

END-TO-END ATTACK SIMULATION AND INVESTIGATION

SIEMBIOT CYBER ACADEMY

<https://cyber-academy.siembiot.eu/>

Zonă de brainstorming:

Brainstorming Zone

Collaborate, explore, and grow. This is where ideas meet feedback, and great solutions are born through shared knowledge.

Search feed by description

- All
- Devices Information
- Accounts Information
- Registries Information
- Applications Information
- Groups Information
- Agents Information
- Logon Types
- Active Directory
- Azure Active Directory
- Azure Activity
- Azure Diagnostics
- Azure Key Vault
- DNS
- Data Management
- Defender for Cloud Apps
- Defender for Endpoint
- Defender for Identity
- Functions
- Heartbeat
- Information Protection
- Intune
- Log Analytics
- Office 365
- Security Alert
- UEBA
- Windows Security Events
- Process Creation

Frenk
17:21 • 24/02/2026 • Accounts Information Copy query

```
1 location:"office365" AND data.office365.Workload:"OneDrive" AND data.office365.EventSource:"SharePoint" AND data.office365.Operation:"FileDownloaded" AND
2 data.office365.UserId:"cbc6fb898c@dom08.SMB01"
```

This query make reference to events generated when a file is downloaded from OneDrive online (for a specific user account). Based on this query, the affected user was informed about anomaly to confirm if this anomaly was generated by his actions or not. The end user informed us that this activity was not generated by him. Therefore, it has been confirmed that the user account is compromised, and account recovery actions have been successfully performed.

2 ❤️ 36 comments

Add comment

Frenk
13:52 • 02/03/2026 • Office 365 Copy query

```
1 location:"office365" AND data.office365.Workload:"OneDrive" AND data.office365.EventSource:"SharePoint" AND data.office365.Operation:"FileDownloaded" AND
2 data.office365.UserId:"cbc6fb898c@dom08.SMB01"
```

Această interogare face referire la evenimentele generate atunci când un fișier este descărcat de pe OneDrive online (pentru un anumit cont de utilizator). Pe baza acestei interogări, utilizatorul afectat a fost informat despre anomalie pentru a confirma dacă această anomalie a fost generată de acțiunile sale sau nu. Utilizatorul ne-a informat că această activitate nu a fost generată de el. Prin urmare, s-a confirmat că respectivul cont de utilizator este compromis.

1 ❤️ 33 comments

Add comment

Descrierea interogărilor:

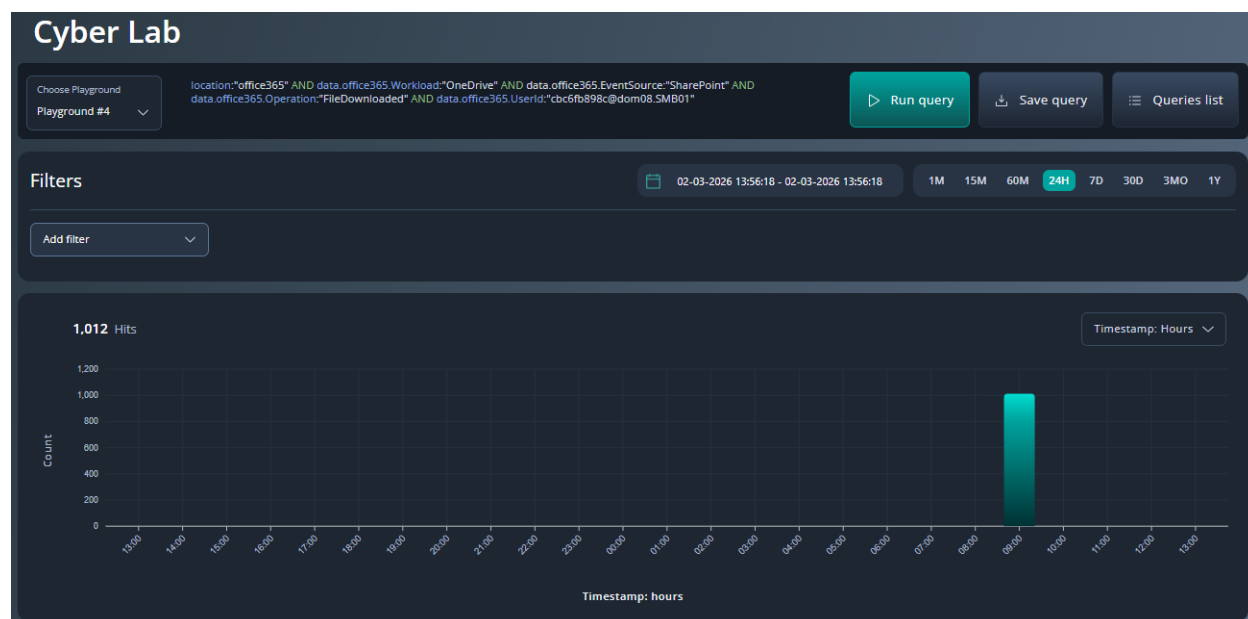
1. Anomalie de descărcare în masă:

- Această interogare a fost definită pentru a detecta toate evenimentele referitoare la acțiunea de descărcare generată de un utilizator în OneDrive utilizând contul său Office 365 (valoarea SharePoint face referire la faptul că descărcarea a fost generată de pe OneDrive-ul online al utilizatorului, nu de pe dispozitivul local).

