



ALTAY TAKIMI

SOC SIMULATOR WRITE-UP RAPORU

Hazırlayan : Efe Körün

Tarih : 28.02.2025

INTRODUCTION TO PHISHING SENARYOSU

Alert ID 1000

1000	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 12:53	Awaiting action	
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	03/01/2025 09:50:49.119					
subject:	You've Won a Free Trip to Hat Wonderland - Click Here to Claim					
sender:	boone@hatventuresworldwide.online					
recipient:	miguel.odonnell@tryhatme.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	inbound					

SIEM'e gelen 1000 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. Bu alert, "You've Won a Free Trip to Hat Wonderland - Click Here to Claim" konu başlığıyla, "boone@hatventuresworldwide.online" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta başlığı incelendiğinde, şirketin adına ("Hat") atıfta bulunarak "Hat Wonderland" gibi var olmayan bir yer hakkında bir çekiliş kazanıldığı iddia edilmektedir.

"hatventuresworldwide.online" uzantılı bir adres kullanılması ve ".online" gibi sık kullanılmayan bir domain tercih edilmesi şüpheli görünmektedir

E-postayı kullanıcıyı tıklamaya teşvik eden bir phishing yöntemi olarak nitelendirebiliriz. Bu yüzden "TRUE POSITIVE" kategorisinde değerlendirilmeli fakat bir üst kademeye bildirmek gerekmemektedir.

Alert ID 1001

1001	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 12:54	Awaiting action	
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	03/01/2025 09:51:49.119					
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping					
sender:	maximilian@chicmillinerydesigns.de					
recipient:	michelle.smith@tryhatme.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	inbound					

SIEM'e gelen 1001 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. Bu alert, "VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping" konu başlığıyla, "maximilian@chicmillinerydesigns.de" adresinden "michelle.smith@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta başlığı incelendiğinde, şirketin adına ("Hat") atıfta bulunarak VIP bir tatil tesisinde konaklama vaadiyle, sadece kargo ücreti ödemesi karşılığında bir teklif sunulduğu görülmektedir.

Bu tür e-postalar genellikle finansal bilgileri ele geçirmeye yönelik olup, kurumsal kullanıcıları hedef alan sosyal mühendislik saldırılarının yaygın bir örneğidir. Bu yüzden bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1002

1002	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 12:56	Awaiting action
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 09:53:58.119				
event.code:	1				
host.name:					
process.name:	taskhostw.exe				
process.pid:	3897				
process.parent.pid:	3902				
process.parent.name:	svchost.exe				
process.command_line:	taskhostw.exe NGCKeYPregen				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1002 id'li alertimiz şüpheli bir process oluşturma işlemi hakkında tetiklenmiştir.

Bu alert, Windows'un olağan işlemlerinden biri olan "svchost.exe"nin, yine Windows'un olağan bir bileşeni olan "taskhostw.exe" ile "taskhostw.exe NGCKeYPregen" komutunun çalıştırıldığını gösteriyor.

NGCKeYPregen parametresi, **Windows Hello** veya **FIDO güvenlik anahtarları** ile ilişkili bir işlemidir ve Windows'un kimlik doğrulama anahtarlarını önceden oluşturmaya yardımcı olur.

Bu yüzden bu olağan işlem "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1003

1003	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 12:57	Awaiting action
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	03/01/2025 09:55:15.119				
subject:	FWD: Convention Registration Now Open: Hat Trends and Insights				
sender:	support@tryhatme.com				
recipient:	warner@yahoo.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	outbound				

SIEM'e gelen 1003 id'li alertimiz şirket içersiniden bir çalışan mailinin bir dış e-postaya yanıt vermesi hakkında tetiklenmiştir.

E-posta, "FWD: Convention Registration Now Open: Hat Trends and Insights" konu başlığıyla, şirket domaini (support@tryhatme.com) üzerinden bir harici adrese (warner@yahoo.com) iletilmiş. Bu e-posta, şirket çalışanın bir konferans kaydı hakkında dış bir adrese yanıt vermesi olduğu için "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1004

1004	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 12:59	Awaiting action	2+
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	03/01/2025 09:56:53.119					
subject:	Force update fix					
sender:	yani.zubair@tryhatme.com					
recipient:	michelle.smith@tryhatme.com					
attachment:	forceupdate.ps1					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	internal					

SIEM'e gelen 1004 ID'li alertimiz şirket içi bir e-postada şüpheli bir ek dosya hakkında tetiklenmiştir.

Bu alert, bir e-postada şüpheli bir ek dosya bulunduğunu göstermektedir. Açıklamada "Şüpheli bir ek dosya e-postada bulundu. Kötü amaçlı olup olmadığını belirlemek için daha fazla inceleme yapın" denilmektedir.

E-posta "Force update fix" konu başlığıyla, şirket içi adreslerden "yaril.zubair@tryhatme.com" göndericisinden "michelle.smith@tryhatme.com" alıcısına gönderilmiştir. Ekte "[forceupdate.ps1](#)" adlı bir PowerShell dosyası bulunmaktadır.

Gönderilen dosya ekine, IT Departmanında çalışan "yaril.zubair@tryhatme.com" tarafından gönderildiği için sistemdeki bir güncelleme hakkında diyebiliriz. Bu yüzden bu olağan işlem **"FALSE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1005

1005	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 12:59	Awaiting action	2+
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	03/01/2025 09:57:13.119					
subject:	Shrinking Hat Sale: Tiny Hats for Extraordinary People					
sender:	sophie.j@tryhatme.com					
recipient:	eileen@gmail.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	outbound					

SIEM'e gelen 1005 ID'li alertimiz dış ağdaki bir adrese gönderilen şüpheli bir e-posta hakkında tetiklenmiştir.

E-posta "Shrinking Hat Sale: Tiny Hats for Extraordinary People" konu başlığıyla, şirket içi "sophie.j@tryhatme.com" adresinden harici "eileen@gmail.com" adresine gönderilmiştir. Bu e-posta, şirket çalışanının şapkalarda indirim olduğu hakkında dış bir adrese yanıt vermesi olduğu için **"FALSE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1006

1006	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 13:01	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	03/01/2025 09:59:10.119				
subject:	Hats Off to Savings: Discounted Vacation Packages Just for You!				
sender:	tim@chicmillinerydesigns.de				
recipient:	invoice@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1006 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir.

E-posta "Hats Off to Savings: Discounted Vacation Packages Just for You!" konu başlığıyla, şirket dışı "tim@chicmillinerydesigns.de" adresinden "invoice@tryhatme.com" alıcısına gönderilmiştir.

E-posta içeriğinin konusu (indirimli tatil paketleri) şirketin normal iş akışıyla ilgisiz görünmektedir. Ayrıca, "invoice@" adlı faturalar hakkındaki bir mail adresine gönderilmiş olması da bu mailin bir spam reklamı olduğunu göstermektedir. Bu yüzden bu alert "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1007

1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 13:04	Awaiting action
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:	emails				
timestamp:	03/01/2025 10:01:33.119				
subject:	Important: Pending Inviocel				
sender:	john@hatmakereurope.xyz				
recipient:	michael.ascot@tryhatme.com				
attachment:	ImportantInvoice-Febrary.zip				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1007 ID'li alertimiz şüpheli bir e-posta eki hakkında tetiklenmiştir.

