superadmin@erasmith.com

IPS TRAFFIC ALLOWED(LAST 30 DAYS)_2025-04-23_10-43-03.pdf

EVENT_ID	ACCOUNT NAME	DEVICE HOST NAME	FILE NAME	DEVICE SEVERITY	MESSAGE	IP ADDRESS	CREATION_TIME
4ee47ee0-32bf-41e1-bf84-5d014761d465	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:54:00Z,te:2025-04-21T15:55:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:0f917fc4-07a8-428c-e346-08dd80ecd7da,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3}	None	2025-04-21 15:54:48
34e53f89-cbf0-49b4-ac11-729fd2b32c78	SERGIO@SIGNZOO.COM	None	74048_Proof.jpg	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:23:00Z,EndTimeUtc:2025-04-21T15:24:00Z,TimeGenerated:2025-04-21T15:23:22.71Z,ProcessingEndTime:2025-04-21T15:32:14.1247163Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,SystemAlertId:null,CorrelationKey:3fd9a910-eca3-46ac-8b68-e72b8ca38c7f,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,Files:[{$id:4,Name:74048_Proof.jpg,FileHashes:[{$id:5,Algorithm:SHA256,Value:0DBD63BCA63B361EF12CA93EE75B2A8A227521D68EA63C3A4795DF1FCDE0118A,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:kevingrant@merchantsfleet.com,Urls:[https://www.signzoo.com/,https://sarasotawebsites.com/clients/sz/facebook.png,https://sarasotawebsites.com/clients/sz/LinkedIn.png,https://sarasotawebsites.com/clients/sz/Instagram.png,https://www.facebook.com/SignZoo,https://sarasotawebsites.com/clients/sz/SignZoo_Mascot.png,https://www.instagram.com/SignZoo,https://www.linkedin.com/company/SignZoo],Sender:sergio@signzoo.com,P1Sender:sergio@signzoo.com,P1SenderDomain:signzoo.com,SenderIP:2a00:1450:4864:20::12a,P2Sender:sergio@signzoo.com,P2SenderDisplayName:Sergio Vippolis,P2SenderDomain:signzoo.com,ReceivedDate:2025-04-21T15:14:03,NetworkMessageId:1b8c2729-6e2a-4759-b834-08dd80e71e6c,InternetMessageId:,Subject:WO#74048 - Proof,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Soft fail},{Name:DKIM,Value:Pass},{Name:DMARC,Value:None},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:2f485efb4d6f678f6ee2e4b48d915e74,Source:OATP,FirstSeen:2025-04-21T15:30:35},{$id:6,MailboxPrimaryAddress:kevingrant@merchantsfleet.com,Upn:kevingrant@merchantsfleet.com,AadId:fa715bb7-b57d-420d-b50b-edc3e3c4331a,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:90a97e88de98268e46dc93288c2e02c4,Source:OATP,FirstSeen:2025-04-21T15:30:35}],LogCreationTime:2025-04-21T15:32:14.1403401Z,MachineName:BN8NAM12BG402,SourceTempl	None	2025-04-21 15:32:16
5a92abe0-d329-4ae9-bb78-51315d818ff0	CORP.LOCAL\MARK SIEGEL	M6CCORNFW02-P	None	medium	Suspicious DNS Query	10.11.248.102	2025-03-24 18:46:05
f906b2b7-b720-411c-b50b-39dadf9a824e	M6CUTLDC01-P$	M6CCORNFW02-P	None	medium	Suspicious DNS Query	10.11.96.9	2025-03-24 18:46:05
a95d4f3f-1071-4241-ae69-69d20e4a1bea	UNKNOWN	M6CCORNFW02-P	52.154.164.159/../../../../../../../../../boot.ini	high	SolarWinds Storage Manager AuthenticationFilter Policy Bypass Vulnerability	64.39.98.47	2025-03-28 06:02:44
040f89e0-4de0-4c82-81d7-be1d552cc2bc	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:06:49
fd090190-a473-4a3a-b533-feb5b4f1a4c2	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:06:39
c7fa4baf-5619-4e20-bb15-04467383f6e7	UNKNOWN	M6CCORNFW02-P	sc_layout	critical	WordPress ThemeREX Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:09
02e1a48b-2ee3-412e-99f0-1c3fd7ce3cfd	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:04
eba1e891-ffbf-4bfe-9f12-3553a3cdd5d0	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:29
b9fcaf1f-006b-4b70-b8cf-49fdea05b4f5	UNKNOWN	M6CCORNFW02-P	sc_layout	high	ThemeREX Addons WordPress Plugin Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:09
79edff88-a209-48c1-a767-7a85b28fb8b1	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:19
f956726c-8f30-4854-a360-43dffd829bdc	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:12:44
b4da029e-44b6-4d9c-9b6a-703a1b25ed4a	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:08:54
2fe91e5b-b770-4714-89f9-118abb1d9872	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:59
a12ea07d-4d84-460d-82d8-58578ee31b13	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:54
936140ce-7287-4081-98bd-ed3df088a05a	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:07:44
629cdbeb-5d92-48de-a614-f4cc493eeb13	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:08:09
ccf4007e-5acc-4adc-b53e-26265f7b7fc5	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:08:24
2ee9aa3a-dab4-4c3f-a887-ea8c857e5759	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:08:29
79383454-c757-4aea-8dea-77ce8924bf28	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:09:04
785df2df-09cf-4dd1-968f-7fbf0b12b98e	UNKNOWN	M6CCORNFW02-P	CrashFileDownloadServlet	high	SAP NetWeaver AS JAVA Directory Traversal Vulnerability	64.39.98.47	2025-03-28 06:08:59
0399dfbb-b235-4318-916f-bf6ae2a0b171	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:08:44
693cb635-cead-43a8-a1d9-7745e2fbefac	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:09:24
f73385dc-4281-45b7-aef9-32544f4559ac	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:09:14
e85c059c-e473-4a4d-aa5a-a25553f7c80a	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:09:34
34bc784b-d942-4b51-8e82-bd18a75a92b7	UNKNOWN	M6CCORNFW02-P	translation-table	high	Cisco ASA and FTD Arbitrary File Read Vulnerability	64.39.98.47	2025-03-28 06:09:24
57bb58c5-bd57-4923-84f9-9866c2801641	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:23:00Z,EndTimeUtc:2025-04-21T15:24:00Z,TimeGenerated:2025-04-21T15:23:22.71Z,ProcessingEndTime:2025-04-21T15:27:10.8151196Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,SystemAlertId:null,CorrelationKey:c138f92d-6f2c-4ae1-bdc3-77cc93b3c178,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T15:27:10.8307431Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 15:27:12
b15a4560-d939-4cc9-954c-c6122293a414	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:23:00.0000000Z,te:2025-04-21T15:24:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:013f16e8-102f-422f-e2c4-08dd80e87b2a,wsrt:2025-04-21T15:26:34,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 15:27:04

8bad2a51-a4c4-4ba4-9dd0-44951b751d23	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:23:00Z,te:2025-04-21T15:24:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:64f26cae-3b15-426a-0af1-08dd80e87408,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4}	None	2025-04-21 15:24:33
7325101f-1a4d-4c76-8716-117bdfe89a5d	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-21T15:23:22.3930609Z,te:2025-04-21T15:23:22.3930609Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:sergio@signzoo.com,sip:,imsgid:393c9c86-9501-49ee-a6b3-fabb6fe493d5@PH7PR11MB6796.namprd11.prod.outlook.com,srt:1,trc:kevingrant@MerchantsFleet.com,ms:WO#74048 - Proof,sid:64f26cae-3b15-426a-0af1-08dd80e87408,aii:1b8c2729-6e2a-4759-b834-08dd80e71e6c,md:2025-04-21T15:13:49.2720692Z,etps:SubmissionId:f002b9f6-adfa-4f5c-9fb8-08dd80e8726b,lon:UserSubmission}	None	2025-04-21 15:23:22
8be68632-63aa-4e24-9db8-1ae59045216a	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:23:00Z,te:2025-04-21T15:24:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:64f26cae-3b15-426a-0af1-08dd80e87408,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4}	None	2025-04-21 15:23:22
aebbcfe4-97a8-4dcd-a1d6-88f92a68ebef	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:10:04