Interogare:

```
location:"office365" AND data.office365.Workload:"OneDrive" AND  
data.office365.EventSource:"SharePoint" AND data.office365.Operation:"FileDownloaded"  
AND data.office365.UserId:"cbc6fb898c@dom08.SMB01"
```

Rezultat:



Mar 02, 2026 @ 09:52:57	SMB01-26bb1d907e	-	-	-	Office 365: User downloads a file.
Mar 02, 2026 @ 09:52:57	SMB01-26bb1d907e	-	-	-	Office 365: User downloads a file.
Mar 02, 2026 @ 09:52:57	SMB01-26bb1d907e	-	-	-	Office 365: User downloads a file.
Mar 02, 2026 @ 09:52:57	SMB01-26bb1d907e	-	-	-	Office 365: User downloads a file.
Mar 02, 2026 @ 09:52:57	SMB01-26bb1d907e	-	-	-	Office 365: User downloads a file.
Mar 02, 2026 @ 09:52:57	SMB01-26bb1d907e	-	-	-	Office 365: User downloads a file.

location	office365
input.type	log
data.office365.Workload	OneDrive
data.office365.ApplicationId	08e18876-6177-487e-b8b5-cf950c1e598c
data.office365.DoNotDistributeEvent	true
data.office365.ListServerTemplate	700
data.office365.Operation	FileDownloaded

data.office365.Subscription	Audit.SharePoint
data.office365.CreationTime	Mar 02, 2026 @ 07:49:01
data.office365.CorrelationId	27fbfba1-1080-f000-c157-d29d8993ed18
data.office365.HighPriorityMediaProcessing	false
data.office365.SourceFileName	p*****2.png
data.office365.UserType	0
data.office365.EventSource	SharePoint
data.office365.IsManagedDevice	false
data.office365.SiteUrl	***
data.office365.ApplicationDisplayName	SharePoint Online Web Client Extensibility
data.office365.RecordType	6
data.office365.Version	1
data.office365.ClientIP	79.16.175.126

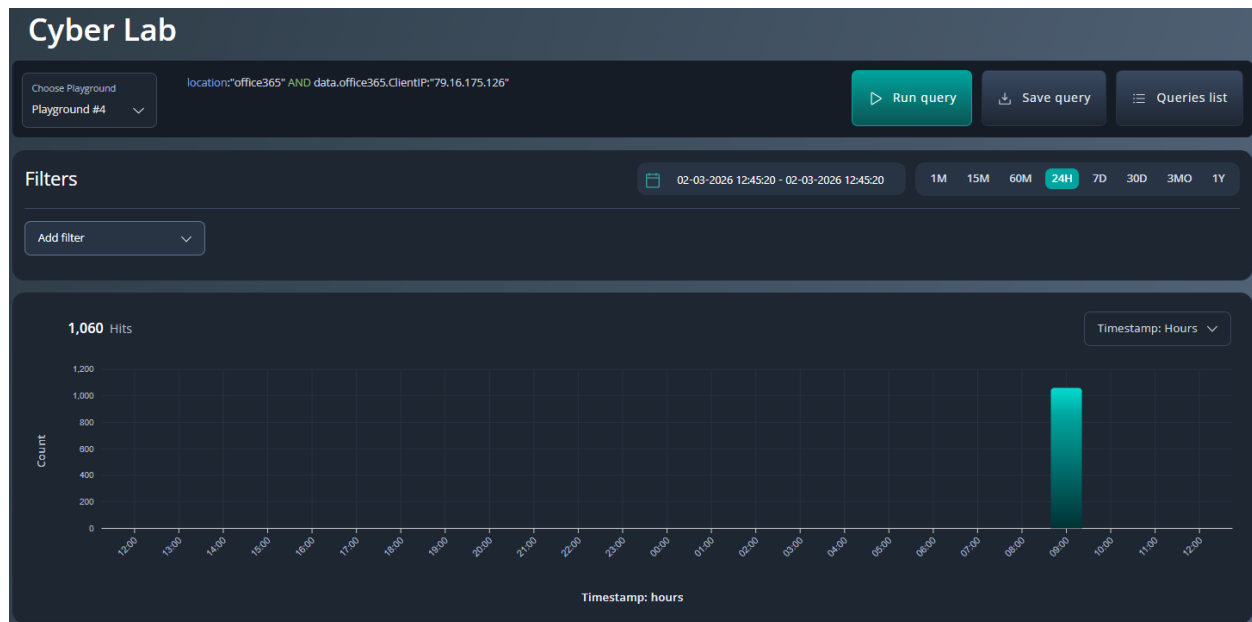
2. Evenimente de la o anumită adresă IP:

- Această interogare va returna toate evenimentele/operațiunile generate în Microsoft Office 365 pentru o anumită adresă IP.