E-posta "Important: Pending Inviocel!" konu başlığıyla, şirket dışı "john@hatmakereurope.xyz" adresinden "michael.ascot@tryhatme.com" alıcısına gönderilmiştir. Ekte "ImportantInvoice-Febrary.zip" adlı bir sıkıştırılmış dosya bulunmaktadır.

Bu e-posta birçok şüpheli özellik taşımaktadır:

- Başlıkta panik ve aciliyet yaratmaya çalışan "Important!" gibi bir ibare bulunmaktadır.
- Göndericinin alan adı (.xyz uzantılı) şüphelidir
- Konu başlığında "Inviocel" şeklinde yazım hatası mevcuttur
- Ek dosya adında "Febrary" şeklinde yazım hatası mevcuttur
- Sıkıştırılmış .zip dosyaları genellikle kötü amaçlı yazılımları gizlemek için kullanılır

Bu mailin gerçek bir phishing olduğu belirlendiği için bu alert "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

PHISHING UNFOLDING SENARYOSU

Alert ID 1000

1000	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:14
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.			
datasource:	emails			
timestamp:	02/28/2025 12:12:14.299			
subject:	You've Won a Free Trip to Hat Wonderland - Click Here to Claim			
sender:	boone@hatventuresworldwide.online			
recipient:	miguel.odonnell@tryhatme.com			
attachment:	None			
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.			
direction:	inbound			

SIEM'e gelen 1000 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. Bu alert, "You've Won a Free Trip to Hat Wonderland - Click Here to Claim" konu başlığıyla, "boone@hatventuresworldwide.online" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta başlığı incelendiğinde, şirketin adına ("Hat") atıfta bulunarak "Hat Wonderland" gibi var olmayan bir yer hakkında bir çekiliş kazanıldığı iddia edilmektedir.

"hatventuresworldwide.online" uzantılı bir adres kullanılması ve ".online" gibi sık kullanılmayan bir domain tercih edilmesi şüpheli görünmektedir.

E-postayı kullanıcıyı tıklamaya teşvik eden bir phishing yöntemi olarak nitelendirebiliriz. Bu yüzden "TRUE POSITIVE" kategorisinde değerlendirilmeli fakat bir üst kademeye bildirmek gerekmemektedir.

Alert ID 1001

1001	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:15
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.			
datasource:	emails			
timestamp:	02/28/2025 12:13:14.299			
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping			
sender:	maximilian@chicmillinerydesigns.de			
recipient:	michelle.smith@tryhatme.com			
attachment:	None			
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.			
direction:	inbound			

SIEM'e gelen 1001 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. Bu alert, "VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping" konu başlığıyla, "maximilian@chicmillinerydesigns.de" adresinden "michelle.smith@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta başlığı incelendiğinde, şirketin adına ("Hat") atıfta bulunarak VIP bir tatil tesisinde konaklama vaadiyle, sadece kargo ücreti ödemesi karşılığında bir teklif sunulduğu görülmektedir.

Bu tür e-postalar genellikle finansal bilgileri ele geçirmeye yönelik olup, kurumsal kullanıcıları hedef alan sosyal mühendislik saldırılarının yaygın bir örneğidir. Bu yüzden bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1002

1002	Suspicious Parent Child Relationship	Low	Process	Feb 28th 2025 at 15:17	Closed
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	02/28/2025 12:15:23.299				
event.code:	1				
host.name:					
process.name:	taskhostw.exe				
process.pid:	3897				
process.parent.pid:	3902				
process.parent.name:	svchost.exe				
process.command_line:	taskhostw.exe NGCKKeyPregen				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1002 id'li alertimiz şüpheli bir process oluşturma işlemi hakkında tetiklenmiştir.

Bu alert, Windows'un olağan işlemlerinden biri olan "svchost.exe"nin, yine Windows'un olağan bir bileşeni olan "taskhostw.exe" ile "taskhost.exe NGCKKeyPregen" komutunun çalıştırıldığını gösteriyor.

NGCKKeyPregen parametresi, **Windows Hello** veya **FIDO güvenlik anahtarları** ile ilişkili bir işlemidir ve Windows'un kimlik doğrulama anahtarlarını önceden oluşturmaya yardımcı olur.

Bu yüzden bu olağan işlem "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1003

1003	Reply to suspicious email.	Low	Phishing	Feb 28th 2025 at 15:19	
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:16:40.299				
subject:	FWD: Convention Registration Now Open: Hat Trends and Insights				
sender:	support@tryhatme.com				
recipient:	warner@yahoo.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	outbound				

SIEM'e gelen 1003 id'li alertimiz şirket içersiniden bir çalışan mailinin bir dış e-postaya yanıt vermesi hakkında tetiklenmiştir.

E-posta, "FWD: Convention Registration Now Open: Hat Trends and Insights" konu başlığıyla, şirket domaini (support@tryhatme.com) üzerinden bir harici adrese (warner@yahoo.com) iletilmiş. Bu e-posta, şirket çalışanının bir konferans kaydı hakkında dış bir adrese yanıt vermesi olduğu için "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1004

1004	Suspicious Attachment found in email	Low	Phishing	Feb 28th 2025 at 15:20	Closed	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	02/28/2025 12:18:18.299					
subject:	Force update fix					
sender:	yani.zubair@tryhatme.com					
recipient:	michelle.smith@tryhatme.com					
attachment:	forceupdate.ps1					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	internal					

SIEM'e gelen 1004 ID'li alertimiz şirket içi bir e-postada şüpheli bir ek dosya hakkında tetiklenmiştir.

Bu alert, bir e-postada şüpheli bir ek dosya bulunduğunu göstermektedir. Açıklamada "Şüpheli bir ek dosya e-postada bulundu. Kötü amaçlı olup olmadığını belirlemek için daha fazla inceleme yapın" denilmektedir.

E-posta "Force update fix" konu başlığıyla, şirket içi adreslerden "yari.zubair@tryhatme.com" göndericisinden "michelle.smith@tryhatme.com" alıcısına gönderilmiştir. Ekte "[forceupdate.ps1](#)" adlı bir PowerShell dosyası bulunmaktadır.

Bu alertin daha detaylı değerlendirilmesi gerekmektedir. Çünkü:

1. E-posta şirket içi iki çalışan arasında gerçekleşmiştir
2. IT departmanında çalışanlar arasında teknik dosya paylaşımı normal bir durum olabilir
3. "Force update fix" konusu meşru bir sistem güncellemesi olabilir

Gönderilen dosya ekine, IT Departmanında çalışan "yari.zubair@tryhatme.com" tarafından gönderildiği için sistemdeki bir güncelleme hakkında diyebiliriz. Bu yüzden bu olağan işlem "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1005

1005	Reply to suspicious email.	Low	Phishing	Feb 28th 2025 at 15:21	Awaiting action	
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	02/28/2025 12:18:38.299					
subject:	Shrinking Hat Sale: Tiny Hats for Extraordinary People					
sender:	sophie.j@tryhatme.com					
recipient:	eileen@gmail.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	outbound					

SIEM'e gelen 1005 ID'li alertimiz dış ağdaki bir adrese gönderilen şüpheli bir e-posta hakkında tetiklenmiştir.

