environment.

DELIVERY METHODOLOGY

RISK ANALYSIS	THREAT MODELING	RESPONSE PLANNING	IMPLEMENTATION
OUTCOME Risk analysis of the environment	OUTCOME Technical verifications and threat modeling	OUTCOME Design based on risk modeling	OUTCOME Implementation based on security best practices

The scope of the services delivered include:

- ✓ **Risk Analysis**--Our cybersecurity consultants analyze the various risks to which your business environment is vulnerable and provide you with the type of risks and the impact of these risks can have on your business.
- ✓ **Technical verifications/threat modeling and security design reviews**-- Our consultants perform threat modeling. and use interviews and assessments to perform technical verifications and design reviews of your security roadmap.
- ✓ **Response planning and execution**--Our team designs the security architecture to respond to the threats modeled above.
- ✓ **Implementation of security best practices and tools**—Our team formulates your implementation methodology based on NIST framework and CIS guidance and Microsoft Security Best Practices.

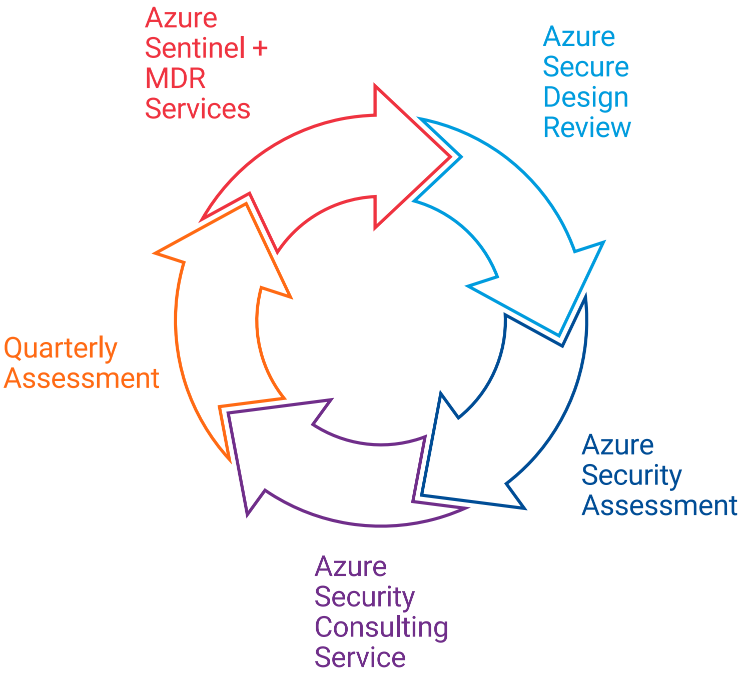
Business outcome: This service gives you guidance for the appropriate adoption of new security concepts, methodologies, and workflows such as “SecOps”, “Security by Design” and “Shift Security left” ideologies.

Microsoft Azure Security and Compliance Consulting and Assessment

Overview: The Azure Security and Compliance Consulting and Assessment services focus on assessing the strength and vulnerabilities of your run-state Azure environment and identifying gaps or opportunities to improve your security.

THE SERVICES AVAILABLE AS PART OF THIS OFFERING ARE:

- ✓ **Azure Secure Design Review**: This service is focused on reviewing your current design and its efficacy using advanced threat modeling and attack analysis. It also analyzes the current design against security best practices.
- ✓ **Azure Security Assessments:** This service is focused on using industry guidelines such as NIST-800, CIS and Microsoft Security Best Practices to validate the administrative and technical security controls in your environment.
- ✓ **Azure Security Consulting Services:** This is an ongoing consulting service where expert security consultants review and fine tune your security controls, allowing you to stay current with your security posture.
- ✓ **Quarterly Assessments:** This service is designed to ensure security governance and continuous security assurance. The reviews are conducted on a quarterly basis and are highly recommended for especially sensitive workloads.
- ✓ **Azure Sentinel + MDR:** This offering provides implementation services for Azure Security products. including Azure Security Center, Azure AD Identity Protection, Azure AD Conditional Access and end-to-end deployment of Azure Sentinel. 24/7 alert monitoring services are available through the CRITICAL**START** MDR solution.