Interogare:

location:"office365" AND data.office365.ClientIP:"79.16.175.126"

Rezultat:



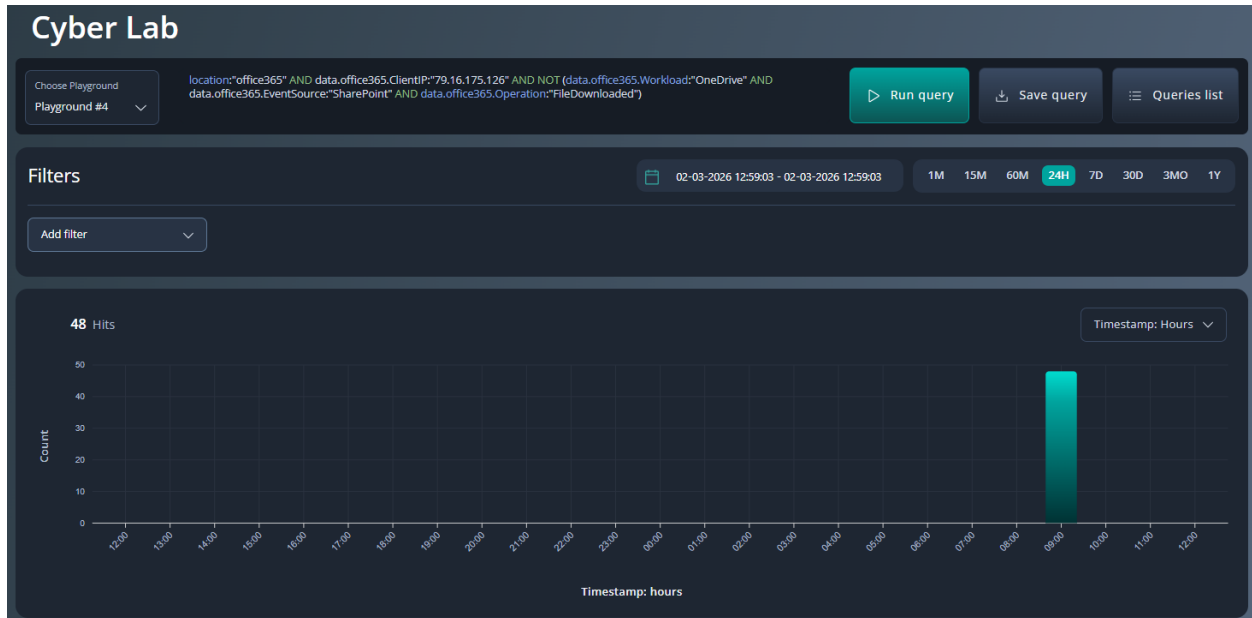
3. Evenimente de la o anumită adresă IP care ignoră descărcarea fișierelor din OneDrive:

- Similar cu precedentul, returnează evenimentele/operațiunile generate în Microsoft Office 365 pentru o anumită adresă IP, excluzând evenimentele/operațiunile despre descărcarea fișierelor în OneDrive.

Interogare:

location:"office365" AND data.office365.ClientIP:"79.16.175.126" AND NOT (data.office365.Workload:"OneDrive" AND data.office365.EventSource:"SharePoint" AND data.office365.Operation:"FileDownloaded")

Rezultat:



Mar 02, 2026 @ 09:47:53	SMB01-26bb1d907e	-	-	-	Office 365: Secure Token Service (STS) logon events in Azure Active Directory.
Mar 02, 2026 @ 09:47:53	SMB01-26bb1d907e	-	-	-	Office 365: Secure Token Service (STS) logon events in Azure Active Directory.
Mar 02, 2026 @ 09:46:41	SMB01-26bb1d907e	-	-	-	Office 365: Planner TaskListRead operation.
Mar 02, 2026 @ 09:46:39	SMB01-26bb1d907e	-	-	-	Office 365: Secure Token Service (STS) logon events in Azure Active Directory.
Mar 02, 2026 @ 09:46:39	SMB01-26bb1d907e	-	-	-	Office 365: Secure Token Service (STS) logon events in Azure Active Directory.

