



Security

# **Cybersecurity Assessment**

**Engagement Overview** 



Unrestricted

# Introducing the Cybersecurity Assessment

Discover vulnerabilities to Microsoft cloud and on-premises environments.



## What we'll do during the engagement





**Analyze** the customer's environment and current cybersecurity maturity level based on v8 of the CIS Critical Security Controls.





Perform a vulnerability assessment and assist with the prioritization of vulnerabilities and misconfigurations across the customer's organization.

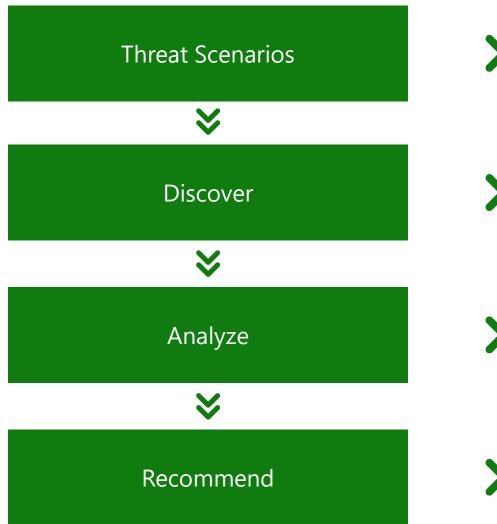


Perform a data security assessment, discover and evaluate sensitive information and potential insider risks in the customer's organization.



**Plan** next steps on how to improve the customer's cyber and data security posture and how you can work together for future engagements.

# **Engagement Methodology**



The engagement covers two commonly seen threat scenarios:

- Human-operated Ransomware
- Data Security risks from company insiders

Using the engagement tools, discover vulnerabilities within the customer's production environment across cloud, servers and endpoints.



The vulnerabilities and risks are analyzed and prioritized to show how prepared the customer's defenses are against the included threat scenarios.



Prepare detailed recommendations from the assessment to help the customer prioritize the improvements to their cybersecurity posture.

### **Objectives and Approach**



#### **Discover vulnerabilities**

Gain visibility into vulnerabilities to the customer's Microsoft 365 cloud using Microsoft Secure Score.

Discover and analyze vulnerabilities to servers and endpoints using Microsoft Defender Vulnerability Management.

# Explore and Evaluate sensitive information and potential insider risk

Gain visibility into sensitive information discovered by Microsoft Purview Information Protection.

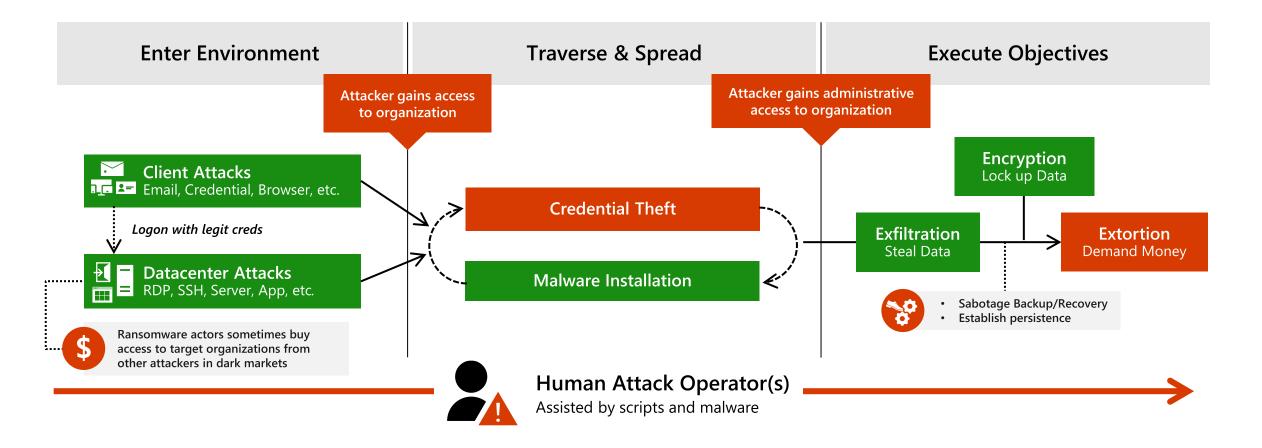
Explore potentially risky data handling activities identified by Microsoft Purview Insider Risk Management Analytics.