d0880194-a877-4208-9fb4-11b88f6ddc19	NOTIFICATIONS@MG.CARDSNACKS3.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T12:51:00Z,EndTimeUtc:2025-04-21T12:52:00Z,TimeGenerated:2025-04-21T12:51:55.9966667Z,ProcessingEndTime:2025-04-21T13:25:06.6429599Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e76f1706-666c-c851-9c6d-08dd80d33802,SystemAlertId:null,CorrelationKey:d5f9acf5-3f52-44ba-a394-e6ba92e8ce05,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=e76f1706-666c-c851-9c6d-08dd80d33802,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:rettisernia@merchantsfleet.com,Upn:rettisernia@merchantsfleet.com,AadId:a65c0711-2063-4f51-adc3-1300bd2cb016,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:8a9f10b68e5e68871b5d653361dcd38e,Source:OATP,FirstSeen:2025-04-21T12:59:58},{$id:4,Recipient:rettisernia@merchantsfleet.com,Urls:[https://www.cardsnacks.com/],Threats:[EmailVolumeAnomaly,EmailVolumeAnomaly,EmailVolumeAnomaly],Sender:notifications@mg.cardsnacks3.com,P1Sender:bounce+489ca9.ba4262-rettisernia=merchantsfleet.com@mg.cardsnacks3.com,P1SenderDomain:mg.cardsnacks3.com,SenderIP:209.61.151.224,P2Sender:notifications@mg.cardsnacks3.com,P2SenderDisplayName:CardSnacks,P2SenderDomain:mg.cardsnacks3.com,ReceivedDate:2025-04-20T10:48:17,NetworkMessageId:a4505378-dfb8-448b-760b-08dd7ff8d96e,InternetMessageId:<20250420104813.bf49b97d38a78143@mg.cardsnacks3.com>,Subject:Reminder: It's Easter - Here's The Perfect Last Minute Gift,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender address list (Safe sender / Blocked sender),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:ce236842423ca476b0c73ab6881abe80,Source:OATP,FirstSeen:2025-04-21T12:59:58},{$id:5,Address:209.61.151.224,Type:ip,Urn:urn:IPEntity:6affcfdba71fc157ada72b9b9099b034,Source:OATP,FirstSeen:2025-04-21T13:02:11},{$id:6,NetworkMessageIds:[bb92f92a-b8b6-49c2-ddb1-08dd7ff8cd17,4185a0c0-89ba-4029-1df6-08dd7ff8c927,ed0c45f3-252d-4a28-b84a-08dd7ff8cd25,a4505378-dfb8-448b-760b-08dd7ff8d96e,4eb3ae3f-	209.61.151.224	2025-04-21 13:25:27
11a91a1a-15c2-4f2a-a654-e798ac8d58e8	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:e76f1706-666c-c851-9c6d-08dd80d33802,f3u:phishing@merchantsfleet.com,ts:2025-04-21T12:51:00.0000000Z,te:2025-04-21T12:52:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:285e3159-9d19-4e10-5376-08dd80d33953,wsrt:2025-04-21T12:54:18,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 13:25:06
43498aee-2d1c-41a0-b238-de4e54f062d5	NOTIFICATIONS@MG.CARDSNACKS3.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T12:51:00Z,EndTimeUtc:2025-04-21T12:52:00Z,TimeGenerated:2025-04-21T12:51:55.9966667Z,ProcessingEndTime:2025-04-21T13:01:54.9885071Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e76f1706-666c-c851-9c6d-08dd80d33802,SystemAlertId:null,CorrelationKey:8f1236b6-2225-475c-bf73-d55884a9a61c,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=e76f1706-666c-c851-9c6d-08dd80d33802,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:rettisernia@merchantsfleet.com,Upn:rettisernia@merchantsfleet.com,AadId:a65c0711-2063-4f51-adc3-1300bd2cb016,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:8a9f10b68e5e68871b5d653361dcd38e,Source:OATP,FirstSeen:2025-04-21T12:59:58},{$id:4,Recipient:rettisernia@merchantsfleet.com,Urls:[https://www.cardsnacks.com/],Sender:notifications@mg.cardsnacks3.com,P1Sender:bounce+489ca9.ba4262-rettisernia=merchantsfleet.com@mg.cardsnacks3.com,P1SenderDomain:mg.cardsnacks3.com,SenderIP:209.61.151.224,P2Sender:notifications@mg.cardsnacks3.com,P2SenderDisplayName:CardSnacks,P2SenderDomain:mg.cardsnacks3.com,ReceivedDate:2025-04-20T10:48:17,NetworkMessageId:a4505378-dfb8-448b-760b-08dd7ff8d96e,InternetMessageId:,Subject:Reminder: It's Easter - Here's The Perfect Last Minute Gift,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,AdditionalActionsAndResults:[Original Delivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender address list (Safe sender / Blocked sender),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:ce236842423ca476b0c73ab6881abe80,Source:OATP,FirstSeen:2025-04-21T12:59:58}],LogCreation Time:2025-04-21T13:01:54.9885071Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	209.61.151.224	2025-04-21 13:01:58
962a674f-7a48-40c9-8041-6cdc509d43ff	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:09:44
4c003186-19ab-4989-9899-4a5c025e9b3a	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T12:51:00Z,EndTimeUtc:2025-04-21T12:52:00Z,TimeGenerated:2025-04-21T12:51:55.9966667Z,ProcessingEndTime:2025-04-21T12:57:05.256078Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e76f1706-666c-c851-9c6d-08dd80d33802,SystemAlertId:null,CorrelationKey:1ecc1bb4-981a-414b-9583-1fbf7df9d5dc,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=e76f1706-666c-c851-9c6d-08dd80d33802,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T12:57:05.256078Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 12:57:10
e710c3e0-4146-4ab5-803e-1189343897ab	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T12:51:00Z,EndTimeUtc:2025-04-21T12:52:00Z,TimeGenerated:2025-04-21T12:51:55.9966667Z,ProcessingEndTime:2025-04-21T12:57:05.256078Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e76f1706-666c-c851-9c6d-08dd80d33802,SystemAlertId:null,CorrelationKey:1ecc1bb4-981a-414b-9583-1fbf7df9d5dc,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=e76f1706-666c-c851-9c6d-08dd80d33802,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T12:57:05.256078Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 12:57:05
c14adae5-8f10-4c5e-a3a6-fd7ebb091461	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:e76f1706-666c-c851-9c6d-08dd80d33802,f3u:phishing@merchantsfleet.com,ts:2025-04-21T12:51:00.0000000Z,te:2025-04-21T12:52:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:285e3159-9d19-4e10-5376-08dd80d33953,wsrt:2025-04-21T12:54:18,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 12:57:02
02bed044-b517-4502-b8f8-a48d0e86279e	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:e76f1706-666c-c851-9c6d-08dd80d33802,f3u:phishing@merchantsfleet.com,ts:2025-04-21T12:51:00Z,te:2025-04-21T12:52:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:49742f4f-d125-4d82-f3ff-08dd80d33886,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96}	None	2025-04-21 12:52:21
95919907-950a-406b-a316-225823aa5283	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-21T12:51:22.9728767Z,te:2025-04-21T12:51:22.9728767Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:notifications@mg.cardsnacks3.com,sip:,imsgid:03bfd7dc-e563-4452-8754-461dc055cf9f@PH0PR11MB4774.namprd11.prod.outlook.com,srt:1,trc:rettisernia@MerchantsFleet.com,ms:Reminder: It's Easter - Here's The Perfect Last Minute Gift,sid:49742f4f-d125-4d82-f3ff-08dd80d33886,aii:a4505378-dfb8-448b-760b-08dd7ff8d96e,md:2025-04-20T10:48:13.2990475Z,etps:SubmissionId:24fbb97d-8c48-4fc8-9c6d-08dd80d33802,lon:UserSubmission}	None	2025-04-21 12:51:56
89cbdbd6-e8e9-4934-94bd-810580b13037	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:e76f1706-666c-c851-9c6d-08dd80d33802,f3u:phishing@merchantsfleet.com,ts:2025-04-21T12:51:00Z,te:2025-04-21T12:52:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:49742f4f-d125-4d82-f3ff-08dd80d33886,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:5ae61c7077678e7369f2008a9bc76a96}	None	2025-04-21 12:51:55