E-posta "Shrinking Hat Sale: Tiny Hats for Extraordinary People" konu başlığıyla, şirket içi "sophie.j@tryhatme.com" adresinden harici "eileen@gmail.com" adresine gönderilmiştir.

Bu e-posta, şirket çalışanın şapkalarda indirim olduğu hakkında dış bir adrese yanıt vermesi olduğu için "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir

Alert ID 1006

1006	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:23	
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:20:35.299				
subject:	Hats Off to Savings: Discounted Vacation Packages Just for You!				
sender:	tim@chicmillinerydesigns.de				
recipient:	invoice@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1006 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir.

E-posta "Hats Off to Savings: Discounted Vacation Packages Just for You!" konu başlığıyla, şirket dışı "tim@chicmillinerydesigns.de" adresinden "invoice@tryhatme.com" alıcısına gönderilmiştir.

E-posta içeriğinin konusu (indirimli tatil paketleri) şirketin normal iş akışıyla ilgisiz görünmektedir. Ayrıca, "invoice@" adlı faturalar hakkındaki bir mail adresine gönderilmiş olması da bu mailin bir spam reklamı olduğunu göstermektedir.

Bu yüzden bu alert "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1007

1007

Suspicious Attachment found in email

^

Low

Phishing

Feb 28th 2025 at 15:25

Awaiting action

Description:

datasource:

timestamp:

subject:

sender:

recipient:

attachment:

content:

direction:

A suspicious attachment was found in the email. Investigate further to determine if it is malicious.

emails

02/28/2025 12:22:58.299

Important: Pending Invoice!

john@hatmakereurope.xyz

michael.ascot@tryhatme.com

ImportantInvoice-Febrary.zip

The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.

inbound

SIEM'e gelen 1007 ID'li alertimiz şüpheli bir e-posta eki hakkında tetiklenmiştir.

E-posta "Important: Pending Invoice!" konu başlığıyla, şirket dışı "john@hatmakereurope.xyz" adresinden "michael.ascot@tryhatme.com" alıcısına gönderilmiştir. Ekte "ImportantInvoice-Febrary.zip" adlı bir sıkıştırılmış dosya bulunmaktadır.

Bu e-posta birçok şüpheli özellik taşımaktadır:

- Başlıkta panik ve aciliyet yaratmaya çalışan "Important!" gibi bir ibare bulunmaktadır.
- Göndericinin alan adı (.xyz uzantılı) şüphelidir
- Konu başlığında "Invoice" şeklinde yazım hatası mevcuttur
- Ek dosya adında "Febrary" şeklinde yazım hatası mevcuttur
- Sıkıştırılmış .zip dosyaları genellikle kötü amaçlı yazılımları gizlemek için kullanılır

Bu mailin gerçek bir phishing olduğu belirlendiği için bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1008

1008	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:26	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:24:14.299				
subject:	Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize				
sender:	le@trendymillineryco.me				
recipient:	ceo@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1008 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir.

E-posta "Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize" konu başlığıyla, şirket dışı "le@trendymillineryco.me" adresinden doğrudan CEO'ya "ceo@tryhatme.com" gönderilmiştir.

Bu e-posta açıkça bir phishing girişimi göstermektedir:

- "Million-Dollar Prize" gibi gerçek dışı vaatler içeren bir konu başlığı
- .co.me uzantılı şüpheli bir alan adı
- Doğrudan CEO'yu hedef alan bir saldırı (whaling/spear-phishing tekniği)

Bu mailin gerçek bir phishing olduğu belirlendiği için bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1009

1009	Reply to suspicious email.	Low	Phishing	Feb 28th 2025 at 15:30	Awaiting action
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:27:38.299				
subject:	Unlock Ancient Hat Secrets with This Ancient Pyramid Scheme				
sender:	yani.zubair@tryhatme.com				
recipient:	conor@modernmillinerygroup.online				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	outbound				

SIEM'e gelen 1009 ID'li alertimiz şüpheli bir e-postaya yanıt verilmesi hakkında tetiklenmiştir.

E-posta "Unlock Ancient Hat Secrets with This Ancient Pyramid Scheme" konu başlığıyla, şirket "yani.zubair@tryhatme.com" adresinden "conor@modernmillinerygroup.online" alıcısına gönderilmiştir.

- Çalışan şüpheli bir e-postaya yanıt vermiştir
- Konu başlığında açıkça "Pyramid Scheme" (piramit şeması) ifadesi yer almaktadır
- .online uzantılı şüpheli bir alan adına yanıt gönderilmiştir
- Bir çalışan potansiyel olarak dolandırıcılık girişimine dahil olmuş olabilir.

Bu mailin gerçek bir şirket içi bilgi sızdırması olarak belirlendiği için bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1010

1010	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:31	
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:29:22.299				
subject:	Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!				
sender:	gamble@fashionindustrytrends.xyz				
recipient:	miguel.odonnell@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1010 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir.


E-posta "Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!" konu başlığıyla, şirket dışı "gamble@fashionindustrytrends.xyz" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilmiştir.

Bu e-posta birçok şüpheli özellik taşımaktadır:

- "FREE" ve "Now!" gibi tipik phishing tekniklerinde kullanılan aciliyet ve bedava teklif kelimeleri
- .xyz uzantılı güvenilir olmayan bir alan adı
- Gönderici adında "gamble" kelimesinin yer alması
- Şirket adımızla (tryhatme) ilişkili "Hat-Themed Vacation" gibi özelleştirilmiş içerik ile güven oluşturmaya çalışma.

Bu mailin gerçek bir phishing olduğu belirlendiği için bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1011

1011	Reply to suspicious email.	^	Low	Phishing	Feb 28th 2025 at 15:33	Awaiting action	
Description:		An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:		emails					
timestamp:		02/28/2025 12:31:04.299					
subject:		Double Your Hat Collection with These Easy Tricks!					
sender:		armaan.terry@tryhatme.com					
recipient:		stark@modernmillinerygroup.online					
attachment:		None					
content:		The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:		outbound					

SIEM'e gelen 1011 ID'li alertimiz şüpheli bir e-postaya yanıt verilmesi hakkında tetiklenmiştir.

E-posta "Double Your Hat Collection with These Easy Tricks!" konu başlığıyla, şirket içi "armaan.terry@tryhatme.com" adresinden şüpheli dış adres "stark@modernmillinerygroup.online" alıcısına gönderilmiştir.

Bu durum ciddi bir güvenlik ihlali olarak değerlendirilmelidir:

- Çalışan şüpheli bir .online uzantılı alan adına e-posta göndermiştir
- Bu e-posta şüpheli bir domain (.modernmillinerygroup.online) ile iletişim kurmuştur
- Bu, şirket içinde organize bir güvenlik ihlali olabileceğini göstermektedir

Alert ID 1012

1012	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:34	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:31:42.299				
subject:	Hot Singles in Your Area Want to Buy Hats From You - Act Now!				
sender:	sharp@hatsonthetise.online				
recipient:	miguel.odonnell@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

E-posta "Hot Singles in Your Area Want to Buy Hats From You - Act Now!" konu başlığıyla, şirket dışı "sharp@hatsonthetise.online" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilmiştir.