data.office365.ResultStatus	Success
data.office365.ErrorNumber	0
data.office365.Operation	UserLoggedIn
data.office365.DeviceProperties.Name	OS
data.office365.DeviceProperties.Value	<input checked="" type="checkbox"/> <input type="checkbox"/> Windows10
data.office365.DeviceProperties.Name	BrowserType
data.office365.DeviceProperties.Value	Chrome
data.office365.DeviceProperties.Name	IsCompliant
data.office365.DeviceProperties.Value	False
data.office365.DeviceProperties.Name	IsCompliantAndManaged
data.office365.DeviceProperties.Value	False
data.office365.DeviceProperties.Name	SessionId
data.office365.DeviceProperties.Value	002e1cca-c50d-edd1-e377-d6f4d5bb7aea
data.office365.Actor.ID	d17abecb-1ead-43e4-92dc-50859b75f792
data.office365.Actor.Type	0
data.office365.Actor.ID	cbc6fb898c@dom08.SMB01
data.office365.Actor.Type	5
data.office365.ActorIpAddress	79.16.175.126
data.office365.OrganizationId	a1614e78-239b-696c-bb3d-3f5eb1d90138
data.office365.Version	1
data.office365.ExtendedProperties.Name	ResultStatusDetail
data.office365.ExtendedProperties.Value	Redirect
data.office365.ExtendedProperties.Name	UserAgent
data.office365.ExtendedProperties.Value	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
data.office365.ExtendedProperties.Name	RequestType
data.office365.ExtendedProperties.Value	OAuth2:Authorize
data.office365.Subscription	Audit.AzureActiveDirectory

data.Type	AADRiskUsers
data.UserDisplayName	*****
data.OperationName	Risky user
data.CorrelationId	d17abecb-1ead-43e4-92dc-50859b75f792
data.TenantId	c874cc34-cd65-9bb5-3bdf-adcb23db5a64
data.IsDeleted	false
data.RiskDetail	none
data.RiskLastUpdatedDateTime	Mar 02, 2026 @ 07:44:56
data.IsProcessing	false
data.RiskLevel	low
data.UserPrincipalName	cbc6fb998c@dom08.SMB01
data.TimeGenerated	Mar 02, 2026 @ 07:44:56
data.RiskState	atRisk
data.azure_tag	azure-log-analytics
data.log_analytics_tag	AADRiskUsers

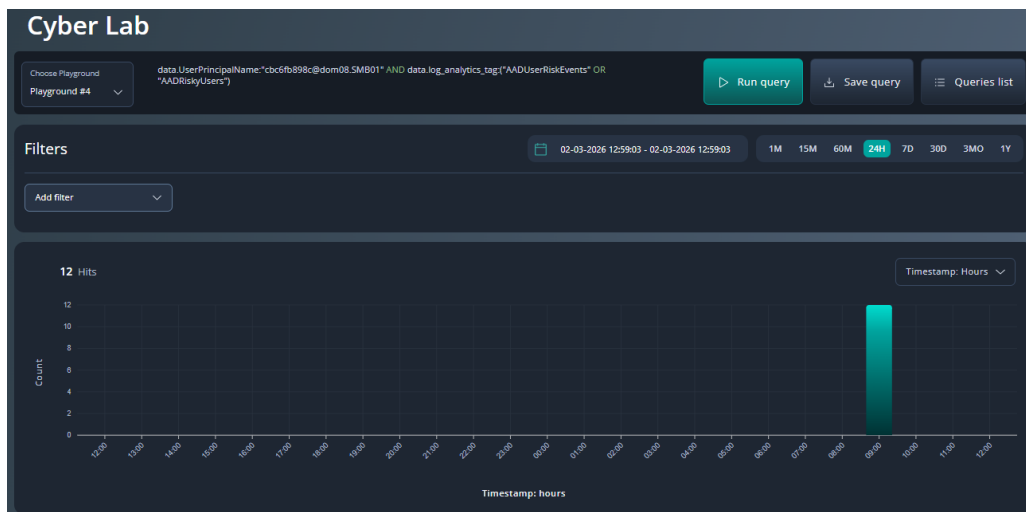
4. Evenimente privind utilizatorul de risc:

- Această interogare returnează evenimente din Azure despre riscul detectat atunci când un utilizator s-a conectat dintr-o locație diferită sau când este detectată o locație nouă în comparație cu cea obișnuită și generează o alertă de risc în contul de utilizator.

Interogare:

```
data.UserPrincipalName:"cbc6fb898c@dom08.SMB01" AND  
data.log_analytics_tag>("AADUserRiskEvents" OR "AADRiskyUsers")
```