8fa5f6a4-700e-4095-8218-9077794531 20	DEXTER@CHRISTIANMONEYBLOG.NET	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-20T16:15:00Z,EndTimeUtc:2025-04-20T16:16:00Z,TimeGenerated:2025-04-20T16:15:50.4133333Z,ProcessingEndTime:2025-04-20T16:57:23.0170765Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:a43a28d3-793a-97c6-43a4-08dd80269cc9,SystemAlertId:null,CorrelationKey:0b66fdd7-ca77-4f52-ba3b-14094288f0a0,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=a43a28d3-793a-97c6-43a4-08dd80269cc9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:michaelsanchez@merchantsfleet.com,Upn:michaelsanchez@merchantsfleet.com,AadId:2dfb84fc-e9f7-42d3-ba90-041614837699,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:1c5ee3f6a89db6ed3dddf0208c65a8a4,Source:OATP,FirstSeen:2025-04-20T16:25:07},{$id:4,Recipient:michaelsanchez@merchantsfleet.com,Urls:[https://smtpdiamond.com/unsub/eng/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvN,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvN,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbjJD,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbkJt,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbIDD,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbmDt,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQb0ID,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQb1It,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQb2lj,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvN.gif],Sender:dexter@christianmoneyblog.net,P1Sender:dexter@christianmoneyblog.net,P1SenderDomain:christianmoneyblog.net,SenderIP:199.244.73.41,P2Sender:dexter@christianmoneyblog.net,P2SenderDisplayName:Dexter Lyons,P2SenderDomain:christianmoneyblog.net,ReceivedDate:2025-04-20T04:49:13,NetworkMessageId:646255ad-1ba6-45c9-3dbe-08dd7fc69558,InternetMessageId:<472685911745122679810413@DexDell-2023>,Subject:Happy Easter! He is Risen!,AntispamDirection:Inbound,DeliveryAction:DeliveredAsSpam,ThreatDetectionMethods:[FingerPrintMatch],Language:en,DeliveryLocation:JunkFolder,OriginalDeliveryLocation:JunkFolder,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pa	199.244.73.41	2025-04-20 16:57:24
afbf3f1e-727f-4eae-b803-d3f90dae7f3b	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:a43a28d3-793a-97c6-43a4-08dd80269cc9,f3u:phishing@merchantsfleet.com,ts:2025-04-20T16:15:00.0000000Z,te:2025-04-20T16:16:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:09bfdcf7-8ba8-43b0-e2ad-08dd80269e62,wsrt:2025-04-20T16:18:15,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-20 16:57:22
95f23248-2f46-437e-9501-d5a2f8115a21	DEXTER@CHRISTIANMONEYBLOG.NET	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-20T16:15:00Z,EndTimeUtc:2025-04-20T16:16:00Z,TimeGenerated:2025-04-20T16:15:50.4133333Z,ProcessingEndTime:2025-04-20T16:25:49.5833678Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:a43a28d3-793a-97c6-43a4-08dd80269cc9,SystemAlertId:null,CorrelationKey:0944ffc1-7378-45a5-8493-d3d4f75b2f04,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=a43a28d3-793a-97c6-43a4-08dd80269cc9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:michaelsanchez@merchantsfleet.com,Upn:michaelsanchez@merchantsfleet.com,AadId:2dfb84fc-e9f7-42d3-ba90-041614837699,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:1c5ee3f6a89db6ed3dddf0208c65a8a4,Source:OATP,FirstSeen:2025-04-20T16:25:07},{$id:4,Recipient:michaelsanchez@merchantsfleet.com,Urls:[https://smtpdiamond.com/unsub/eng/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvN,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvN,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbjJD,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbkJt,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbIDD,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQbmDt,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQb0ID,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQb1It,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvM5qzS4qaR9ZQb2lj,https://smtpdiamond.com/tracking/qaR9ZwNIAGN5AGx2AGH1BGL2BQpmAvN.gif],Sender:dexter@christianmoneyblog.net,P1Sender:dexter@christianmoneyblog.net,P1SenderDomain:christianmoneyblog.net,SenderIP:199.244.73.41,P2Sender:dexter@christianmoneyblog.net,P2SenderDisplayName:Dexter Lyons,P2SenderDomain:christianmoneyblog.net,ReceivedDate:2025-04-20T04:49:13,NetworkMessageId:646255ad-1ba6-45c9-3dbe-08dd7fc69558,InternetMessageId:<472685911745122679810413@DexDell-2023>,Subject:Happy Easter! He is Risen!,AntispamDirection:Inbound,DeliveryAction:DeliveredAsSpam,ThreatDetectionMethods:[FingerPrintMatch],Language:en,DeliveryLocation:JunkFolder,OriginalDeliveryLocation:JunkFolder,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:P	199.244.73.41	2025-04-20 16:25:50

608ac09a-f2fb-4c54-b4fe-1b3c224eeaea	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-20T16:15:00Z,EndTimeUtc:2025-04-20T16:16:00Z,TimeGenerated:2025-04-20T16:15:50.4133333Z,ProcessingEndTime:2025-04-20T16:20:39.647518Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:a43a28d3-793a-97c6-43a4-08dd80269cc9,SystemAlertId:null,CorrelationKey:8c78a553-f50b-485e-ad65-7542e5e509a9,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=a43a28d3-793a-97c6-43a4-08dd80269cc9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-20T16:20:39.647518Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-20 16:20:39
379f40af-ecf6-4882-bf2a-11c9e34138dd	CORP.LOCAL\KARTIKMIRAJKARJOSHI	M6CCORNFW02-P	None	high	LDAP: User Login Brute Force Attempt	10.11.252.188	2025-04-01 09:26:12
271a7d67-420a-4580-99dc-075a46a9484b	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:a43a28d3-793a-97c6-43a4-08dd80269cc9,f3u:phishing@merchantsfleet.com,ts:2025-04-20T16:15:00Z,te:2025-04-20T16:16:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:0f11cb2a-8ec8-49aa-b7d0-08dd80269d77,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129}	None	2025-04-20 16:16:59
e1ba488e-5509-4025-ae44-748f296c5fbf	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-20T16:15:49.5459792Z,te:2025-04-20T16:15:49.5459792Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:dexter@christianmoneyblog.net,sip:,imsgid:c634ab23-2d1a-4e73-97b4-d5911ced52d4@PH0PR11MB5904.namprd11.prod.outlook.com,srt:1,trc:michaelsanchez@MerchantsFleet.com,ms:Happy Easter! He is Risen!,sid:0f11cb2a-8ec8-49aa-b7d0-08dd80269d77,aii:646255ad-1ba6-45c9-3dbe-08dd7fc69558,md:2025-04-20T04:48:24.2318782Z,etps:SubmissionId:1161da23-5d2d-49a3-43a4-08dd80269cc9,lon:UserSubmission}	None	2025-04-20 16:15:50
145c5f41-2861-4153-ae2f-474c0331042b	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:a43a28d3-793a-97c6-43a4-08dd80269cc9,f3u:phishing@merchantsfleet.com,ts:2025-04-20T16:15:00.0000000Z,te:2025-04-20T16:16:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:0f11cb2a-8ec8-49aa-b7d0-08dd80269d77,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-20 16:15:50
5c1cf7a9-9ea9-40d1-9348-04bb56bbeb70	CORP.LOCAL\STEFHENBOND	M6CCORNFW02-P	None	medium	Suspicious DNS Query	10.11.248.249	2025-04-10 16:43:47
560b0198-b4d5-4d79-b073-c567ec1a7603	HGREGOIRELT-W10$	M6CCORNFW02-P	None	medium	Suspicious DNS Query	10.11.96.9	2025-04-10 16:43:47
07dfc0b1-ad55-4b4b-8287-656c5dc612f9	CORP.LOCAL\STEFHENBOND	M6CCORNFW02-P	None	medium	Suspicious DNS Query	10.11.248.249	2025-04-10 16:43:47
c3ed6f65-1a35-4bbb-9f84-96a6340d5a55	M6CUTLDC02-P$	M6CCORNFW02-P	None	medium	Suspicious DNS Query	10.11.96.8	2025-04-10 16:43:47
baafdcf9-e35a-4ec4-82a5-c6f5e2425ca3	UNKNOWN	M6CCORNFW02-P	20.84.136.112/	medium	AndroxGh0st Scanning Traffic Detection	165.154.235.97	2025-04-08 02:37:54
4ca8eb63-2760-49a9-863e-901aa4b18a0d	UNKNOWN	M6CCORNFW02-P	20.84.136.112/.env	medium	AndroxGh0st Scanning Traffic Detection	165.154.235.97	2025-04-08 02:37:54