Bu e-posta tipik bir spam/phishing e-postası özellikleri taşımaktadır:

- "Hot Singles in Your Area" gibi klasik spam/oltalama ifadeleri içermektedir
- "Act Now!" ifadesi ile aciliyet yaratmaya çalışmaktadır
- .online uzantılı şüpheli bir alan adından gönderilmiştir

Alert ID 1013

1013	Suspicious Attachment found in email	Low	Phishing	Feb 28th 2025 at 15:35	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:	emails				
timestamp:	02/28/2025 12:33:13.299				
subject:	RE: Force update fix				
sender:	michelle.smith@tryhatme.com				
recipient:	yani.zubair@tryhatme.com				
attachment:	forceupdate.ps1				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	internal				

SIEM'e gelen 1013 ID'li alertimiz şirket içi bir e-postada şüpheli bir ek dosya hakkında tetiklenmiştir.

E-posta "RE: Force update fix" konu başlığıyla, şirket içi "michelle.smith@tryhatme.com" adresinden "yani.zubair@tryhatme.com" adresine gönderilmiştir. Ekte "forceupdate.ps1" adlı bir PowerShell dosyası bulunmaktadır.

Bu alertin daha detaylı deęerlendirilmesi gerekmektedir. Çünkü:

- E-posta şirket ii iki alıřan arasında gerekleřmiřtir
- IT departmanında alıřanlar arasında teknik dosya paylařımı normal bir durum olabilir
- "Force update fix" konusu meřru bir sistem gncellemesi olabilir

Gnderilen dosya ekine, IT Departmanında alıřan "michelle.smith@tryhatme.com" tarafından gnderildięi iin sistemdeki bir gncelleme hakkında diyebiliriz. Bu yzden bu olaęan iřlem "FALSE POSITIVE" kategorisinde deęerlendirilmelidir.

Alert ID 1014

1014

Suspicious email from external domain.

Low

Phishing

Feb 28th 2025 at 15:36

Awaiting action

Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:	emails
timestamp:	02/28/2025 12:33:41.299
subject:	Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize
sender:	elle@headwearinnovations.online
recipient:	liam.espinoza@tryhatme.com
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	inbound

SIEM'e gelen 1014 ID'li alertimiz řüpheli bir dıř domain'den gelen bir e-posta hakkında tetiklenmiřtir.

E-posta "Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize" konu bařlıęıyla, řüpheli "elle@headwearinnovations.online" adresinden "liam.espinoza@tryhatme.com" adresine gnderilmiřtir. E-posta konusu ve gnderen domain incelendięinde tipik phishing denemesi olduęu grlmektedir. "Piyango bileti" ve "Milyon dolarlık dl" ifadeleri sosyal mhendislik saldırılarında sıka kullanılan cazibe unsurlarıdır. Ayrıca ".online" uzantılı řüpheli bir domaine sahip olması da riski artırmaktadır.

Bu yzden bu alert "TRUE POSITIVE" kategorisinde deęerlendirilmelidir.

Alert ID 1015

1015

Suspicious Parent Child Relationship

Low

Process

Feb 28th 2025 at 15:38

Awaiting action

Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:	sysmon
timestamp:	02/28/2025 12:35:40.299
event.code:	1
host.name:	win-3450
process.name:	TrustedInstaller.exe
process.pid:	3949
process.parent.pid:	3714
process.parent.name:	services.exe
process.command_line:	C:\Windows\servicing\TrustedInstaller.exe
process.working_directory:	C:\Windows\system32\
event.action:	Process Create (rule: ProcessCreate)

SIEM'e gelen 10015 id'li alertimiz şüpheli bir parent-child process oluşturma işlemi hakkında tetiklenmiştir.

Bu alert, Windows'un olağan işlemlerinden biri olan "services.exe"nin, yine Windows'un olağan bir bileşeni olan "TrustedInstaller.exe" işlemini başlattığını gösteriyor.

TrustedInstaller.exe, **Windows Update** veya **Windows Modül Yükleyici** ile ilişkili bir işlemidir ve Windows'un sistem dosyalarını güncellemesine veya yeni bileşenler yüklemesine yardımcı olur.

İşlemin çalıştığı dizinler de (C:\Windows\system32\ ve C:\Windows\servicing) sistemde beklenen normal konumlardır.

Bu yüzden bu olağan işlem **"FALSE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1016

1016	Suspicious Parent Child Relationship	Low	Process	Feb 28th 2025 at 15:39	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	02/28/2025 12:36:39.299					
event.code:	1					
host.name:						
process.name:	TrustedInstaller.exe					
process.pid:	3817					
process.parent.pid:	3922					
process.parent.name:	services.exe					
process.command_line:	C:\Windows\servicing\TrustedInstaller.exe					
process.working_directory:	C:\Windows\system32\					
event.action:	Process Create (rule: ProcessCreate)					

SIEM'e gelen 1016 id'li alertimiz şüpheli bir parent-child process oluşturma işlemi hakkında tetiklenmiştir.

Bu alert, Windows'un olağan işlemlerinden biri olan "services.exe"nin, yine Windows'un olağan bir bileşeni olan "TrustedInstaller.exe" işlemini başlattığını gösteriyor.

TrustedInstaller.exe, **Windows Update** veya **Windows Modül Yükleyici** ile ilişkili bir işlemidir ve Windows'un sistem dosyalarını güncellemesine veya yeni bileşenler yüklemesine yardımcı olur.

İşlemin çalıştığı dizinler de (C:\Windows\system32\ ve C:\Windows\servicing) sistemde beklenen normal konumlardır.

Bu yüzden bu olağan işlem **"FALSE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1017

1017	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:40	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:37:50.299				
subject:	Win a Trip to Hat Disneyland - Magical Memories Await!				
sender:	elle@gmail.com				
recipient:	miguel.odonnell@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1017 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir.

Bu alert, "Win a Trip to Hat Disneyland - Magical Memories Await!" konu başlığıyla, "elle@gmail.com" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta başlığı incelendiğinde, şirketin adına ("Hat") atıfta bulunarak "Hat Disneyland" gibi var olmayan bir yer hakkında bir çekiliş düzenlendiği görülmektedir.

Gmail uzantılı adres kullanılması (elle@gmail.com) tek başına şüpheli olmasa da, kişisel bir e-posta adresinden şirket çalışanlarına gönderilen bu tür ödül/tatil kazanma içerikli e-postalar genellikle sosyal mühendislik girişimleridir.

Bu yüzden bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1018

1018	Suspicious Parent Child Relationship	Low	Process	Feb 28th 2025 at 15:40	Awaiting action
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	02/28/2025 12:38:24.299				
event.code:	1				
host.name:	win-3457				
process.name:	svchost.exe				
process.pid:	3812				
process.parent.pid:	3558				
process.parent.name:	services.exe				
process.command_line:	C:\Windows\system32\svchost.exe -k w sapppx -p				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1018 id'li alertimiz şüpheli bir parent-child process oluşturma işlemi hakkında tetiklenmiştir.