Rezultat:



data.DisplayName	D*****
data.AdditionalInfo.Key	userAgent
data.AdditionalInfo.Value	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
data.AdditionalInfo.Key	mitreTechniques
data.AdditionalInfo.Value	T1090.003,T1078
data.CorrelationId	54cf6dc3-ee3b-4805-a5f6-3f1a0ce6f4ad
data.DetectedDateTime	Mar 02, 2026 @ 07:38:33
data.IpAddress	64.145.79.69
data.Location	{\"city\":\"New York\", \"state\":\"New York\", \"countryOrRegion\":\"US\", \"geoCoordinates\":{\"altitude\":0, \"latitude\":40.75891, \"longitude\":-73.37902}}
data.RiskState	remediated
data.RiskDetail	userPassedMFADrivenByRiskBasedPolicy
data.RiskLevel	low
data.Source	IdentityProtection
data.UserId	96f1b0ef-f2c5-cd5a-2263-66e34899b325
data.TimeGenerated	Mar 02, 2026 @ 07:40:30
data.TenantId	c874ce34-cd65-9bb5-3bdf-adcb23db5a64
data.Id	93ce129da112866eaf9ba02d6ee6bb5e444dca3c9e3c89b45ed62740da9ca999
data.LastUpdatedDateTime	Mar 02, 2026 @ 07:40:30
data.UserPrincipalName	cbc6fb898c@dom08.SMB01
data.OperationName	User Risk Detection
data.Type	AADUserRiskEvents
data.azure_tag	azure-log-analytics
data.log_analytics_tag	AADUserRiskEvents
data.Activity	signin

5. Evenimente privind crearea proceselor generate de browsere:

- Această interogare va returna toate evenimentele cu ID-ul „1” (Sysmon: Process Creation) generate de următoarele browsere: Chrome, Firefox, Opera, Brave.

Interogare:

```
data.win.system.eventID:1 AND rule.description:(*Process* AND *creation* AND (*Brave* OR *Chrome* OR *Firefox* OR *Opera*)) AND data.win.system.providerName:"Microsoft-Windows-Sysmon"
```

Rezultat:



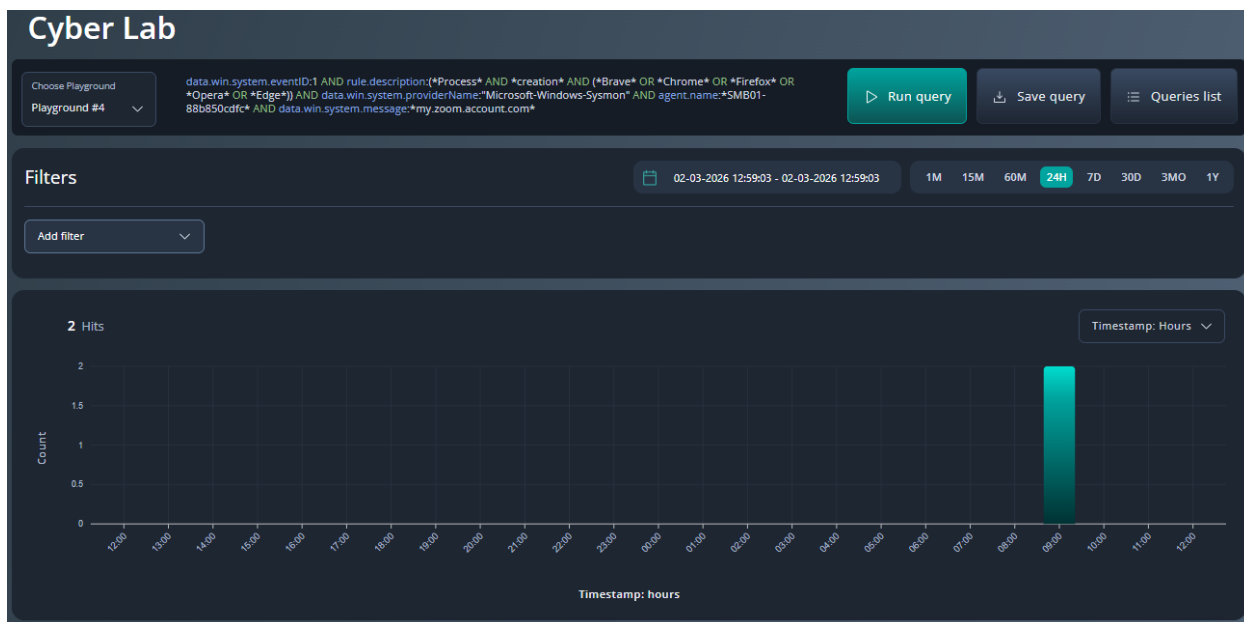
6. Evenimente privind crearea de procese generate de browsere pe un anumit dispozitiv și o anumită adresă URL:

- Similar cu ultima interogare, aceasta va returna evenimente referitoare la „Crearea procesului” de către un browser, cu diferența că această interogare va returna pentru un anumit dispozitiv și pentru o adresă URL specifică accesată de utilizatorul final.