929349c3-c1ff-4722-9bda-7bd7fd685980	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	AndroxGh0st Scanning Traffic Detection	157.230.81.223	2025-04-06 22:54:56
7dca20a5-688e-418c-8755-cfcd2628d1f9	UNKNOWN	M6CCORNFW02-P	52.154.164.159/	medium	AndroxGh0st Scanning Traffic Detection	157.230.81.223	2025-04-06 13:54:38
8bee9950-4c83-4a5e-a415-50d74dccdcac	UNKNOWN	M6CCORNFW02-P	.env	medium	AndroxGh0st Scanning Traffic Detection	157.230.81.223	2025-04-05 21:15:38
2f857d61-3003-47b1-b5d6-a4ba080340fc	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	AndroxGh0st Scanning Traffic Detection	157.230.81.223	2025-04-05 21:15:38
876adf71-bc04-4135-84cb-1b86933b2373	UNKNOWN	M6CCORNFW02-P	52.154.164.159/.env	medium	AndroxGh0st Scanning Traffic Detection	157.230.81.223	2025-04-05 12:36:01
f2d8eb79-b489-42cc-aace-bfd59ae4739a	UNKNOWN	M6CCORNFW02-P	52.154.164.159/	medium	AndroxGh0st Scanning Traffic Detection	157.230.81.223	2025-04-05 12:36:01
92fcf73f-4935-40e3-a5b0-416894c0da41	CORP.LOCAL\KARTIKMIRAJKARJOSHI	M6CCORNFW02-P	None	high	LDAP: User Login Brute Force Attempt	10.11.252.188	2025-04-01 09:26:27
319933d9-6725-439b-924a-f6f02add4df7	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:19:44
a71cf490-c544-4917-8c39-10a8ef2a7b15	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:19:34
101363fd-a49d-4b93-8a2f-260ec200e8f7	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:19:24
08eb14f4-c61a-4831-8c7f-fa58fddc1cc0	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:19:14
a67add64-2a57-4d4c-aed6-1eafb3967b99	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:19:04
5b444ff4-d009-403b-a4d3-f01fa9c5b399	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:18:49
1fb5a732-d037-446e-bc0a-0646dd0bf617	UNKNOWN	M6CCORNFW02-P	www.merchantstotalview.com/	high	Shiro Deserialization Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:18:39
4ee763b8-bb6e-4052-a125-e1c9307e8f6c	UNKNOWN	M6CCORNFW02-P	weblogin.cgi	critical	Zyxel Multiple Products Command Injection Vulnerability	64.39.98.47	2025-03-28 06:14:04
4eac175a-b7da-40cf-a95f-cabb4833e6c8	UNKNOWN	M6CCORNFW02-P	passwd	high	aiohttp Directory Traversal Vulnerability	64.39.98.47	2025-03-28 06:13:54
a18bc40e-db2d-4377-b4dc-8ea5a67371a1	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:12:54
f7df7e5b-d161-469a-a116-bab79e13009f	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:12:34
fc903a1a-4210-4d91-832e-23d56102b156	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:12:24
0bab66b9-c8d6-4606-8d3a-314bc51fdccc	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:12:14
ec2f5d48-b2d3-4c9a-97fc-6f32186fe2f9	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:12:04
3b1c8d58-54d6-4a78-ac6a-3b037118f804	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:11:54
f9a0ee1b-ac1c-400c-b4e8-14c132928df2	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:11:44

99461fed-d33a-41ac-924b-c3fdad3f75df	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:11:34
b496eb9b-95d2-4954-b2e8-652d97a821fd	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:11:24
884e2a6d-0db5-4ace-8508-8da2be6d48ea	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:11:14
0f891bb0-638c-48dd-b117-8f0703b4d949	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:11:04
b749f40a-93e4-455f-a71d-2b14575c121c	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:10:54
53ecb8a2-d3d6-49f6-9c8c-431de933701c	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:10:44
cf0548e9-a74a-4129-96a5-b842fa6d9cf6	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:10:34
3bdfc679-8021-4d4e-843c-cb9274a52126	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:10:24
3759233d-4a19-43f2-bfbf-3bddf4194dad	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:10:14
0749ae2e-ca7f-4881-9d12-fc25019 8fbd5	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	64.39.98.47	2025-03-28 06:09:49
2166a6d9-1680-4bb2-af05-17636c985461	UNKNOWN	M6CCORNFW02-P	None	critical	Gh0st.Gen Command and Control Traffic	66.240.205.34	2025-04-15 13:26:40
ff74ed15-602e-46bc-b649-e166a4b135b5	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.35.38	2025-04-15 12:43:05
6c0dbc8a-c511-47a5-b29d-9eda6643bd74	UNKNOWN	M6CCORNFW02-P	20.84.136.118/portal/redlion	medium	ZGrab Application Layer Scanner Detection	20.65.194.143	2025-04-15 10:27:39
e6566bad-7fd2-4c25-bd70-a5d3a41f108a	UNKNOWN	M6CCORNFW02-P	20.84.136.112/portal/redlion	medium	ZGrab Application Layer Scanner Detection	20.65.194.143	2025-04-15 10:27:29
4077a400-eaba-4945-83ad-e78bac961495	UNKNOWN	M6CCORNFW02-P	20.84.136.119/portal/redlion	medium	ZGrab Application Layer Scanner Detection	20.65.194.143	2025-04-15 10:26:29
43e41c20-f500-41c6-b1bd-e8282bdf007d	UNKNOWN	M6CCORNFW02-P	52.154.164.159/portal/redlion	medium	ZGrab Application Layer Scanner Detection	128.203.205.78	2025-04-15 10:20:14
084d3f71-0797-49dd-9fa6-f267ae6548c8	UNKNOWN	M6CCORNFW02-P	redlion	medium	ZGrab Application Layer Scanner Detection	128.203.205.78	2025-04-15 10:20:14
3a48f03e-56c3-46c5-91e8-340f9cdfe389	UNKNOWN	M6CCORNFW02-P	20.84.136.118:443/	medium	ZGrab Application Layer Scanner Detection	20.169.104.255	2025-04-15 09:55:39
b485a0ad-7ba2-4266-9646-c086eb49eef7	UNKNOWN	M6CCORNFW02-P	20.84.136.119:443/	medium	ZGrab Application Layer Scanner Detection	20.169.104.255	2025-04-15 09:53:29
32e3f156-f462-4d1d-941e-fde7174df0a5	UNKNOWN	M6CCORNFW02-P	20.84.136.112:443/	medium	ZGrab Application Layer Scanner Detection	20.169.104.255	2025-04-15 09:53:24
acee7fbd-acfc-43ce-b5f5-10e7d129db1f	UNKNOWN	M6CCORNFW02-P	52.154.164.149:443/	medium	ZGrab Application Layer Scanner Detection	172.202.117.179	2025-04-15 09:48:09
072a46a5-b2ca-493a-804a-90db3714a8e2	UNKNOWN	M6CCORNFW02-P	52.154.164.159:443/	medium	ZGrab Application Layer Scanner Detection	172.202.117.179	2025-04-15 09:47:39
b9ced43f-9921-4253-a150-da386a66df97	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	167.94.138.133	2025-04-15 09:26:29
83f38e9b-f434-43c5-851c-8b8064796a85	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	ZGrab Application Layer Scanner Detection	20.65.194.88	2025-04-15 07:20:08
0ba8ac1d-abf5-45fb-9841-313adca38498	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.34.175	2025-04-15 05:11:38
975cfd73-f551-4d07-bec1-526b642d7057	UNKNOWN	M6CCORNFW02-P	20.84.136.112/	medium	ZGrab Application Layer Scanner Detection	20.171.25.191	2025-04-15 04:13:42
2789fc71-0bda-4f2e-83a7-3f124294f853	UNKNOWN	M6CCORNFW02-P	20.84.136.119/	medium	ZGrab Application Layer Scanner Detection	20.171.25.191	2025-04-15 04:10:52
5b76693f-7fc3-4b7d-9f2f-6c2b34fe74de	UNKNOWN	M6CCORNFW02-P	20.84.136.118/	medium	ZGrab Application Layer Scanner Detection	20.171.25.191	2025-04-15 04:10:42
6ab6486e-0542-41b2-adeb-4bd166e08e28	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	ZGrab Application Layer Scanner Detection	20.83.25.188	2025-04-15 03:58:22
2a3692bc-0288-473f-a78a-41a71d8667aa	UNKNOWN	M6CCORNFW02-P	52.154.164.159/	medium	ZGrab Application Layer Scanner Detection	20.83.25.188	2025-04-15 03:58:12
c56a03ae-a190-4c50-a3ee-2d0238a2963c	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	198.235.24.155	2025-04-15 03:42:42
855970f0-159b-4cec-988b-cfab8ce4761e	UNKNOWN	M6CCORNFW02-P	None	critical	NetWire RAT Command and Control Traffic Detection	157.245.225.41	2025-04-15 03:01:07
2831fd21-ed1f-40a5-b4e1-510f95a7a4e0	UNKNOWN	M6CCORNFW02-P	None	critical	NJRat.Gen Command and Control Traffic	157.245.225.41	2025-04-15 03:01:02