Azure Sentinel + MDR Services
Azure Secure Design Review
Azure Security Assessment
Azure Security Consulting Service
Quarterly Assessment

Business outcome: These services ensure that your Azure Security solutions are in compliance with the best practices laid out in industry standards and your unique security requirements. They provide you with your security gaps, prioritized recommendations, risk exposure, and product implementation.

Microsoft Azure Sentinel (Microsoft's cloud-based SIEM)

Objective: This offering provides one of the most advanced Azure Sentinel deployments in the market to implement data connectors to Microsoft and non-Microsoft sources. Expert security consultants also design a comprehensive log collection strategy and custom detection rules, dashboards, and automation playbooks, as required.

DELIVERY METHODOLOGY

Service offerings include the following:

✓ **Planning**
During this phase of the service offering, we develop the implementation plan for your Azure Sentinel deployment, including:

- Details regarding timeline and deployment phases
- Details regarding roles, responsibilities, permissions, and authorizations

✓ **Deployment Services**
This phase of the service offering includes:

- End- to- end deployment of Azure Sentinel to enable all features of the solution
- Implementation of data connectors for Microsoft data sources, such as Microsoft Defender for Office 365, Microsoft Defender for Endpoints, and Microsoft Cloud App Security.
- Implementation of connectors for non-Microsoft data/log sources
- Design and implementation of the log collection strategy
- Deployment of the Log Analytics Gateway for any on-prem data collection

✓ **Configuration Services**
These services cover the following configurations:

- Multiple log analytics workspace designed to enable log isolation and storage cost separation
- Governance and access control
- Microsoft's built-in detection rules
- Azure Sentinel analytics (alert) rules to match customer log sources
- Built-in security workbooks (interactive dashboards)
- "Security Metrics Tracker" dashboard (Mean-Time-to-Detection, Mean-Time-to-Remediate etc.)

Training that covers the following curriculum:

✓ Investigations using workbooks or dashboards

✓ Advanced Investigations using Graph UI

✓ Advanced Investigations using User Behavior Analytics

✓ Scenario-based, real-world threat identification

✓ Incident life-cycle management

Business outcome: These services provide you with a fully deployed Azure Sentinel with data connectors (Microsoft and non-Microsoft sources) that are enabled and detection- ready.

Microsoft 365 Defender

Objective: This offering includes deployment services for Microsoft Defender for Office 365, Microsoft Defender for Endpoint, and Microsoft Cloud App Security. We customize these deployments to ensure compliance to your internal security policies and business requirements.

Microsoft Defender for Office 365

Objective: The scope of this engagement is the design and implementation of the Microsoft Defender for Office 365.

THREAT PROTECTION WITH MICROSOFT DEFENDER FOR OFFICE 365

Microsoft Defender for Office 365 provides protection in four phases:

1. **Edge protection –** protects Office 365 infrastructure and customers from Denial of Service (DOS) attacks, blocks messages being sent from known bad connecting IP addresses, automatically block known bad domain.
2. **Sender intelligence –** enables catching spam, bulk, impersonation, and unauthorized spoof messages and phish detection.
3. **Content filtering –** handles the contents of the mail including hyperlinks and attachments.
4. **Post delivery protection –** provides protection after mail delivery, including safe links, zero-hour auto-purge for phishing, and malware.

DELIVERY METHODOLOGY

This service offering includes the following end-to-end deployment steps:

- ✓ Review the subscriptions required
- ✓ Configure the required M365 roles and permissions
- ✓ Turn on audit logging for reporting and investigation
- ✓ Configure the policies and controls for the following:
  - – Anti-malware protection
  - – Anti-phishing protection
  - – Anti-spam protection
  - – Protection from malicious URLs and files including Safe Links and Safe Attachment policies
- ✓ Verify that Safe Attachments for SharePoint, OneDrive and Microsoft Teams is turned on
- ✓ Set up alerts in the Security and Compliance Center
- ✓ Configure the zero-hour auto purge against spam and malware

Business outcome: This service results in full deployment of Microsoft Defender for Office with protection enabled for malware, spam, phishing and malicious content.