Interogare:

```
data.win.system.eventID:1 AND rule.description:(*Process* AND *creation* AND (*Brave* OR *Chrome* OR *Firefox* OR *Opera* OR *Edge*)) AND data.win.system.providerName:"Microsoft-Windows-Sysmon" AND agent.name:*SMB01-88b850cdfc* AND data.win.system.message:*my.zoom.account.com*
```

Rezultat:



data.win.eventdata.company	Brave Software, Inc.
data.win.eventdata.hashes	MDS=CE19EAF58B0D33762DFE76D3938D999_5HA256=0FFEB1260BE7D19C2CAF20780E82C84AB32F526A234E658335936811028DB368_IMPHASH=7096BEE3CDF08C3616FFC732973FEDF2
data.win.eventdata.parentUser	dom01\365754f81a
data.win.eventdata.processGuid	{edada798-3d66-69a5-d115-000000003d00}
data.win.eventdata.image	C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe
data.win.eventdata.description	Brave Browser
data.win.eventdata.originalFileName	brave.exe
data.win.eventdata.user	dom01\365754f81a
data.win.eventdata.logonGuid	{edada798-3704-69a5-29f0-841000000000}
data.win.eventdata.processId	38820
data.win.eventdata.fileVersion	238.207.72.80
data.win.eventdata.currentDirectory	C:\Program Files\BraveSoftware\Brave-Browser\Application\
data.win.eventdata.logonId	0x1084f029
data.win.eventdata.parentImage	C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe
data.win.eventdata.parentCommandLine	"C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" --single-argument http://my.zoom.account.com/?rid=ZuRPFGL
data.win.eventdata.product	Brave Browser
data.win.eventdata.commandLine	"C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" --type=crashpad-handler --user-data-dir=C:\Users\365754f81a\AppData\Local\BraveSoftware\Brave-Browser\User Data\ /prefetch-4 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\365754f81a\AppData\Local\BraveSoftware\Brave-Browser\User Data\Crashpad\ --metrics-dir=C:\Users\365754f81a\AppData\Local\BraveSoftware\Brave-Browser\User Data\ --url=https://cr.brave.com --annotation=plat=Win64 --annotation=prod=Brave --annotation=ver=238.207.72.80 --initial-client-data=0x140,0x144,0x148,0x118,0x14c,0x7ffb4ac1f0e8,0x7ffb4ac1f0f4,0x7ffb4ac1f100
data.win.eventdata.terminalSessionId	2
data.win.eventdata.integrityLevel	Medium
data.win.eventdata.parentProcessGuid	{edada798-3d66-69a5-d015-000000003d00}
data.win.eventdata.parentProcessId	16564
location	EventChannel
rule.level	3
rule.description	Sysmon - Event 1: Process creation Brave Browser

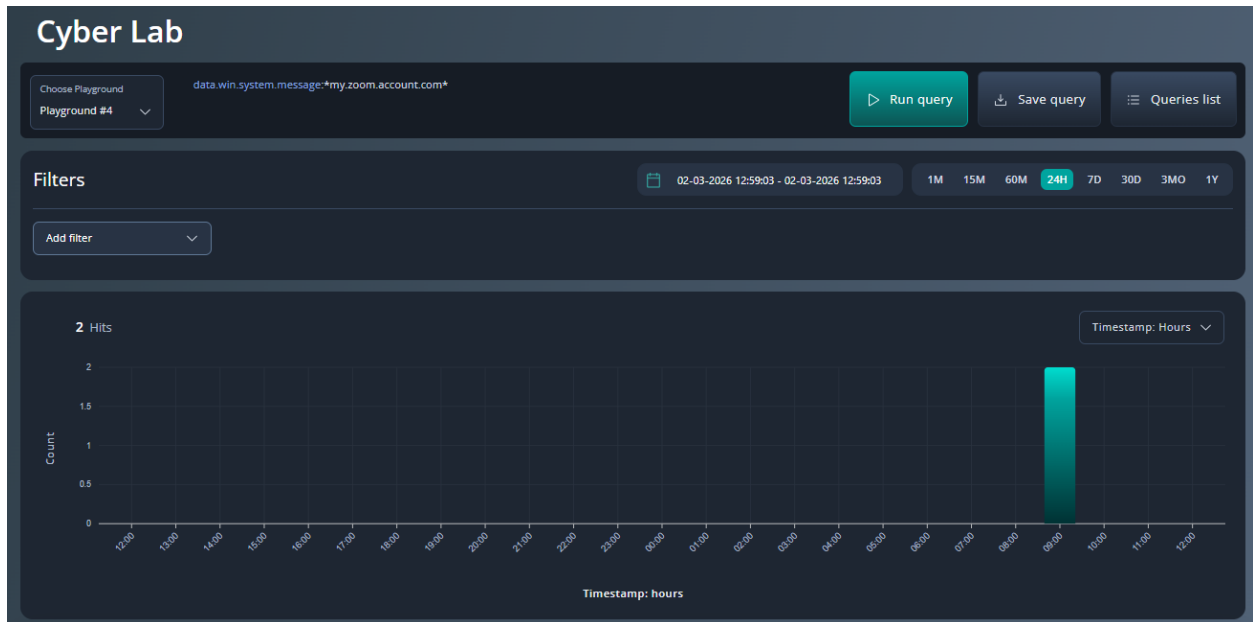
7. Toate evenimentele care au în context o valoare specifică:

- În cazul nostru, va returna toate evenimentele care au o adresă URL specifică în context.