#### Define next steps

As part of the engagement, work together with the customer to define a list of next steps based on their needs, objectives, and results from the Cybersecurity Assessment.

# Human-operated Ransomware Overview

Human-operated ransomware is the result of an active attack by cybercriminals that infiltrate an organization's on-premises or cloud IT infrastructure, elevate their privileges, and deploy ransomware to critical data.



#### Top data security concerns



### Data security incidents are widespread



of organizations experience more than one data breach in their lifetime<sup>1</sup>

Malicious insiders account for 20% of data breaches, adding to costs



Total average cost of activities to resolve insider threats over 12 month period<sup>2</sup>

Organizations are struggling with a fragmented solution landscape

80%

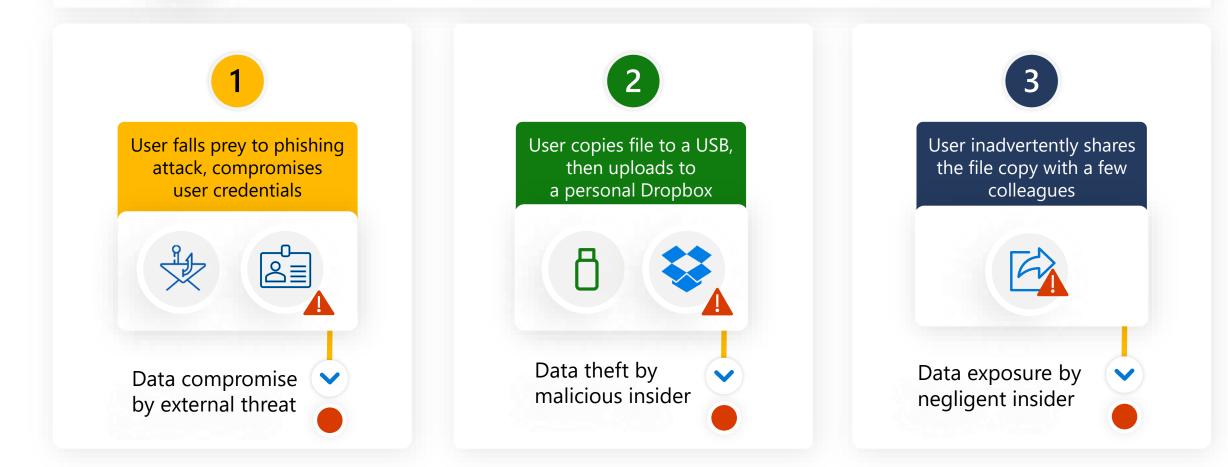
of decision makers purchased multiple products to meet compliance and data protection needs<sup>3</sup>

1. Cost of a Data Breach Report 2022, IBM

- 2. Cost of Insider Threats Global Report 2022, Ponemon Institute
- 3. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

## Data security incidents can happen anytime, anywhere

Data at risk of misuse if organization has no visibility into their data estate



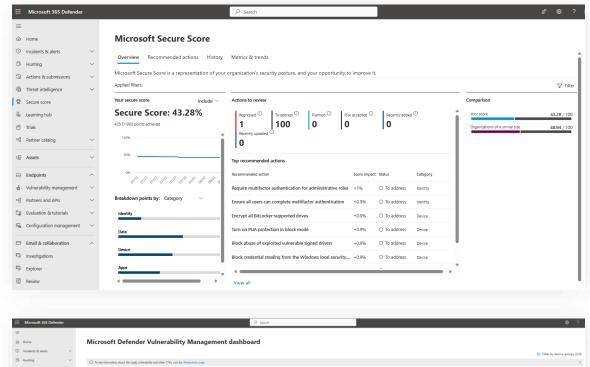
# **Vulnerabilities Exploration**

### $\gg$

Help the customer gain visibility into vulnerabilities in their cloud and onpremises environments obtained through Microsoft Secure Score and Microsoft Defender Vulnerability Management.



- Provide recommendations on:
- How to discover and prioritize vulnerabilities and misconfigurations.