517b10d0-def7-4917-b7b8-00af79ccd3f5	UNKNOWN	M6CCORNFW02-P	None	critical	Gh0st.Gen Command and Control Traffic	157.245.225.41	2025-04-15 03:01:02
2fa9b3ee-440a-479a-be90-ddfdc6e690ff	UNKNOWN	M6CCORNFW02-P	login.esp	critical	Palo Alto Networks GlobalProtect OS Command Injection Vulnerability	216.218.206.68	2025-04-15 01:53:52
a13b73fa-77df-4ed8-ad53-a505b876f2f7	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	147.185.132.52	2025-04-15 01:39:32

0db88c96-39d8-4445-8370-efd7219c4524	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.35.192	2025-04-15 01:15:31
8a7d28ff-5839-4e5f-8381-4cc9dfd097bc	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	47.251.36.190	2025-04-15 01:12:56
d888fbb4-c52a-4a89-bea5-18e2e592db44	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	199.45.154.176	2025-04-14 20:37:20
d7a54c9c-d118-4e7c-b3ca-ee6d7a0c1abd	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	162.142.125.92	2025-04-14 20:30:15
33e8e351-f677-4fac-8f0d-62eff2636afc	UNKNOWN	M6CCORNFW02-P	health	medium	ZGrab Application Layer Scanner Detection	20.171.29.202	2025-04-14 20:07:25
685759ec-d904-413e-b7d6-21334351d956	UNKNOWN	M6CCORNFW02-P	52.154.164.159/actuator/health	medium	ZGrab Application Layer Scanner Detection	20.171.29.202	2025-04-14 20:07:10
9e490943-ab1d-4112-8338-f333d574379f	UNKNOWN	M6CCORNFW02-P	20.84.136.118/actuator/health	medium	ZGrab Application Layer Scanner Detection	20.171.25.180	2025-04-14 19:44:20
4800d890-6834-4452-9275-2278fcf4fc22	UNKNOWN	M6CCORNFW02-P	20.84.136.119/actuator/health	medium	ZGrab Application Layer Scanner Detection	20.171.25.180	2025-04-14 19:42:15
3c00ce74-9215-44d5-b0c1-bc8ec41a4b5c	UNKNOWN	M6CCORNFW02-P	20.84.136.112/actuator/health	medium	ZGrab Application Layer Scanner Detection	20.171.25.180	2025-04-14 19:39:40
bf5df3cd-74db-42c2-8d73-5a349b9162b2	UNKNOWN	M6CCORNFW02-P	None	critical	NJRat.Gen Command and Control Traffic	66.240.205.34	2025-04-14 18:03:29
4290dd8e-ae13-4731-8e74-30825ac2e332	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	162.142.125.94	2025-04-14 16:31:39
993a89e5-3c7c-4536-8fb3-009709c0c98b	UNKNOWN	M6CCORNFW02-P	health	medium	ZGrab Application Layer Scanner Detection	20.65.194.9	2025-04-14 13:48:08
4b065f37-6c32-4d59-99bf-53f98eeef6fc	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:36:38
5561e901-40fa-41f2-9a3e-ce7a0db962fb	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:36:28
95d3caf5-8dc4-4d37-b86a-9e63d915b60b	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:35:33
f224b601-6c24-47d8-9182-bc5c54cb3c6b	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:35:28
70d02fe1-967f-4daf-8c58-2fd0e7d0d505	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:34:28
42862abe-d322-4661-9387-bd1693cd1dbb	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:34:18
487bdfc3-7895-49eb-8adb-202a9dac616a	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:33:23
26996049-57eb-422f-93a1-aab0a2de5893	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:33:13
73e62baf-0dad-47fe-a4ad-cead94bac5db	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:32:18
51f50ccb-99a7-4ec6-b759-4befd5bbd5ca	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:32:13
6a881b3f-581d-42f8-bee3-e12acbd2acc4	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:31:13
3587b990-5673-41cb-ba71-f850c912174a	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:31:08
cc3a5cd4-8915-48ee-8c8c-43fe98c273de	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:30:13
39bc8290-9363-4eea-aa6a-03dbcb7e714c	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:30:03
6a0bd99b-1b96-4f0a-a4cd-d60412d8b3fb	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:29:03
7ab3b498-61a2-4b8b-a986-430fca6202b0	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:28:08
e5f6f63e-d61a-4984-8943-b137ed17a1e3	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:27:58
d49fd48b-41dd-4f98-aef1-db786faaef04	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:27:08
c2658049-ada0-4b7c-bd50-57f380736a75	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:26:58
8cfb2597-3dda-421a-b2d3-9a87ae676c54	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:25:58
013c6524-5580-437c-834f-9c9b0f64b5e1	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:25:48
d905e0ff-6e53-4022-be37-6b3c1a41f4eb	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:24:58
052376ed-61de-4bce-850a-e2361b160932	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:24:48
34a89a3a-f6f1-4fbf-9e3e-f9c6ce84c8a7	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:23:48

1b27b8e1-4327-441a-bd8e-b6a45f0ac9be	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:23:38
2744e094-cf29-4780-ae65-9fcee6609da0	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:22:43
ec73abc8-5cd1-4952-bd88-eb847862e2b5	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:22:38
34b01f23-71e1-4beb-9f57-117d69bf5294	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:21:43
44378793-5e88-4885-bbf5-2fabf5e26e3f	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:21:33
1d80ce6e-925f-4e5d-89af-876ee2e668e8	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:20:38
5074844f-600e-4eee-85f2-94bf0141027c	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:20:33
5685367a-6b61-406d-93d9-1ed07f3c5784	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:19:33
8ac663a7-b578-435d-a6ac-d4571aff9b5a	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:19:23
d02cb127-090a-4785-a183-765d10294c50	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:18:33
9b3b6e53-b23c-4b3d-9274-fc14bc0af1da	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:18:23
4f8435b6-674f-4c33-99b2-d353c0ba2b35	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:17:28
e06cd56c-77af-4140-acd4-3ade3ff3a39e	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:17:28
51023a56-920d-41ae-a258-b62432eb5fc1	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:16:28
0bd4dd5f-2d65-4c34-97af-b074f064f64c	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:16:23
0da50e80-eafb-4efc-a70c-bbccf23c034d	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:15:23
252991b6-77c4-442f-b9f9-79f39dd610d3	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:15:13
335de85e-e143-4dc4-8ceb-53dc591eb03d	UNKNOWN	M6CCORNFW02-P	login.esp	critical	Palo Alto Networks GlobalProtect OS Command Injection Vulnerability	74.82.47.5	2025-04-14 13:14:38
414c35b6-fe61-4c32-9f5c-8dcecad7ca96	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:14:13
38289daa-c1b3-4974-ac66-33eb3ec38fbb	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:14:08
58917e3f-c686-424c-9b63-5851ed153597	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:13:13
113a2e27-5265-4e78-8b05-91d4b4db6a48	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:13:03
e79925b0-064d-4cec-ae08-164910bfc060	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:12:03
61a47bb2-3012-4e91-9486-71367d17797e	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:12:03
48d659b9-d04d-44fe-b1ef-e6c388620959	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:11:13
0cff3e43-3b2e-45f6-bb89-a9f365c76b18	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:10:53
aad79fea-8c5f-441f-959a-199c0d33a206	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:09:58
d7c22348-3cb8-40ef-a6af-f33235dc7e1d	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:09:48
4c2373ad-a5e2-4e1a-a8c7-74df3692852c	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:09:08
b013ed77-2fcd-4382-ba33-d72a9d2a1677	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:08:53