Interogare:

`data.win.system.message:*my.zoom.account.com*`

Rezultat:



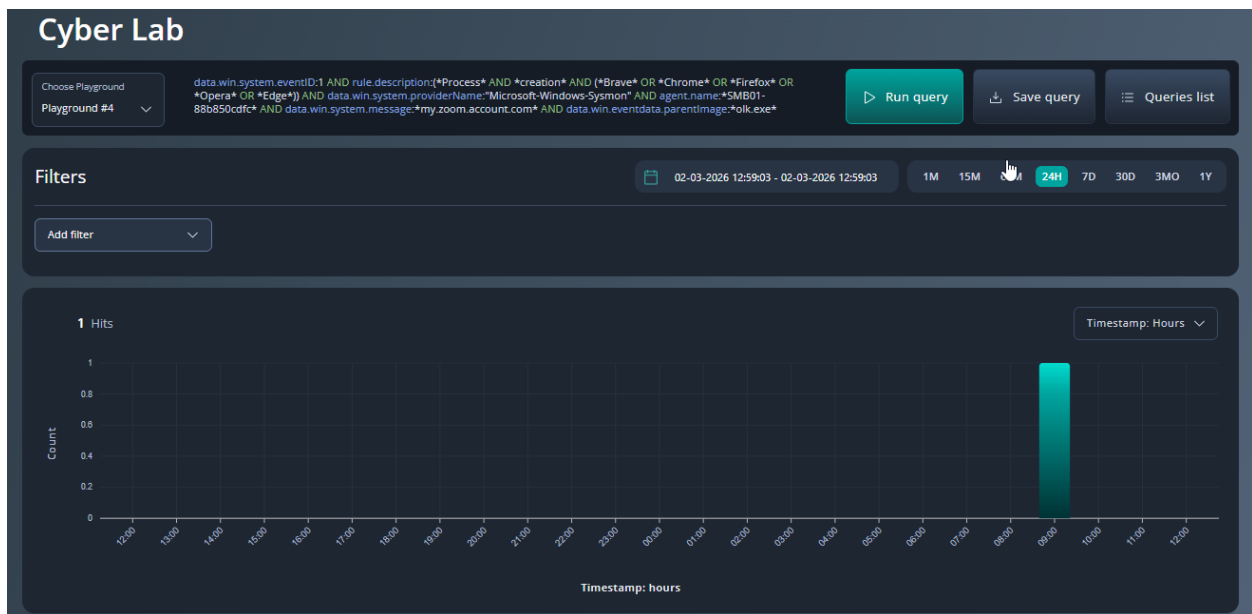
8. Evenimente privind crearea de procese generate de browsere pe un anumit dispozitiv și o anumită adresă URL - Outlook pentru procesul părinte:

- Similar cu celelalte 2 interogări, va returna evenimente referitoare la „Crearea procesului” generate pe dispozitivul afectat pentru o anumită adresă URL și dacă procesul părinte a fost generat de Outlook.

Interogare:

```
data.win.system.eventID:1 AND rule.description:(*Process* AND *creation* AND (*Brave* OR *Chrome* OR *Firefox* OR *Opera* OR *Edge*)) AND data.win.system.providerName:"Microsoft-Windows-Sysmon" AND agent.name:*SMB01-88b850cdfc* AND data.win.system.message:*my.zoom.account.com* AND data.win.eventdata.parentImage:*olk.exe*
```

Rezultat:



data.win.eventdata.user	dom01\365754f81a
data.win.eventdata.hashes	MDS=CE19EAF5880D33762BDFE76D3938D999.SHA256=0FFEB1260BE7D19C2CAF20780E82C84AB32F526A234E658335936811028DB368,IMPHASH=7096BEE3CDF08C3616FFC732973FEDF2
data.win.eventdata.parentImage	C:\Program Files\WindowsApps\Microsoft.OutlookForWindows_1.2026.213.100_x64_8wekyb3d8bbwe\olk.exe
data.win.eventdata.utcTime	2026-03-02 07:33:58.735
data.win.eventdata.processGuid	{edada798-3d66-69a5-d015-000000003d00}
data.win.eventdata.company	Brave Software, Inc.
data.win.eventdata.originalFileName	brave.exe
data.win.eventdata.integrityLevel	Medium
data.win.eventdata.parentProcessGuid	{edada798-38cf-69a5-a214-000000003d00}
data.win.eventdata.parentProcessId	18248
data.win.eventdata.fileVersion	238.207.72.80
data.win.eventdata.product	Brave Browser
data.win.eventdata.commandLine	"C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" --single-argument http://my.zoom.account.com/?rid=ZuRPFGI
data.win.eventdata.currentDirectory	C:\WINDOWS\System32\
data.win.eventdata.terminalSessionId	2
data.win.eventdata.parentCommandLine	"C:\Program Files\WindowsApps\Microsoft.OutlookForWindows_1.2026.213.100_x64_8wekyb3d8bbwe\olk.exe"
data.win.eventdata.parentUser	dom01\365754f81a