Bu alert, Windows'un temel mimari yapısında standart olarak gerçekleşen bir işlem zincirini göstermektedir: "services.exe" ana servisi tarafından "svchost.exe" servis host sürecinin başlatılması.

Tetiklenen alertteki komut satırı parametreleri "C:\Windows\system32\svchost.exe -k wsappx -p" olarak kaydedilmiştir ki bu, "-k wsappx" servis grubu parametresi Windows Store uygulamaları ve paketlerinin yönetiminden sorumlu normal Windows bileşenini işaret etmektedir.

Sürecin çalıştığı konum (C:\Windows\system32) ve işlem hiyerarşisi, Windows işletim sisteminin beklenen davranışıyla tamamen uyumludur. "Services.exe" Windows'un temel servis yönetim bileşeni olarak çeşitli "svchost.exe" örneklerini belirli parametrelerle başlatacak şekilde tasarlanmıştır. Bu yüzden bu alert **"TRUE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1019

1019	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:43	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:41:19.299				
subject:	FWD: Partner With Us: Exploring Collaboration Opportunities Together				
sender:	barker@yahoo.com				
recipient:	yani.zubair@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1019 ID'li alertimiz şüpheli bir e-posta hakkında tetiklenmiştir.

Bu alert, "FWD: Partner With Us: Exploring Collaboration Opportunities Together" konu başlığıyla, "barker@yahoo.com" adresinden "yani.zubair@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta detaylarına bakıldığında, kişisel bir Yahoo adresinden şirket çalışanına iş birliği teklifinde bulunduğu görülmektedir. Resmi iş tekliflerinin kurumsal adreslerden yapılması beklenirken, kişisel bir e-posta adresi kullanılması şüpheli bir durum olsa da bazı küçük ölçekli işletmeler ve bireysel girişimciler kişisel e-posta adresleri üzerinden iletişim kurabilmektedir. Bu yüzden bu alert **"FALSE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1020

1020	Suspicious Parent Child Relationship	Low	Process	Feb 28th 2025 at 15:45	Awaiting action
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	02/28/2025 12:43:01.299				
event.code:	1				
host.name:					
process.name:	taskhostw.exe				
process.pid:	3557				
process.parent.pid:	3539				
process.parent.name:	svchost.exe				
process.command_line:	taskhostw.exe KEYROAMING				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1020 ID'li alertimiz şüpheli bir süreç ilişkisi hakkında tetiklenmiştir.

"taskhostw.exe", Windows'un yasal bir bileşeni olup, çeşitli sistem görevlerini çalıştırmak için kullanılır. Ancak, "KEYROAMING" parametresiyle çağırılması olağan dışıdır ve daha fazla araştırma gerektirir.

KEYROAMING, Windows'ta yaygın olarak bilinen bir parametre değildir ve özellikle kimlik bilgisi hırsızlığı veya kimlik avı saldırılarında kullanılabilecek potansiyel bir göstergedir. Bu nedenle, saldırıların LSASS gibi kritik süreçlerden şifreleri çalmaya çalışıyor olabileceği göz önünde bulundurulmalıdır. Bu yüzden bu alert **"TRUE POSITIVE"** olabilir.

Alert ID 1021

1021	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:45	Awaiting action
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.				
datasource:	emails				
timestamp:	02/28/2025 12:43:26.299				
subject:	Click Here to Win a Trip to Antarctica with Penguin Hats				
sender:	hickman@fashionindustrytrends.xyz				
recipient:	kyra.flores@tryhatme.com				
attachment:	None				
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.				
direction:	inbound				

SIEM'e gelen 1021 ID'li alert şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. E-posta "Click Here to Win a Trip to Antarctica with Penguin Hats" konu başlığıyla, şirket dışı "hickman@fashionindustrytrends.xyz" adresinden "kyra.flores@tryhatme.com" alıcısına gönderilmiştir.

Bu e-posta birçok şüpheli özellik taşımaktadır:

- "Win a Trip" gibi tipik phishing tekniklerinde kullanılan ücretsiz teklif ifadesi
- .xyz uzantılı güvenilir olmayan bir alan adı
- Şirket adıyla (tryhatme) ilişkili "Penguin Hats" gibi özelleştirilmiş içerik ile güven oluşturmaya çalışma
- "Click Here" ifadesiyle kullanıcıyı bir bağlantıya tıklamaya yönlendirme

Bu mailin phishing girişimi olma olasılığı yüksek olduğundan bu alert **"TRUE POSITIVE"** kategorisinde değerlendirilmelidir ve gerekli önlemler alınmalıdır.

Alert ID 1022

1022	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:47	Awaiting action	+
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	02/28/2025 12:44:36.299					
subject:	Meet Local Singles Who Love Spam Emails - Click to Chat!					
sender:	nguyen@styleaccessorieshub.xyz					
recipient:	miguel.odonnell@tryhatme.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	inbound					

SIEM'e gelen 1022 ID'li alert şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. E-posta "Meet Local Singles Who Love Spam Emails - Click to Chat!" konu başlığıyla, şirket dışı "nguyen@styleaccessorieshub.xyz" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilmiştir.

Bu e-posta birçok şüpheli özellik taşımaktadır:

- "Meet Local Singles" ve "Click to Chat!" gibi tipik spam/phishing tekniklerinde kullanılan ifadeler
- .xyz uzantılı güvenilir olmayan bir alan adı
- Konuda "Spam Emails" ifadesinin bulunması, meşru bir iletişimde kullanılmayacak bir içerik
- "Click to" ifadesiyle kullanıcıyı bir bağlantıya tıklamaya yönlendirme

Bu mail açıkça spam/phishing özellikleri taşıdığından "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir ve gerekli önlemler alınmalıdır.

Alert ID 1023

1023	Network drive mapped to a local drive	Medium	Execution	Feb 28th 2025 at 15:48	Awaiting action	+
Description:	A network drive was mapped to a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.					
datasource:	sysmon					
timestamp:	02/28/2025 12:46:23.299					
event.code:	1					
host.name:	win-3450					
process.name:	net.exe					
process.pid:	5784					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					

SIEM'e gelen 1023 ID'li alert bir ağ sürücüsünün yerel sürücüye eşlendiğini gösteren bir durum hakkında tetiklenmiştir.

Olay "Network drive mapped to a local drive" açıklamasıyla, orta riskli bir "Execution" kategorisinde sınıflandırılmıştır.

Alarmdaki şüpheli unsurlar:

- PowerShell'den başlatılan net.exe komutu (PID: 5784, Üst PID: 3728)
- Komut: "C:\Windows\system32\net.exe" use Z: \FILESRV-01\SSF-FinancialRecords" komutu ile finansal kayıtlar içeren bir klasöre erişim sağlanmaya çalışılmıştır
- İşlem kullanıcının indirmeler klasöründen çalıştırılmıştır.
- Alert açıklamasında belirtildiği gibi "Normalde, bu bir endişe kaynağı değildir, ancak kötü amaçlı olup olmadığını belirlemek için daha fazla araştırma yapın."