0274ee7c-6a39-4678-b3f5-d1b900ccccc7	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:07:53
910c6c5b-f6ac-463f-bacf-4f0c82cb99e6	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:07:48
bf26ac79-7040-43bc-937f-9ebf1637616f	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:06:48
0a53840a-8ed9-4001-81ad-4c206371cdc5	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:06:38
3adfb4ac-5507-4b79-b7b6-e90b37f55d18	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:05:43
2097ba68-efaf-47ca-9e7f-371377659dea	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:05:33

3643e1ad-9844-4d8f-afac-7f6818b02b87	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:04:53
a204f27b-5cf7-42a-94ff-52fc6d923c99	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:04:53
2d2213d3-e57b-4324-9632-2e380b5db766	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:04:08
de45fac1-6bb1-4de4-b3ef-3e6f510e5067	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:04:03
e41fed57-5f1b-442d-984b-b9ceedcaf162	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:03:13
7dd1581d-7f6c-41b7-8270-e20ff8fb1325	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 13:03:08
47dd0e22-2840-420e-bb46-7b29d0a51129	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	167.94.138.138	2025-04-14 12:05:28
a3ea240f-f2c3-4b36-8092-65c9d50376ef	UNKNOWN	M6CCORNFW02-P	login.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	64.222.98.170	2025-04-14 11:58:18
54f33008-1fb1-4911-ba86-6f9f3b742216	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.35.147	2025-04-14 11:48:53
a10ff295-f06d-4931-a14a-2c965537dde6	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	49.144.24.1	2025-04-14 09:02:17
91f871e3-482f-4aeb-aedb-0bd73e7bb30c	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.34.163	2025-04-14 08:29:47
5124a34b-1e66-4a15-8aa2-ec1e02933f84	UNKNOWN	M6CCORNFW02-P	20.84.136.119/manager/text/list	medium	ZGrab Application Layer Scanner Detection	130.131.163.187	2025-04-14 05:45:21
76618741-240f-45c1-9926-eb480db228b8	UNKNOWN	M6CCORNFW02-P	52.154.164.159/manager/text/list	medium	ZGrab Application Layer Scanner Detection	135.119.93.157	2025-04-14 05:43:56
bf2dcf26-2734-4386-bfa3-25db3c61a85d	UNKNOWN	M6CCORNFW02-P	list	medium	ZGrab Application Layer Scanner Detection	135.119.93.157	2025-04-14 05:43:01
a192b3a3-ad5d-4201-98da-e1a42429764a	UNKNOWN	M6CCORNFW02-P	20.84.136.118/manager/text/list	medium	ZGrab Application Layer Scanner Detection	130.131.163.187	2025-04-14 05:42:31
2b5d5869-7eb8-4eae-b508-05a1e0d51209	UNKNOWN	M6CCORNFW02-P	20.84.136.112/manager/text/list	medium	ZGrab Application Layer Scanner Detection	130.131.163.187	2025-04-14 05:41:51
3ff6eedf-8ea7-47db-9d46-c4cca7c9bce9	UNKNOWN	M6CCORNFW02-P	index.html	medium	ZGrab Application Layer Scanner Detection	172.174.212.107	2025-04-14 05:30:26
9b216baa-a360-4ab6-a2ba-fd277e7edba0	UNKNOWN	M6CCORNFW02-P	52.154.164.159/druid/index.html	medium	ZGrab Application Layer Scanner Detection	172.174.212.107	2025-04-14 05:30:21
1030e423-bcdd-4fad-b595-91bc4fc14a5f	UNKNOWN	M6CCORNFW02-P	20.84.136.112/druid/index.html	medium	ZGrab Application Layer Scanner Detection	20.221.67.31	2025-04-14 05:23:01
108027bb-9def-46fd-9938-33b782669774	UNKNOWN	M6CCORNFW02-P	20.84.136.118/druid/index.html	medium	ZGrab Application Layer Scanner Detection	20.221.67.31	2025-04-14 05:22:21
ad9fc613-3731-4e9c-806e-179b7374b9b5	UNKNOWN	M6CCORNFW02-P	20.84.136.119/druid/index.html	medium	ZGrab Application Layer Scanner Detection	20.221.67.31	2025-04-14 05:20:56
7f626b6d-0a7f-457d-93bf-e85532bde511	UNKNOWN	M6CCORNFW02-P	52.154.164.149:443/	medium	ZGrab Application Layer Scanner Detection	20.163.15.124	2025-04-14 05:06:01
646ed44c-5ea3-4118-bd52-bab094802588	UNKNOWN	M6CCORNFW02-P	52.154.164.159:443/	medium	ZGrab Application Layer Scanner Detection	20.163.15.124	2025-04-14 05:04:26
6e321cbc-deda-4948-806a-c38f3b7de9fb	UNKNOWN	M6CCORNFW02-P	20.84.136.118:443/	medium	ZGrab Application Layer Scanner Detection	172.212.226.201	2025-04-14 04:52:21
e8642ea7-ecad-4b48-8c10-646b6caf2068	UNKNOWN	M6CCORNFW02-P	20.84.136.119:443/	medium	ZGrab Application Layer Scanner Detection	172.212.226.201	2025-04-14 04:51:01
ca9cd8d1-6029-442d-9011-7fbb5856ff7c	UNKNOWN	M6CCORNFW02-P	20.84.136.112:443/	medium	ZGrab Application Layer Scanner Detection	172.212.226.201	2025-04-14 04:50:36
8ffbb6a5-b3e9-453a-a3be-8723b1cf394b	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	20.150.202.209	2025-04-14 04:49:36
125dc8f8-9330-473c-9a2a-0b5a908c11e3	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 04:33:36
b75b7135-6f04-4281-875c-8a9c4e42d439	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 04:32:41
5ca8b90c-3934-431e-a489-475c7b1cb84a	UNKNOWN	M6CCORNFW02-P	getconfig.esp	medium	Palo Alto Networks GlobalProtect Authentication Brute Force Attempt	47.186.23.135	2025-04-14 04:32:31
6d5fde95-23f8-4890-be6e-6117c93ed1eb	UNKNOWN	M6CCORNFW02-P	20.84.136.112/manager/text/list	medium	ZGrab Application Layer Scanner Detection	40.90.232.236	2025-04-14 04:15:16
f06d1df9-2dba-476d-b835-0788cbf594a9	UNKNOWN	M6CCORNFW02-P	20.84.136.119/manager/text/list	medium	ZGrab Application Layer Scanner Detection	40.90.232.236	2025-04-14 04:14:51
75c1a0c2-c2be-43f9-944d-0d5c1186a462	UNKNOWN	M6CCORNFW02-P	20.84.136.118/manager/text/list	medium	ZGrab Application Layer Scanner Detection	40.90.232.236	2025-04-14 04:14:36
53f316f4-1e39-4169-9816-1caa0e0137bd	UNKNOWN	M6CCORNFW02-P	list	medium	ZGrab Application Layer Scanner Detection	48.217.87.249	2025-04-14 04:11:00
6dabbed5-7043-4261-a983-13d264f5a77c	UNKNOWN	M6CCORNFW02-P	52.154.164.159/manager/text/list	medium	ZGrab Application Layer Scanner Detection	48.217.87.249	2025-04-14 04:10:25
854e71fc-8a85-41f9-9f9a-daa78142ec69	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.35.55	2025-04-14 04:00:30

2feef686-6f21-4f1a-9d10-08614024e056	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	147.185.132.69	2025-04-14 02:49:05
1fe00ba4-8ba5-4931-b5d0-f53c026f7459	UNKNOWN	M6CCORNFW02-P	20.84.136.118/hudson	medium	ZGrab Application Layer Scanner Detection	20.127.159.21	2025-04-14 02:40:20
cb2b9258-e39c-421c-848f-211fa3a69e26	UNKNOWN	M6CCORNFW02-P	20.84.136.112/hudson	medium	ZGrab Application Layer Scanner Detection	20.127.159.21	2025-04-14 02:38:40
95c885a2-aca3-45df-8b5b-e64de42e5f7c	UNKNOWN	M6CCORNFW02-P	20.84.136.119/hudson	medium	ZGrab Application Layer Scanner Detection	20.127.159.21	2025-04-14 02:37:30
a97fcf09-110d-46e6-b873-a342aa2f3a76	UNKNOWN	M6CCORNFW02-P	hudson	medium	ZGrab Application Layer Scanner Detection	52.186.182.169	2025-04-14 02:34:25
ebe2cc63-1357-45a0-ba3c-fe24a9da16e6	UNKNOWN	M6CCORNFW02-P	52.154.164.159/hudson	medium	ZGrab Application Layer Scanner Detection	52.186.182.169	2025-04-14 02:32:35
e8fb1709-1582-4741-8989-c9053dae086f	UNKNOWN	M6CCORNFW02-P	list	medium	ZGrab Application Layer Scanner Detection	20.150.204.7	2025-04-14 02:08:45
f57b1e27-e009-42ab-b311-9a3bc16cd105	UNKNOWN	M6CCORNFW02-P	52.154.164.159/manager/text/list	medium	ZGrab Application Layer Scanner Detection	20.150.204.7	2025-04-14 02:07:25
487726c8-578b-4381-9f6e-d1e220d5ef35	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	ZGrab Application Layer Scanner Detection	20.150.202.58	2025-04-14 01:26:40
56c1264d-74c3-4241-8552-aa96ed8479e8	UNKNOWN	M6CCORNFW02-P	20.84.136.119/manager/text/list	medium	ZGrab Application Layer Scanner Detection	20.163.14.222	2025-04-14 01:24:05