Microsoft Defender for Endpoint

Objective: The scope of this engagement is the design and implementation of Microsoft Defender for Endpoint, including the following:

- Endpoint vulnerability mitigation
- Application management
- Windows 10 and Windows Server security optimization
- Endpoint incident response and recovery

DELIVERY METHODOLOGY AND SERVICE SCOPE

Our service scope includes the following:

IDENTIFY ARCHITECTURE	SELECT DEPLOYMENT METHOD	CONFIGURE CAPABILITIES
Identify which architecture best represents your enterprise:	Select your preferred deployment	Configure the following capabilities:
Cloud-native	Local script (upt to 10 devices)	Endpoint detection & response
Co-management	Group policy	Next-generation protection
On-premise	Microsoft Endpoint Manager/Mobile Device Manager	Attack surface reduction
Evaluation and local onboarding	Microsoft Endpoint Configuration Manager	
	Script	

- ✓ **Identify architecture:** We help you plan your architecture based on your environment that includes Cloud-native, Co-management, on-premise and Evaluation and local onboarding.
- ✓ **Select deployment method:** Defender for Endpoint supports a variety of endpoints. Each endpoint has deployment tools that can be used to support the deployment. We help you select the right deployment method to meet your needs.
- ✓ **Deployment:** We guide you to work across stakeholders in your organization to prepare your environment and onboard devices, moving from evaluation to pilot,' to full deployment.
- ✓ **Migrate from non-Microsoft solution to Microsoft Defender for Endpoint:** If you have a non-Microsoft anti-virus and want to move to Microsoft Defender for Endpoint, we provide you with all the services needed for this migration.
- ✓ **Set up the threat and vulnerability management for Microsoft Defender for Endpoint.** We also set up the Microsoft Defender Security Center.

Business outcome: When this service is complete, your organization will have the right design and configuration of Microsoft Defender for Endpoint and the ability to secure the devices in your environment.

Microsoft Cloud App Security

Objective: The scope of this engagement is the design and implementation of the Microsoft Cloud App Security and includes the following:

- Controls to enable identification and management of unsanctioned applications
- Governance and control policies for sensitive data
- SaaS/Cloud app compliance assessment and controlled use strategy

SECURITY WITH MICROSOFT CLOUD APP SECURITY

Microsoft Cloud App Security brings four distinct values to your organization.

Our service scope includes the following:

- ✓ Discover and identify the cloud apps, IaaS and PaaS services used by your organization and control the use of Shadow IT.
- ✓ Identify, classify and protect sensitive information with the Data Loss Prevention capabilities of Microsoft Cloud App Security
- ✓ Detect unusual behavior across apps, users and potential ransomware using the multiple detection methods used by Cloud App Security
- ✓ Assess your compliance with regulations and industry standards across all your cloud apps and specific to your organization.

DELIVERY METHODOLOGY

As part of this service offering, we:

- ✓ Set up your app connectors to ensure instant visibility, protection and governance actions for your apps.
- ✓ Enable file monitoring and create file policies to protect sensitive information with DLP policies.
- ✓ Create policies to control your cloud apps.
- ✓ Set up cloud discovery. As part of this, we integrate Microsoft Defender for endpoints, integrate Zscaler if you use that today and create a continuous cloud discovery report.
- ✓ Deploy Conditional Access App Control for featured apps.
- ✓ Personalize your experience by adding your organization details to the application.
- ✓ Organize your data according to your needs.

Business outcome: Following this service, your organization has the assurance that it is protected against threats to your cloud applications and that it has control against Shadow IT.

About CRITICAL**START** Cybersecurity Consulting

You can rely on our expert cybersecurity consultants to serve as your trusted advisors throughout your Microsoft implementation journey. CRITICAL**START** is a Microsoft MSSP Program Partner and member of the Microsoft Intelligent Security Association.

Contact your Microsoft or CRITICAL**START** **sales representative to learn more.**

Member of
Microsoft Intelligent
Security Association

Microsoft

Gold
Microsoft Partner

Microsoft

Contact Us

Request a Free Assessment

CRITICALSTART
They're good. We're better.