Bu olayın, özellikle PowerShell'den başlatılması ve finansal kayıtlara erişim sağlaması nedeniyle **"TRUE POSITIVE"** kategorisinde değerlendirilmesi ve michael.ascot kullanıcısının bu erişim için geçerli bir nedeni olup olmadığının araştırılması gerekmektedir.

Alert ID 1024

1024	Suspicious Parent Child Relationship	Low	Process	Feb 28th 2025 at 15:49	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	02/28/2025 12:47:10.299				
event.code:	1				
host.name:	win-3450				
process.name:	Robocopy.exe				
process.pid:	8356				
process.parent.pid:	3,728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E				
process.working_directory:	Z:\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1024 ID'li alert şüpheli bir işlem ilişkisi hakkında tetiklenmiştir.

Olayın detayları şu şekildedir:

- İşlem Robocopy.exe (PID: 8356) olarak görülmektedir
- Üst işlem powershell.exe (PID: 3,728) tarafından başlatılmıştır
- Komut satırı: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E
- PowerShell tarafından tetiklenen Robocopy komutu, Z: sürücüsünden dosyaların kopyalanması için kullanılmıştır.
- Komutun hedef klasörünün adı "exfiltration" olarak belirlenmiştir.
- /E parametresi alt klasörler dahil tüm dosyaları kopyalamayı sağlar

Bu alert michael.ascot kullanıcısının finansal kayıtları içeren bir sunucudan dosyaları kendi bilgisayarına "exfiltration" adlı bir klasöre kopyaladığını göstermektedir. Bu durum ciddi bir veri sızıntısı girişimi olabilir ve **"TRUE POSITIVE"** olarak değerlendirilmelidir.

Alert ID 1025

1025	Network drive disconnected from a local drive	Medium	Execution	Feb 28th 2025 at 15:49	
Description:	A network drive was disconnected from a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.				
datasource:	sysmon				
timestamp:	02/28/2025 12:47:21.299				
event.code:	1				
host.name:	win-3450				
process.name:	net.exe				
process.pid:	8004				
process.parent.pid:	3728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\net.exe" use Z: /delete				
process.working_directory:	C:\Users\michael.ascot\downloads\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1025 ID'li alert şüpheli bir network bağlantısı kesintisi hakkında tetiklenmiştir.

Olayın detayları şu şekildedir:

- Bir network sürücüsü yerel sürücüden bağlantısı kesilmiştir
- "net.exe use Z: /delete" komutu çalıştırılmıştır
- Komut, PowerShell üzerinden (powershell.exe) başlatılmıştır
- İşlem çalışma dizini: C:\Users\michael.ascot\downloads
- Komut kullanıcının downloads klasöründen çalıştırılmıştır.

Bu olay "**TRUE POSITIVE**" olarak değerlendirilmelidir ve şu adımların atılması önerilir:

Alert ID 1026

1026Suspicious Parent Child Relationship^LowProcessFeb 28th 2025 at 15:50Awaiting action

Description:

A suspicious process with an uncommon parent-child relationship was detected in your environment.

datasource:

sysmon

timestamp:

02/28/2025 12:47:42.299

event.code:

1

host.name:

process.name:

rdpclip.exe

process.pid:

3634

process.parent.pid:

3942

process.parent.name:

svchost.exe

process.command_line:

rdpclip

process.working_directory:

C:\Windows\system32\

event.action:

Process Create (rule: ProcessCreate)

SIEM'e gelen 1026 ID'li alert şüpheli bir parent-child process ilişkisi hakkında tetiklenmiştir.

Bu alert, Windows'un olağan işlemlerinden biri olan "svchost.exe"nin, yine Windows'un olağan bir bileşeni olan "rdpclip.exe" işlemini başlattığını gösteriyor.

rdpclip.exe, **Remote Desktop Protocol** ile ilişkili bir işlemdir ve Windows'un uzak masaüstü bağlantısı sırasında panoya erişim sağlamasına yardımcı olur.

İşlemin çalıştığı dizin de (C:\Windows\system32) sistemde beklenen normal bir konumdur. Bu yüzden bu olağan işlem **"FALSE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1027

1027	Suspicious Parent Child Relationship	High	Process	Feb 28th 2025 at 15:50	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	02/28/2025 12:48:08.299					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	5520					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLfVU3cDIgAAAI.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

SIEM'e gelen 1027 ID'li alert şüpheli bir parent-child process ilişkisi hakkında tetiklenmiştir.

Bu alert, "powershell.exe" işleminin "nslookup.exe" işlemini şüpheli parametrelerle başlattığını gösteriyor.

nslookup.exe, DNS sorgulamaları için kullanılan meşru bir araç olmasına rağmen, komut satırında görülen "UEsDBBQAAAAIANigLfVU3cDIgAAAI.haz4rdw4re.io" parametresi son derece şüphelidir ve muhtemelen bir veri sızıntısı veya komuta kontrol (C2) iletişimine işaret etmektedir.

İşlemin çalıştığı dizinin (C:\Users\michael.ascot\downloads\exfiltration) adında "exfiltration" ifadesinin bulunması ve bu işlemin daha önce aynı kullanıcı tarafından gerçekleştirilen şüpheli ağ sürücüsü bağlantı kesme işlemiyle (ID 1025) ilişkili olması durumu daha da şüpheli hale getirmektedir.

Bu yüzden bu alert **"TRUE POSITIVE"** kategorisinde değerlendirilmelidir

Alert ID 1028

1028	Suspicious Parent Child Relationship	^	High	Process	Feb 28th 2025 at 15:50	● Awaiting action	👤+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	02/28/2025 12:48:08.299						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	3952						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						

SIEM'e gelen 1028 id'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarmda gözlemlenen benzer bir domain yapısını kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişimini göstermektedir. İşlem yine aynı şüpheli dizinde ("C:\Users\michael.ascot\downloads\exfiltration") çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden **"TRUE POSITIVE"** olarak değerlendirilmelidir

Alert ID 1029

1029	Suspicious Parent Child Relationship	^	High	Process	Feb 28th 2025 at 15:50	● Awaiting action	👤+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	02/28/2025 12:48:08.299						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	5432						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						

SIEM'e gelen 1029 ID'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarmlarda gözlemlenen benzer bir domain yapısını (.faz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişiminin devam ettiğini göstermektedir.

İşlem ("C:\Users\michael.ascot\downloads\exfiltration") dizininde çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden "TRUE POSITIVE" olarak değerlendirilmelidir.

Alert ID 1030

1030	Suspicious Parent Child Relationship	High	Process	Feb 28th 2025 at 15:50	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	02/28/2025 12:48:08.299					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3800					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

SIEM'e gelen 1030 ID'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "nLz8nMDy7NzU0SqtSryCmu4OVyprsk.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarmlarda gözlemlenen aynı şüpheli domain yapısını (.faz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişiminin devam ettiğini göstermektedir.

İşlem yine aynı şüpheli dizinde ("C:\Users\michael.ascot\downloads\exfiltration") çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden "TRUE POSITIVE" olarak değerlendirilmelidir.

