Microsoft 365

OXFORD
COMPUTER GROUP

Security Workshop

Oxford Computer Group

Introducing Security Workshop

Introducing the Security Workshop

An executive deep dive into security strategy, tailored to your organization.

Microsoft Security Workshop at a Glance

Designed for today's security leaders, the Microsoft Security Workshop focuses on learning your organization's unique needs and develops a strategic security plan based on approaches recommended by Microsoft experts.

After the workshop, you'll...

→ Get customized security strategy reports for your teams and stakeholders

→ Gain a better understanding on how to prioritize, and mitigate potential threats

→ Set next steps based on your needs and objectives

Workshop activities

Pre-engagement call
We'll confirm scope, logistics, and prerequisites for the experience.

Assessment set up
We'll help you set up your Threat Check and any other assessments.

Workshop day
We'll deep dive on your assessment and security needs, talk about Microsoft security, and plan next steps.

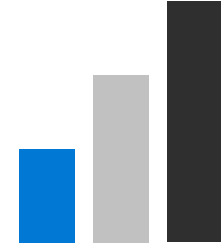# What we'll do during the workshop

Focus on learning about your priorities, initiatives and key influences on your security strategy.
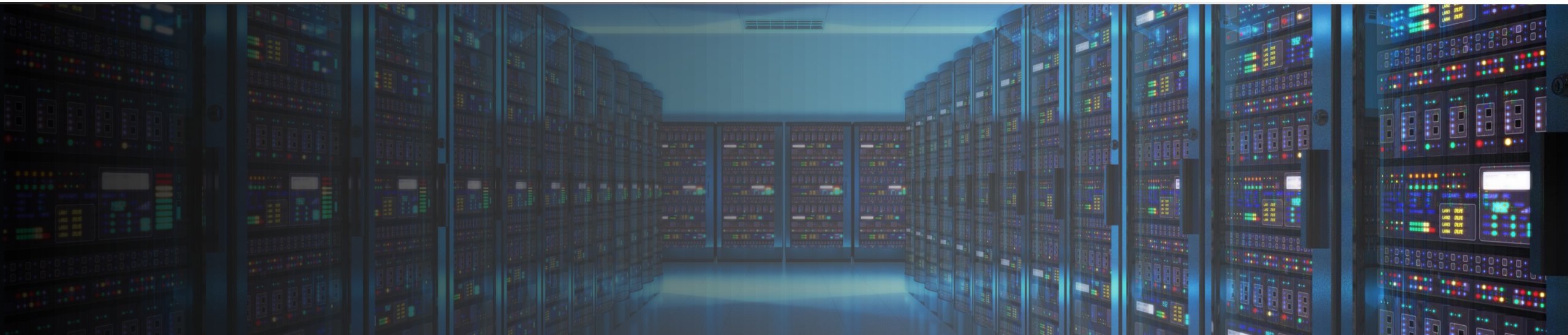
Discover threats to your environment across email, identity, and data.
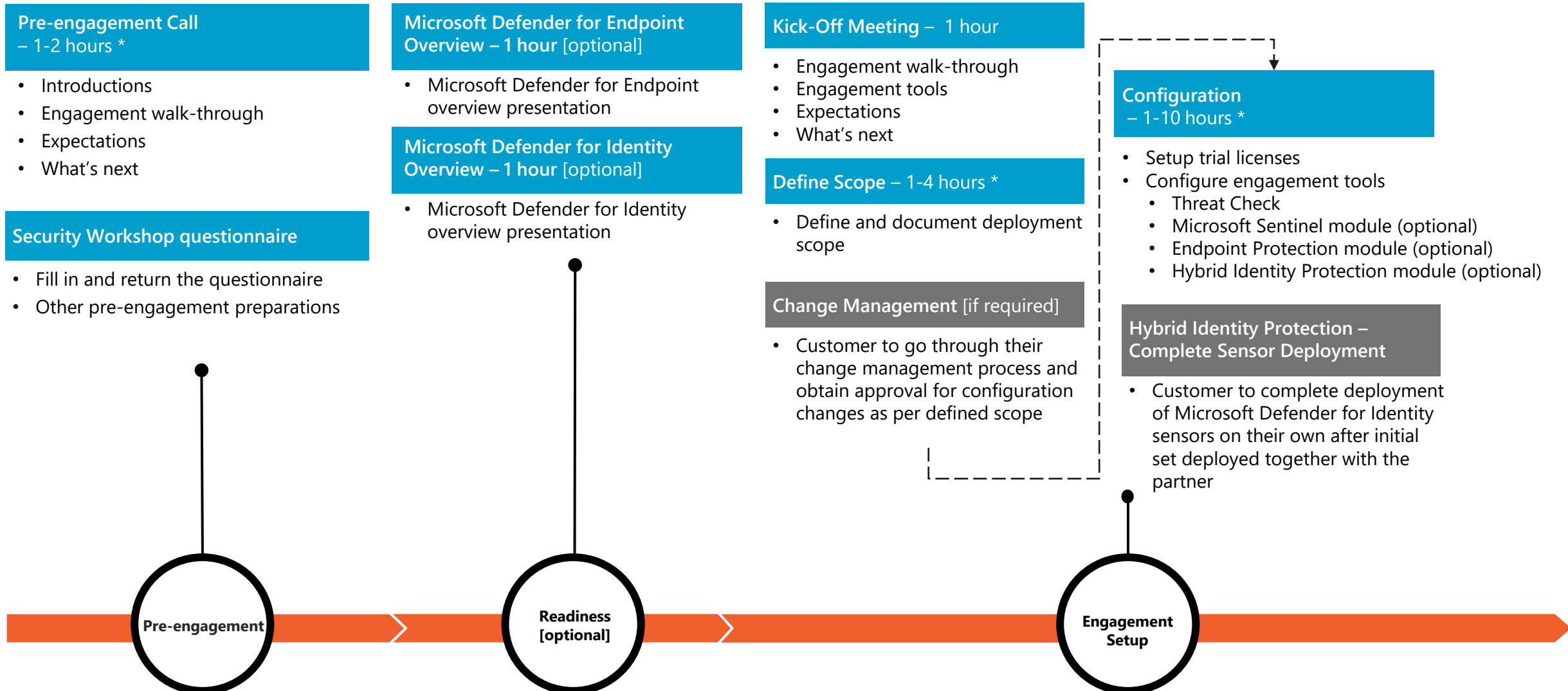
Learn about Microsoft's approach to security with an immersive experience.