950b3db4-8363-464d-aaa1-37ccfb469423	UNKNOWN	M6CCORNFW02-P	20.84.136.118/manager/text/list	medium	ZGrab Application Layer Scanner Detection	20.163.14.222	2025-04-14 01:22:40
9a424210-959a-4e76-b3dd-6cbad8c7c229	UNKNOWN	M6CCORNFW02-P	20.84.136.112/manager/text/list	medium	ZGrab Application Layer Scanner Detection	20.163.14.222	2025-04-14 01:22:05
88332911-b4e2-4020-9fb5-547ec2927f73	UNKNOWN	M6CCORNFW02-P	20.84.136.118/	medium	ZGrab Application Layer Scanner Detection	20.186.236.153	2025-04-14 00:31:19
248fcb09-5b85-49f5-8c4b-2c95eb20e1fe	UNKNOWN	M6CCORNFW02-P	20.84.136.112/	medium	ZGrab Application Layer Scanner Detection	20.186.236.153	2025-04-14 00:29:14
fd0ebf35-5cad-4f54-bfe6-e9a4e825e9fa	UNKNOWN	M6CCORNFW02-P	20.84.136.119/	medium	ZGrab Application Layer Scanner Detection	20.186.236.153	2025-04-14 00:28:34
c5942ded-885a-4bc3-a44a-b8478cd4230f	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	ZGrab Application Layer Scanner Detection	20.163.15.34	2025-04-14 00:27:04
ac75ed91-806f-475f-9b2a-d13938e97f52	UNKNOWN	M6CCORNFW02-P	52.154.164.159/	medium	ZGrab Application Layer Scanner Detection	20.163.15.34	2025-04-14 00:26:19
fb27d916-db07-4de5-bc49-9549406abc1e	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	205.210.31.19	2025-04-13 22:04:29
56d1fd07-5251-409d-a64b-e4d27d69f6dd	UNKNOWN	M6CCORNFW02-P	autodiscover.json	medium	ZGrab Application Layer Scanner Detection	20.171.27.227	2025-04-13 21:57:34
cb852ae2-853b-4c20-9d69-ed7cf5995875	UNKNOWN	M6CCORNFW02-P	None	critical	Gh0st.Gen Command and Control Traffic	66.240.205.34	2025-04-13 21:21:49
5795cd7c-046a-4887-8384-805991a06b4f	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	medium	ZGrab Application Layer Scanner Detection	148.113.206.49	2025-04-13 21:13:34
6153d5a8-316f-4844-b5b0-8fd85250681c	UNKNOWN	M6CCORNFW02-P	None	critical	NJRat.Gen Command and Control Traffic	174.138.43.3	2025-04-13 20:41:03
a06137bd-8feb-4497-a534-df35cd472752	UNKNOWN	M6CCORNFW02-P	None	critical	Gh0st.Gen Command and Control Traffic	174.138.43.3	2025-04-13 20:41:03
98eea1bb-6d96-408c-9335-321ad8c86ccb	UNKNOWN	M6CCORNFW02-P	None	critical	NetWire RAT Command and Control Traffic Detection	174.138.43.3	2025-04-13 20:41:03
9ac59330-3c8e-4623-bcaf-a21461821a3d	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.35.136	2025-04-13 20:01:48
2e522457-86a4-45ed-95cd-2c694bed84ef	UNKNOWN	M6CCORNFW02-P	52.154.164.159/	medium	ZGrab Application Layer Scanner Detection	143.110.182.33	2025-04-13 16:44:57
d7c29afe-e209-4434-8bdd-768d5fc33932	UNKNOWN	M6CCORNFW02-P	52.154.164.159/aaa9	medium	ZGrab Application Layer Scanner Detection	143.110.182.33	2025-04-13 16:44:47
39508baa-65ed-4fb1-bd00-66d595b4b6b5	UNKNOWN	M6CCORNFW02-P	None	critical	NJRat.Gen Command and Control Traffic	66.240.205.34	2025-04-13 15:40:57
5a60c3e1-3de4-4591-ad31-30338d358cbc	UNKNOWN	M6CCORNFW02-P	diag_Form	critical	GPON Home Routers Remote Code Execution Vulnerability	117.217.196.11	2025-04-13 14:33:22
9f603962-08e6-42fc-9d8e-59a6ca7c6832	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	167.94.138.148	2025-04-13 12:26:36
5e95d377-ea8a-4362-863d-16b886467f22	UNKNOWN	M6CCORNFW02-P	ab2g	medium	ZGrab Application Layer Scanner Detection	162.243.20.89	2025-04-13 12:06:01
cac9078d-5e49-4bc6-b5e3-79a75ed794e0	UNKNOWN	M6CCORNFW02-P	52.154.164.146/	critical	Korplug Command and Control Traffic Detection	162.243.20.89	2025-04-13 12:06:01
27b0c8ac-2da8-4030-b902-3642831db12e	UNKNOWN	M6CCORNFW02-P	52.154.164.159:443/manager/html	medium	ZGrab Application Layer Scanner Detection	20.65.193.148	2025-04-13 08:49:30
f20a0078-393c-43b7-a70b-ccff4cde497b	UNKNOWN	M6CCORNFW02-P	52.154.164.149:443/manager/html	medium	ZGrab Application Layer Scanner Detection	20.65.193.148	2025-04-13 08:49:20
99a810a3-3e1d-4370-b6b7-4c8c6298dda6	UNKNOWN	M6CCORNFW02-P	20.84.136.119:443/manager/html	medium	ZGrab Application Layer Scanner Detection	20.163.15.19	2025-04-13 08:47:25
850eebaa-3957-4a6f-aa7c-98db0e101973	UNKNOWN	M6CCORNFW02-P	20.84.136.112:443/manager/html	medium	ZGrab Application Layer Scanner Detection	20.163.15.19	2025-04-13 08:45:55

744865a5-baf8-4955-8f43-f8c4f450c0b5	UNKNOWN	M6CCORNFW02-P	20.84.136.118:443/manager/html	medium	ZGrab Application Layer Scanner Detection	20.163.15.19	2025-04-13 08:45:35
49c1942f-602e-482d-8edf-7167d5096187	UNKNOWN	M6CCORNFW02-P	login.esp	critical	Palo Alto Networks GlobalProtect OS Command Injection Vulnerability	64.62.156.94	2025-04-13 08:19:40
6083f65a-c5a8-457e-bd25-87bfaed1a841	UNKNOWN	M6CCORNFW02-P	login.esp	critical	Palo Alto Networks GlobalProtect OS Command Injection Vulnerability	64.62.156.104	2025-04-13 08:19:40
8c572174-f387-4dcc-98c7-93550349c6ec	UNKNOWN	M6CCORNFW02-P	None	medium	Metasploit VxWorks WDB Agent Scanner Detection	206.168.35.172	2025-04-13 07:51:05
9e446545-ba7b-4bb6-845d-fc73f5c0feb9	UNKNOWN	M6CCORNFW02-P	20.84.136.119:443/	medium	ZGrab Application Layer Scanner Detection	20.171.25.155	2025-04-13 03:46:34
1f4360c0-e4db-43fd-98c5-b23353adaaf4	UNKNOWN	M6CCORNFW02-P	20.84.136.118:443/	medium	ZGrab Application Layer Scanner Detection	20.171.25.155	2025-04-13 03:46:14
9bf3a46b-4b32-43e6-bd22-9267d9696524	UNKNOWN	M6CCORNFW02-P	20.84.136.112:443/	medium	ZGrab Application Layer Scanner Detection	20.171.25.155	2025-04-13 03:46:09
410ecbeb-851e-41bd-aafa-929151c1749b	UNKNOWN	M6CCORNFW02-P	52.154.164.149:443/	medium	ZGrab Application Layer Scanner Detection	20.150.206.166	2025-04-13 03:42:34
4939e4a8-0b75-4e5a-a54e-e738d3b328d3	UNKNOWN	M6CCORNFW02-P	None	critical	Gh0st.Gen Command and Control Traffic	66.240.205.34	2025-04-13 03:12:24
abc6d731-018f-4034-9e5d-6a5658f28a73	UNKNOWN	M6CCORNFW02-P	20.84.136.112/.env	medium	AndroxGh0st Scanning Traffic Detection	165.154.235.97	2025-04-15 09:00:14
cb0d01bc-b923-4bd6-9eb9-e949a2c9d6cb	UNKNOWN	M6CCORNFW02-P	20.84.136.119/	medium	AndroxGh0st Scanning Traffic Detection	165.154.235.97	2025-04-13 17:58:03
ab2aee1e-79b6-43ed-b5a8-663865fc3b49	UNKNOWN	M6CCORNFW02-P	20.84.136.119/.env	medium	AndroxGh0st Scanning Traffic Detection	165.154.235.97	2025-04-13 17:58:03
44512284-ba57-4d3a-87d0-67cb91be36c4	UNKNOWN	M6CCORNFW02-P	20.84.136.112/	medium	AndroxGh0st Scanning Traffic Detection	165.154.235.97	2025-04-15 09:00:19
d8e7e68b-2c3d-4048-9198-ea6a28baa92b	KENNES APODACA	None	None	low	Access was blocked to "https://havenly.com/products/details/Valencia-Console-Table-Wayfair-71138876" because of "Mal/ExpJS-N".	192.168.0.46	2025-04-17 20:38:12.853000
5d59b238-aa2e-4ee1-92b7-9ac646d08c2a	KENNES APODACA	None	None	low	Access was blocked to "https://havenly.com/products/details/Valencia-Console-Table-Wayfair-71138876" because of "Mal/ExpJS-N".	192.168.0.46	2025-04-17 20:37:55.775000
02439462-e44c-43bc-bd9d-7d94e8893fc9	NAGESH RAI	None	None	low	Access was blocked to "https://files.umso.co/lib_cZGpwPhfNYOuAywh/oqkvv43xq9by5tms.png" because of "Mal/HTMLGen-A".	192.168.7.106	2025-04-17 16:27:48.453000
ee69d2d2-b011-4eb7-95dc-6b129f011431	CORP\STEPHANIEKULESA	None	None	low	Access was blocked to "admedia.gotrackier.io" because of "Mal/HTMLGen-A".	10.11.248.90	2025-04-17 15:59:12.316000
f4987453-016f-49ad-b4bb-11c6fbdfe423	CORP\CHRISVINCENT	None	None	low	Access was blocked to "pycaga.com" because of "Mal/HTMLGen-A".	192.168.1.109	2025-04-15 19:38:23.195000
2925ed1d-1da2-42e9-8023-044e01bf101b	RILEY CAVANAUGH	None	None	low	Access was blocked to "systemtracer.life" because of "Mal/HTMLGen-A".	10.10.10.46	2025-04-15 18:50:09.743000
3e3afbc8-f226-45fa-b876-4d897b5baa85	MICHAEL PALUMBO	None	None	low	Access was blocked to "vaanitech.com" because of "Mal/HTMLGen-A".	10.10.85.160	2025-04-15 17:35:00