Alert ID 1031

1031	Suspicious Parent Child Relationship	^	High	Process	Feb 28th 2025 at 15:50	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	02/28/2025 12:48:08.299						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	6604						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" AFBLAwQUAAACAC9oC5XHhIO5R8AAA.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						

SIEM'e gelen 1031 ID'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir. Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "AFBLAwQUAAACAC9oC5XHhIO5R8AAA.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarmlarda gözlemlenen aynı şüpheli domain yapısını (.haz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişiminin devam ettiğini göstermektedir.

İşlem yine aynı şüpheli dizinde ("C:\Users\michael.ascot\downloads\exfiltration") çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden "TRUE POSITIVE" olarak değerlendirilmelidir.

Alert ID 1032

1032	Suspicious Parent Child Relationship	^	High	Process	Feb 28th 2025 at 15:50	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	02/28/2025 12:48:08.299						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	5704						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" AdAAAAHQAAEludmVzdG9yUHJlc2Vu.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						

SIEM'e gelen 1032 ID'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir. Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "AdAAAAHQAAAEIudmVzdG9yUHJlc2Vu.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarlarda gözlemlenen aynı şüpheli domain yapısını (.faz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişiminin devam ettiğini göstermektedir. İşlem yine aynı şüpheli dizinde ("C:\Users\michael.ascot\downloads\exfiltration") çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden **"TRUE POSITIVE"** olarak değerlendirilmelidir.

Alert ID 1033

1033	Suspicious Parent Child Relationship	High	Process	Feb 28th 2025 at 15:50	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	02/28/2025 12:48:08.299					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	5696					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					

SIEM'e gelen 1033 ID'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarlarda gözlemlenen aynı şüpheli domain yapısını (.faz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişiminin devam ettiğini göstermektedir. İşlem yine aynı şüpheli dizinde ("C:\Users\michael.ascot\downloads\exfiltration") çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden **"TRUE POSITIVE"** olarak değerlendirilmelidir.

Alert ID 1034

1034	Suspicious Parent Child Relationship	^	High	Process	Feb 28th 2025 at 15:50	Awaiting action	+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:		sysmon					
timestamp:		02/28/2025 12:48:08.299					
event.code:		1					
host.name:		win-3450					
process.name:		nslookup.exe					
process.pid:		4752					
process.parent.pid:		3728					
process.parent.name:		powershell.exe					
process.command_line:		"C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io					
process.working_directory:		C:\Users\michael.ascot\downloads\exfiltration\					
event.action:		Process Create (rule: ProcessCreate)					

SIEM'e gelen 1034 ID'li bu alarm, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io" parametresi oldukça şüphelidir ve önceki alarmlarda gözlemlenen aynı şüpheli domain yapısını (.haz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 iletişim girişiminin devam ettiğini göstermektedir. İşlem yine aynı şüpheli dizinde ("C:\Users\michael.ascot\downloads\exfiltration") çalışmaktadır, bu da kötü niyetli faaliyetin devam ettiğine işaret etmektedir. Bu yüzden **"TRUE POSITIVE"** olarak değerlendirilmelidir.

Alert ID 1035

1035	Suspicious Parent Child Relationship	^	High	Process	Feb 28th 2025 at 15:50		-
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:		sysmon					
timestamp:		02/28/2025 12:48:24.299					
event.code:		1					
host.name:		win-3450					
process.name:		nslookup.exe					
process.pid:		3700					
process.parent.pid:		3728					
process.parent.name:		powershell.exe					
process.command_line:		"C:\Windows\system32\nslookup.exe" VEhNezE00TczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io					
process.working_directory:		C:\Users\michael.ascot\downloads\					
event.action:		Process Create (rule: ProcessCreate)					

SIEM'e gelen 1035 ID'li güvenlik alarmı, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io" parametresi oldukça şüphelidir ve potansiyel olarak kötü amaçlı domain yapısını (.haz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 (Command and Control) iletişim girişiminin devam ettiğini göstermektedir. İşlem "C:\Users\michael.ascot\downloads" dizininde çalışmaktadır, bu da önceki alarmla aynı kullanıcı hesabında şüpheli aktivitelerin devam ettiğine işaret etmektedir. Bu alarm **"TRUE POSITIVE"** olarak değerlendirilmeli ve acilen incelenmelidir.

Alert ID 1036

1036	Suspicious Parent Child Relationship	High	Process	Feb 28th 2025 at 15:50	Awaiting action
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	02/28/2025 12:48:24.299				
event.code:	1				
host.name:	win-3450				
process.name:	nslookup.exe				
process.pid:	3648				
process.parent.pid:	3728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlIQ==.haz4rdw4re.io				
process.working_directory:	C:\Users\michael.ascot\downloads\				
event.action:	Process Create (rule: ProcessCreate)				

SIEM'e gelen 1036 ID'li güvenlik alarmı, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "powershell.exe" ana işleminin farklı bir "nslookup.exe" alt işlemini şüpheli parametrelerle başlattığını bildiriyor.

Nslookup normalde meşru bir DNS sorgulama aracı olmasına rağmen, komut satırındaki "RmYjEyNGZiMTY1NjZlIQ==.haz4rdw4re.io" parametresi oldukça şüphelidir ve potansiyel olarak kötü amaçlı domain yapısını (.haz4rdw4re.io) kullanmaktadır.

Bu durum, muhtemelen sistematik bir veri sızıntısı veya C2 (Command and Control) iletişim girişiminin devam ettiğini göstermektedir. İşlem "C:\Users\michael.ascot\downloads" dizininde çalışmaktadır, önceki alarmlarla aynı kullanıcı hesabında şüpheli aktivitelerin devam ettiğine işaret ediyor. Bu alarm **"TRUE POSITIVE"** olarak değerlendirilmeli ve acilen incelenmelidir.

Alert ID 1037

1037	Suspicious Parent Child Relationship	^	Low	Process	Feb 28th 2025 at 15:51	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	02/28/2025 12:49:02.299						
event.code:	1						
host.name:	win-3461						
process.name:	svchost.exe						
process.pid:	3816						
process.parent.pid:	3693						
process.parent.name:	services.exe						
process.command_line:	C:\Windows\system32\svchost.exe -k wsappx -p						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						

SIEM'e gelen 1037 id'li alertimiz şüpheli bir parent-child process oluşturma işlemi hakkında tetiklenmiştir.

Bu alert, Windows'un temel mimari yapısında standart olarak gerçekleşen bir işlem zincirini göstermektedir: "services.exe" ana servisi tarafından "svchost.exe" servis host sürecinin başlatılması.

Tetiklenen alertteki komut satırı parametreleri "C:\Windows\system32\svchost.exe -k wsappx -p" olarak kaydedilmiştir ki bu, "-k wsappx" servis grubu parametresi Windows Store uygulamaları ve paketlerinin yönetiminden sorumlu normal Windows bileşenini işaret etmektedir.

Sürecin çalıştığı konum (C:\Windows\system32) ve işlem hiyerarşisi, Windows işletim sisteminin beklenen davranışıyla tamamen uyumludur. "Services.exe" Windows'un temel servis yönetim bileşeni olarak çeşitli "svchost.exe" örneklerini belirli parametrelerle başlatacak şekilde tasarlanmıştır. Bu yüzden bu alert **"TRUE POSITIVE"** kategorisinde değerlendirilmelidir.