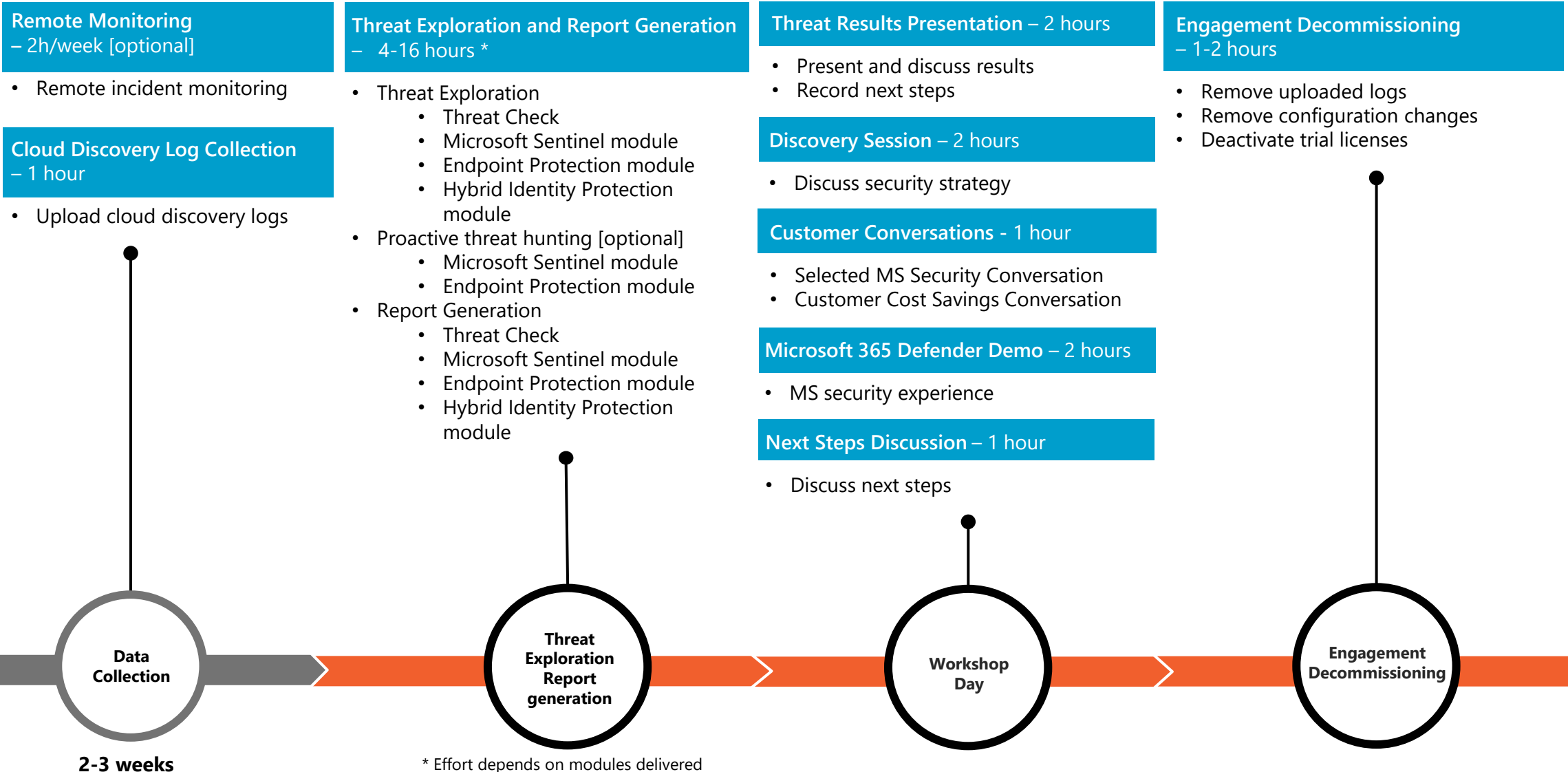**Plan** next steps on how we can work together.