Home	n	licrosoft Defender vulner	ability Management dashb	oard									
Incidents & alerts	~											🔊 Filter by	device groups (3/
Hunting	×	To see information about the Log4j vulnerability and other 0	CVEs, visit the Weaknesses page										
Actions & submissions Threat intelligence	ž	Organization exposure score	Top security recommendations			Microsoft Secure Score for	Devices	Top events (7 days)					
Secure score	Ť	r				Your score fo	. destant						
		Exposure score	Recommendation	Exposed devices Threats Impact	Tags			Date (UTC) Event				Origi	nally impacted d
Learning hub		This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.	Block all Office applications from creating child	4 © Õ ▼21.00  +9.00	+2	This score reflects the collective posture of your devices across O Accounts and Security Controls 1	25, Application, Network,						
rials		impacted by active enceptions.	Block Office applications from creating executa	4 <sup>®</sup> <sup>®</sup> ▼21.00   +9.00	+1	impacted by active exceptions. 282/110 points actived	actes prientery						
Partner catalog	~		Block JavaScript or VBScript from launching do	4 @ Ŏ ▼21.00   +9.00	+1	Application	N A						
Assets	^		Show more Show exceptions			05	107/2	Show more					
levices													
dentities		27/100	Device exposure distribution	Top remediation activities		Network	50/	Top vulnerable software					
ndpoints	~	Exposure score over time	<b>Exposure distribution</b>	Remediation act	vities	Accounts	45/	Software	OS platform	Weaknesses	Threats	Exposed dev	ices
ulnerability management	^	60	Exposed devices are easy targets for cybersecurity attacks.	No activities to show. Create remediation	activities based	Score for device	es over time	Opensal	Windows	22	@ 0	1/4	
lashboard		40	Ensure that these devices can receive security updates, have critical security controls, and are properly configured.	on your security recommendations.		48.5%		Opensal	HT100H	**		1/4	
ecommendations		» \					1	Php	Windows	10	8 Ö	1/1	
emediation renotories		0 05/08 05/02				47.4% 05/0	8 05/22	Firefox	Windows	75	0 D	1/1	
ventories Ieakinesses		Improve score				Improve score		Show more					
ent timeline													
aselines assessment		Expiring server certificates				Top exposed devices							
artners and APIs	$\sim$												
valuation & tutorials	$\sim$	1 certificates expired				Name	Security recomm	endations Discovered vulnerabilities					
onfiguration management	$\sim$					seclabcit01	59	97	A Medium				
nail & collaboration	~	Expired Expires In 30 Days 2 more				seclabsrv01	57	19	🔥 Medium				
vestigations			Low Medium			attacksim-dc	51	2	▲ Low				
plorer		View all		Go to security recommendation	s	Show more							
view													

# **Data Security Exploration**

- Help the customer gain visibility into data security risks in their organization obtained through zero change management configurations.

Provide snapshots of what sensitive information exists within the customer's Microsoft 365 environment



Conduct an evaluation of potential insider risks in the customer's organization without configuring any insider risk policies.

Top sensitive info types

Sensitive info

All Full Nam EU Tax Iden

EU Nationa Malta Tax ID

#### Sensitive info types used most in your content

Proseware Merger All	I Full Names	EL	J Tax lo	dentificatior	n Number (TIN) 📃 EU National Identification Number 2 more
${\cal P}$ Filter on labels, info types, or cate	egories	All Id	ocatio	ns	
ensitive info types	^ 1	<u>↓</u> E	xport		4 items
Proseware Merger	4659		۵	Name	Files
All Full Names	1497			Exchange	169 >
EU Tax Identification Number (TIN)	627			OneDrive	110 >
EU National Identification Number	561			SharePoint	10 >
Malta Tax ID Number	498			Teams	Potential data theft activities
Malta Identity Card Number	496				The exfiltration activities below might be related to data theft by departing users near
					their resignation or termination date. After reviewing them, consider setting up the recommended policy to help address potential risks. What we detected The following is recent activity based on a scan of 219 users who are leaving your organization. 5.9% of users with a resignation date performed exfiltration activities 4.6% of users with a resignation date performed activities involving sensitive info 3.2% of users with a resignation date performed activities with people outside your organization 2.3% of users with a resignation date shared SharePoint files 2.3% of users with a resignation date shared SharePoint folders with people outside your organization 2.3% of users with a resignation date emailed people outside your organization 1.8% of users with a resignation date copied content to USB
					<ul> <li>1.8% of users with a resignation date printed a large number of files</li> <li>1.4% of users with a resignation date shared SharePoint files with people outside your organization</li> <li>1.4% of users with a resignation date copied sensitive content to personal cloud</li> <li>0.9% of users with a resignation date shared files across network</li> </ul>

# Cloud Discovery Exploration - Optional

>>

Help the customer gain visibility into Shadow IT usage, identifying apps accessed by users across their organization using Microsoft Defender for Cloud Apps.