Alert ID 1038

1038	Suspicious Parent Child Relationship	^	Low	Process	Feb 28th 2025 at 15:52		-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	02/28/2025 12:50:27.299						
event.code:	1						
host.name:	win-3455						
process.name:	WUDFHost.exe						
process.pid:	3638						
process.parent.pid:	3642						
process.parent.name:	services.exe						
process.command_line:	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{0f14c433-1363-42ce-a9d0-0030e9e775ca} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fd5c32fb-5bb6-4693-82a7-6cec85d58bc4 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-3ba97dd6-3700-4e8a-8921-1e24128d9c7d -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-2a6ae716-7c20-4d0c-97b6-bb3346775edf -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-54470b14-46b9-4c56-abe1-d9b12ef13c5f -LifetimeId:39d16a20-5092-495b-95b9-c7e0ec216f0f -DeviceGroupId: -HostArg:0						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						

SIEM'e gelen 1038 ID'li güvenlik alarmı, şüpheli bir parent-child process ilişkisi tespit edildiğini göstermektedir.

Bu alert "services.exe" ana işleminin "WUDFHost.exe" alt işlemini başlattığını bildiriyor.

WUDFHost.exe (Windows User-Mode Driver Framework Host Process) normalde meşru bir Windows bileşeni olmasına rağmen, komut satırındaki parametreler oldukça karmaşık ve uzun GUID değerleri içermektedir. Komut satırında "-HostGUID:{0f14c433-1363-42ce-a9d0-0030e9e775ca}" ve çeşitli event port isimleri bulunmaktadır.

Windows Driver Framework'ün normal işleyişi kapsamında değerlendirilebilecek bu işlem, bu yüzden bu alert "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1039

1039

Reply to suspicious email.

^

Low

Phishing

Feb 28th 2025 at 15:53

Awaiting action

+

Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:	emails
timestamp:	02/28/2025 12:51:10.299
subject:	You've Won a Free Trip to Hat Wonderland - Click Here to Claim
sender:	liam.espinoza@tryhatme.com
recipient:	sharp@trendymillinery.co.me
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	outbound

SIEM'e gelen 1039 ID'li alertimiz şirket dışından gelen şüpheli bir e-posta hakkında tetiklenmiştir. Bu alert, "You've Won a Free Trip to Hat Wonderland - Click Here to Claim" konu başlığıyla, "sharp@trendymillinery.co.me" adresinden "liam.espinoza@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta başlığı incelendiğinde, şirketin adına ("Hat") atıfta bulunarak "Hat Wonderland" gibi var olmayan bir yer hakkında bir çekiliş kazanıldığı iddia edilmektedir.

"trendymillinery.co.me" uzantılı bir adres kullanılması ve ".co.me" gibi sık kullanılmayan bir domain tercih edilmesi şüpheli görünmektedir

E-postayı kullanıcıyı tıklamaya teşvik eden bir phishing yöntemi olarak nitelendirebiliriz. Bu yüzden "**TRUE POSITIVE**" kategorisinde değerlendirilmeli fakat bir üst kademeye bildirmek gerekmemektedir.

Alert ID 1040

1040	Suspicious Attachment found in email	Low	Phishing	Feb 28th 2025 at 15:54	Awaiting action	+
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	02/28/2025 12:52:27.299					
subject:	Force update fix					
sender:	yani.zubair@tryhatme.com					
recipient:	michelle.smith@tryhatme.com					
attachment:	forceupdate.ps1					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	internal					

SIEM'e gelen 1040 ID'li güvenlik alarmı, şüpheli bir e-posta eki tespit edildiğini göstermektedir.

Bu alarm "FALSE POSITIVE" olarak değerlendirilmelidir. İnceleme sonucunda şu bulgulara ulaşılmıştır: E-posta şirket içi iletişim olarak kaydedilmiş olup, yani.zubair@tryhatme.com adresinden michelle.smith@tryhatme.com adresine gönderilmiştir. Her iki adres de aynı şirket domaininde (tryhatme.com) bulunmaktadır.

E-postanın konusu "Force update fix" şeklinde olup, ekteki "forceupdate.ps1" dosyası BT departmanı tarafından hazırlanan ve düzenli güncelleme işlemlerinde kullanılan meşru bir PowerShell script olduğu doğrulanmıştır.

Bu alarm, PowerShell uzantılı bir dosya içerdiği için otomatik olarak tetiklenmiş olsa da, gönderen bilgileri kontrol edildikten sonra zararlı olmadığı tespit edilmiştir. Bu nedenle "FALSE POSITIVE" olarak kapatılabilir.

Alert ID 1041

1041	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 15:55	Awaiting action	+
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	02/28/2025 12:53:23.299					
subject:	RE: RE: Exploring Alliances: Partnership Discussion at Industry Expo					
sender:	chanel@yahoo.com					
recipient:	miguel.odonnell@tryhatme.com					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	inbound					

SIEM'e gelen 1041 ID'li güvenlik alarmı şüpheli bir e-posta hakkında tetiklenmiştir.

Bu alert, "RE: RE: Exploring Alliances: Partnership Discussion at Industry Expo" konu başlığıyla, "chanel@yahoo.com" adresinden "miguel.odonnell@tryhatme.com" alıcısına gönderilen bir e-postayı göstermektedir.

E-posta detaylarına bakıldığında, Yahoo gibi kişisel bir e-posta servisinden şirket çalışanına iş birliği konusunda yazıldığı anlaşılmaktadır. Konu başlığındaki "RE: RE:" ifadesi, bu iletişimin devam eden bir yazışmanın parçası olduğunu göstermektedir.

E-postada herhangi bir ek bulunmaması ve gönderilen adresin yaygın kullanılan bir e-posta servisi olması dikkate alındığında, bu uyarı "**FALSE POSITIVE**" kategorisinde değerlendirilmelidir.

Alert ID 1044

1044	Reply to suspicious email.	^	Low	Phishing	Feb 28th 2025 at 16:00	👤-
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	02/28/2025 12:58:21.299					
subject:	Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes					
sender:	michelle.smith@tryhatme.com					
recipient:	molina@headtoppersinc.xyz					
attachment:	None					
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.					
direction:	outbound					

SIEM'e gelen 1044 ID'li alertimiz şüpheli bir e-posta yanıtı hakkında tetiklenmiştir.

Bir çalışan "Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes" konu başlığıyla gelen e-postayı yanıtlamıştır. E-posta "michelle.smith@tryhatme.com" adresinden "molina@headtoppersinc.xyz" adresine gönderilmiştir.

Bu e-posta açıkça bir phishing girişimi göstermektedir:

- "Unknown Billionaire Relative" gibi gerçek dışı vaatler içeren bir konu başlığı
- .xyz uzantılı şüpheli bir alan adı
- Çalışanın bu tür şüpheli bir e-postaya yanıt vermesi (sosyal mühendislik tekniğinin başarılı olduğunu gösterir)

Bu mailin gerçek bir phishing olduğu belirlendiği için bu alert "**TRUE POSITIVE**" kategorisinde değerlendirilmelidir.