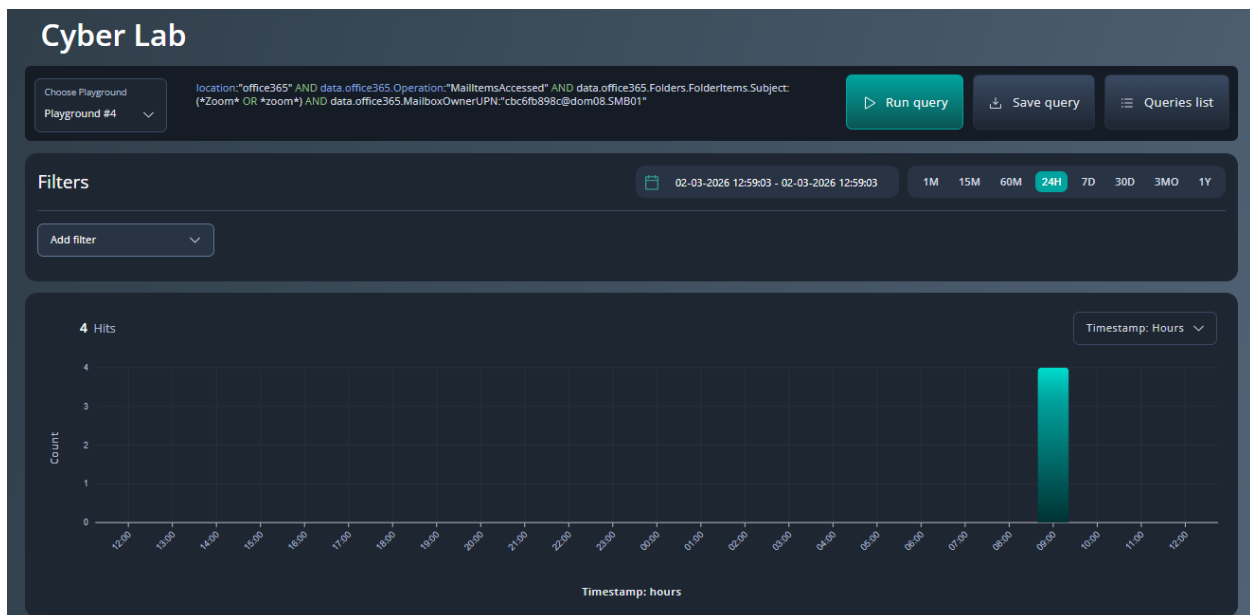
9. Evenimente despre e-mailuri accesate pentru e-mailuri care au o anumită valoare în subiect și pentru un anumit utilizator:

- Această interogare va returna toate evenimentele care fac referire la e-mailuri accesate de un utilizator compromis și care au în subiect o referință la o valoare din adresa URL care s-a constatat a fi accesată din Outlook.

Interogare:

```
location:"office365" AND data.office365.Operation:"MailItemsAccessed" AND data.office365.Folders.FolderItems.Subject:(*Zoom* OR *zoom*) AND data.office365.MailboxOwnerUPN:"cbc6fb898c@dom08.SMB01"
```

Rezultat:



data.office365.Operation	MailItemsAccessed
data.office365.UserType	5
data.office365.ExternalAccess	false
data.office365.LogonUserSid	S-1-5-87-974536641-122911913-015996381-7842632
data.office365.MailboxGuid	49f5cbbd-0978-7421-5f27-2310e05c2d10
data.office365.MailboxOwnerUPN	<input checked="" type="checkbox"/> <input type="checkbox"/> cbc6fb898c@dom08.SMB01
data.office365.RecordType	50
data.office365.LogonType	0
data.office365.Id	f367f9dc-b221-43ec-89a6-1b3afacd001c
data.office365.Workload	Exchange
data.office365.AppId	82d8ab62-be52-a567-14ea-1616c4ee06c4
data.office365.OrganizationName	SMB01.onmicrosoft.com
data.office365.ResultStatus	Succeeded
data.office365.OrganizationId	a1614e78-239b-696c-bb3d-3f5eb1d90138
data.office365.ClientInfoString	Client=REST;Client=RESTSystem;
data.office365.OriginatingServer	VI2PR07MB11007 (15.20.4200.000)
data.office365.Folders.Id	LgAAAABtajUQhjtSYQZedlvV5IHAQBskr/A2CCfQY/zzm0JqnYAAAAAEMAAAB
data.office365.Folders.Path	\Inbox
data.office365.Folders.FolderItems.Subject	Action Required to Reset Your Zoom Account Password
data.office365.Folders.FolderItems.ClientRequestId	bc06abff-8d91-4762-a133-d63248518221