Security Workshop phases and activities

Pre-engagement Call – 1-2 hours *

- Introductions
- Engagement walk-through
- Expectations
- What's next

Security Workshop questionnaire

- Fill in and return the questionnaire
- Other pre-engagement preparations

Microsoft Defender for Endpoint Overview – 1 hour [optional]

- Microsoft Defender for Endpoint overview presentation

Microsoft Defender for Identity Overview – 1 hour [optional]

- Microsoft Defender for Identity overview presentation

Kick-Off Meeting – 1 hour

- Engagement walk-through
- Engagement tools
- Expectations
- What's next

Define Scope – 1-4 hours *

- Define and document deployment scope

Change Management [if required]

- Customer to go through their change management process and obtain approval for configuration changes as per defined scope

Configuration – 1-10 hours *

- Setup trial licenses
- Configure engagement tools
  - Threat Check
  - Microsoft Sentinel module (optional)
  - Endpoint Protection module (optional)
  - Hybrid Identity Protection module (optional)

Hybrid Identity Protection – Complete Sensor Deployment

- Customer to complete deployment of Microsoft Defender for Identity sensors on their own after initial set deployed together with the partner

Pre-engagement

Readiness [optional]

Engagement Setup

* Effort depends on modules delivered

Security Workshop phases and activities

Remote Monitoring – 2h/week [optional]

- Remote incident monitoring

Cloud Discovery Log Collection – 1 hour

- Upload cloud discovery logs

Threat Exploration and Report Generation – 4-16 hours *

- Threat Exploration
  - Threat Check
  - Microsoft Sentinel module
  - Endpoint Protection module
  - Hybrid Identity Protection module
- Proactive threat hunting [optional]
  - Microsoft Sentinel module
  - Endpoint Protection module
- Report Generation
  - Threat Check
  - Microsoft Sentinel module
  - Endpoint Protection module
  - Hybrid Identity Protection module

Threat Results Presentation – 2 hours

- Present and discuss results
- Record next steps

Discovery Session – 2 hours

- Discuss security strategy

Customer Conversations - 1 hour

- Selected MS Security Conversation
- Customer Cost Savings Conversation

Microsoft 365 Defender Demo – 2 hours

- MS security experience

Next Steps Discussion – 1 hour

- Discuss next steps

Engagement Decommissioning – 1-2 hours

- Remove uploaded logs
- Remove configuration changes
- Deactivate trial licenses

Data Collection

Threat Exploration Report generation

Workshop Day

Engagement Decommissioning

2-3 weeks

* Effort depends on modules delivered

Introducing the Threat Check

Use selected Microsoft 365 security products and features to gain visibility into threats to your Microsoft 365 cloud across email, identity, and data.

Approach

Discover

- Use Microsoft 365 Defender to understand the correlation between threats

- Use Microsoft Entra ID Protection and Microsoft Defender for Cloud Apps to understand threats to identity

- Use Microsoft Defender for Office and Microsoft Defender for Cloud Apps to understand threats to your email and data

- Use Microsoft Defender for Cloud Apps to understand unsanctioned use of cloud applications and service ("shadow IT")

Recommend

- Provide remediation suggestions by mapping discovered threats to Microsoft 365 security products

After the Security Workshop, you'll...

OXFORD COMPUTER GROUP

✓ Have security strategy documentation for your teams and stakeholders.

✓ Better understand, prioritize, and mitigate potential threats.

✓ Accelerate your security journey with Microsoft.

✓ Have defined next steps based on your needs and objectives.

Optional Add-On Modules

Microsoft Sentinel

Allows you to experience Microsoft Sentinel and find threats in your environment. Understand the benefits of a cloud native SIEM, prioritize and mitigate threats, and define objectives.

Endpoint Protection

Gain insights on active threats and weaknesses related to your Windows 10 endpoints and better understand the features and benefits of Microsoft Defender for Endpoint.

Hybrid Identity Protection

Gain insights on active threats and weaknesses related to your Active Directory and understand the benefits and features of Microsoft Defender for Identity.

Customer Cost Savings

Understand how Microsoft Security can help you specifically Streamline and strengthen your security posture through an introductory cost savings analysis.

Contact

 info@oxfordcomputergroup.com

 @OCGUSOfficial

 Search for Oxford Computer Group

 www.facebook.com/oxfordcomputergroup/