 $\gg$ 

Evaluate discovered apps for more than 90 risk indicators, allowing you to sort through the discovered apps and assess the customer's security and compliance posture.

pdated on Mar 15, 2023, 8:08 PM	1						
ashboard Discovered a	apps Discovered resources	IP addresses Users	Devices				
Apps 4	IP addresses 2	<sup>Users</sup>	Devices 2	Traffic 20 MB	● 99 KB ● 20 MB		
App categories			<1-4 of	f 4 ▶ Traffic	∨ 🖻	Risk levels	All categories 💙 by Traffic
			Sanctioned	Unsanctioned	🖾 🕻 Other		
					16 MB 4 MB 157 KB 80 KB	20 MB Total	Traffic from high risk apps Traffic from medium risk apps Traffic from low risk apps Configure score metric
Discovered apps		<1-4 of 4 ► View all app	IS All categories	♥ Traffic	▼ 🖾	Top entities	View all users User V by Traffic
•			Sanctioned	d Unsanctione	d Other 16 MB 4 MB 157 KB 80 KB	User alice@	
Cloud Discovery > Micros	soft MSN						
Cloud Discovery > Microsoft Wicrosoft Web ap News and errert UNSANCTIONED	soft MSN t MSN talmmer - Microsoft	Overview II	nfo Cloud app usage				₩ Win10 Endpoint Users ∨ ③ Last 30 days ∨ Actions ∨
Cloud Discovery > Microsoft Web app Web app Wicrosoft UNSANCTIONED App summary	soft MSN <b>t MSN</b> asimmet + Microsoft	< Overview II Cloud app score			Usage		Win10 Endpoint Users ∨ ⊙ Last 30 days ∨ Actions ∨           Usage trend         Usage
Cloud Discovery > Microsoft Wicrosoft Web ap News and errert UNSANCTIONED	soft MSN t MSN talmmer - Microsoft	Cloud app score		<b>10</b> /10	Usage Users 1	Traffic 157 KB	
Cloud Discovery > Microsoft Web ap News and ervert URGANCTONED	soft MSN t MSN aliment + Microsoft	Cloud app score	2		Users	Traffic 157 KB Devices 1	Usage trend Us Users: 1
Cloud Discovery > Microsoft Web app Web apo Web apo Web apo Web apo Microsoft UNGAUCIONED	soft MSN t MSN taimmet - Microsoft Cloud usage level High	Cloud app score Cloud a app score General Security Compliance	pp score: 10/10	10/10 10/10 10/10	Users 1	157 KB	Usage trend Us Users: 1
Cloud Discovery > Microsoft Wick ago Microsoft Web ago Microsoft Micro	soft MSN t MSN taimmet - Microsoft Cloud usage level High	Cloud app score Cloud ap General Security Compliance Legal	pp score: 10/10	10/10 10/10 10/10	Users 1 IPs 1	157 KB	Usage trend Us Users: 1 2 0 0 0 0 0 0 0 0 0 0 0 0 0

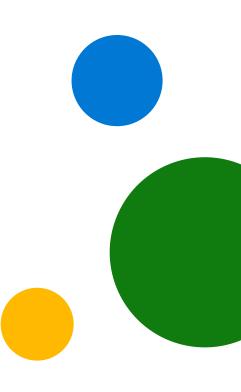
# After the Cybersecurity Assessment, the customer will...

Better understand, prioritize, and address cybersecurity vulnerabilities and how to improve their defenses against human-operated ransomware.



Better understand, prioritize, and address data security vulnerabilities and how to minimize data security risks from company insiders.

Have defined next steps based on the engagement findings and their needs and objectives.



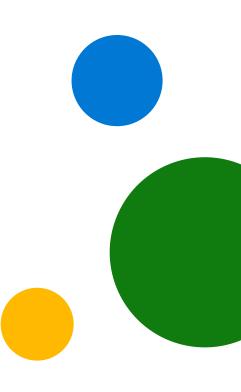
# After the Cybersecurity Assessment, the customer will...

Better understand, prioritize, and address cybersecurity vulnerabilities and how to improve their defenses against human-operated ransomware.



Better understand, prioritize, and address data security vulnerabilities and how to minimize data security risks from company insiders.

Have defined next steps based on the engagement findings and their needs and objectives.







# **Cybersecurity Assessment**

For more information, please contact us at

www.cloudguard.ai hello@cloudguard.ai +44 (0)161 504 3313