2854e63c-004a-4166-a5aa-b4beda43079c	UNKNOWN	M6CCORNFW02-P	translation-table	high	Cisco ASA and FTD Arbitrary File Read Vulnerability	185.250.151.242	2025-04-21 05:36:53
a1370322-4fe9-4b64-b66f-937f5799191b	UNKNOWN	M6CCORNFW02-P	rb_bf67351fjp	high	HTTP SQL Injection Attempt	139.87.117.45	2025-04-21 20:24:38
60f497ad-f32c-48c1-8635-19ab5b3f2e40	UNKNOWN	M6CCORNFW02-P	rb_bf67351fjp	high	HTTP SQL Injection Attempt	139.87.117.45	2025-04-21 20:24:53
12c49105-4144-403e-93a9-26ece97d9924	UNKNOWN	M6CCORNFW02-P	rb_bf67351fjp	high	HTTP SQL Injection Attempt	139.87.117.45	2025-04-21 20:24:23
2aa0da33-0473-4316-9195-3e36a3d51c94	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	139.87.117.45	2025-04-21 20:53:18
c43fe2f0-cc6d-4d78-b4e7-21e875d64ccf	UNKNOWN	M6CCORNFW02-P	rb_bf67351fjp	high	HTTP SQL Injection Attempt	139.87.117.45	2025-04-21 20:24:33
3079096e-98e6-4abf-9c70-eed4c5e85b56	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	139.87.117.45	2025-04-21 20:48:18
420493ad-d894-4774-9a81-4896c23adb8d	UNKNOWN	M6CCORNFW02-P	None	high	Apache Tomcat Remote Code Execution Via JSP Upload Vulnerability	139.87.117.45	2025-04-21 21:24:43
19329045-b891-4d82-be24-61c0c68d44f0	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	139.87.117.45	2025-04-21 22:21:18
3c20659f-ac74-4671-9c7a-7361c737121b	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	139.87.117.45	2025-04-21 22:20:48
4c293782-b19e-4aeb-b20f-93ee9006c256	UNKNOWN	M6CCORNFW02-P	console.portal	critical	Oracle WebLogic Server Remote Code Execution Vulnerability	139.87.117.45	2025-04-21 22:16:33
39f20534-3c64-45d7-9686-812e7fb1e2c9	HASINFO@VOYA.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-22T11:59:00Z,EndTimeUtc:2025-04-22T12:00:00Z,TimeGenerated:2025-04-22T11:59:47.5266667Z,ProcessingEndTime:2025-04-22T12:34:28.7324331Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:f63e1966-9521-549d-f92d-08dd81952cfb,SystemAlertId:null,CorrelationKey:dbc1c53b-0fd6-4c1d-9fc1-492f8066fc9b,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=f63e1966-9521-549d-f92d-08dd81952cfb,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:alyssaramirez@merchantsfleet.com,Upn:alyssaramirez@merchantsfleet.com,AadId:fd80b955-d567-457e-b975-4424e6fa04ee,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:0a24c6b1d2b5f9c544e9c08f98da3f7e,Source:OATP,FirstSeen:2025-04-22T12:08:25},{$id:4,Recipient:alyssaramirez@merchantsfleet.com,Urls:[http://voyamarketingzone.13931640.128149@bounce.dmpemail1.com/?subject=unsubscribe,https://www4.dmp-voyamail.com/voyamarketingzone/dsc/collateral/Email_Banner_XLarge(3).jpg,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/voya_facebook.png,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/voya_youtube.png,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/footer_bar.png,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/logo.png],Threats:[EmailVolumeAnomaly,EmailVolumeAnomaly,EmailVolumeAnomaly,EmailVolumeAnomaly],Sender:hasinfo@voya.com,P1Sender:www-data+voyamarketingzone@bounce.dmp-voyamail.com,P1SenderDomain:bounce.dmp-voyamail.com,SenderIP:208.82.211.28,P2Sender:hasinfo@voya.com,P2SenderDisplayName:Voya Health Account Solutions,P2SenderDomain:voya.com,ReceivedDate:2025-04-21T17:52:03,NetworkMessageId:555b55ef-20e6-45ac-dc12-08dd80fd36f3,InternetMessageId:<20250421175158.B959888D6E@mail.voya.dmpemail1.com>,Subject:Update to Voya Health Account Solutions homepage,AntispamDirection:Inbound,DeliveryAction:DeliveredAsSpam,ThreatDetectionMethods:[MLModel],Language:en,DeliveryLocation:JunkFolder,OriginalDeliveryLocation:JunkFolder,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Fail}	208.82.211.28	2025-04-22 12:34:47

68c729bb-b463-4409-98b9-2aef48584c19	CARLOS.MEJIA2@THOMSONREUTERS.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-22T11:58:00Z,EndTimeUtc:2025-04-22T11:59:00Z,TimeGenerated:2025-04-22T11:59:20.1433333Z,ProcessingEndTime:2025-04-22T12:34:25.2793432Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:6f6b3c7e-f560-7657-2a2a-08dd819509c9,SystemAlertId:null,CorrelationKey:760e1888-fdb0-4deb-86d2-52e6dc0108d7,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=6f6b3c7e-f560-7657-2a2a-08dd819509c9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,Recipient:alyssaramirez@merchantsfleet.com,Sender:carlos.mejia2@thomsonreuters.com,P1Sender:carlos.mejia2@bouncebm.thomsonreuters.com,P1SenderDomain:bouncebm.thomsonreuters.com,SenderIP:65.110.55.248,P2Sender:carlos.mejia2@thomsonreuters.com,P2SenderDisplayName:Mejia Carlitos,P2SenderDomain:thomsonreuters.com,ReceivedDate:2025-04-21T20:44:42,NetworkMessageId:c33559bf-ffdf-4855-cfc7-08dd81155607,InternetMessageId:<4adb2df1a7674999a8b9cb999ea2bcd4@thomsonreuters.com>,Subject:Reaching out,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:30e379dc7abec44f19c1b6cd01977689,Source:OATP,FirstSeen:2025-04-22T12:08:25},{$id:4,MailboxPrimaryAddress:alyssaramirez@merchantsfleet.com,Upn:alyssaramirez@merchantsfleet.com,AadId:fd80b955-d567-457e-b975-4424e6fa04ee,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:2398da6da1a912e916cd863b90884969,Source:OATP,FirstSeen:2025-04-22T12:08:25},{$id:5,Address:65.110.55.248,Type:ip,Urn:urn:IPEntity:203b269c57cb765b6cca54b1eeff7965,Source:OATP,FirstSeen:2025-04-22T12:10:41},{$id:6,NetworkMessageIds:[c33559bf-ffdf-4855-cfc7-08dd81155607],CountByThreatType:{HighConfPhish:0,Phish:0,Malware:0,Spam:0},CountByProtectionStatus:{Delivered:1},CountByDeliveryLocation:{Inbox:1},Query:((((Subject:\Reaching out\)) AND ((P2SenderDomain: homsonreuters.com\)) AND ((AntispamDirection:\1\)) AND ((ContentType: 1))) AND NOT(XmlInfoTenantPolicyFinalVerdictSource:PhishEdu) AND NOT(XmlInfoTenantPolicyFinalVerdictSource:SecOps)	65.110.55.248	2025-04-22 12:34:47
0e99400e-dfde-4c67-add3-a8e12deaef86	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:f63e1966-9521-549d-f92d-08dd81952cfb,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:59:00.0000000Z,te:2025-04-22T12:00:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:e420ac93-3916-4ed3-17b7-08dd81952ed8,wsrt:2025-04-22T12:02:51,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-22 12:34:28
eb9a4093-18f4-4fdf-8bf4-cf93d941578f	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:6f6b3c7e-f560-7657-2a2a-08dd819509c9,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:58:00.0000000Z,te:2025-04-22T11:59:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:e756159b-cd9e-40e1-4445-08dd81950b2e,wsrt:2025-04-22T12:00:31,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-22 12:34:24
a1d777ceb-276b-450e-8e81-c9c0d14fbac0	HASINFO@VOYA.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-22T11:59:00Z,EndTimeUtc:2025-04-22T12:00:00Z,TimeGenerated:2025-04-22T11:59:47.5266667Z,ProcessingEndTime:2025-04-22T12:10:33.6160212Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:f63e1966-9521-549d-f92d-08dd81952cfb,SystemAlertId:null,CorrelationKey:f62e8c35-fe93-4bdb-846d-18759bdab6a6,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=f63e1966-9521-549d-f92d-08dd81952cfb,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:alyssaramirez@merchantsfleet.com,Upn:alyssaramirez@merchantsfleet.com,AadId:fd80b955-d567-457e-b975-4424e6fa04ee,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:0a24c6b1d2b59c544e9c08f98fda3f7e,Source:OATP,FirstSeen:2025-04-22T12:08:25},{$id:4,Recipient:alyssaramirez@merchantsfleet.com,Urls:[http://voyamarketingzone.1393164.128149@bounce.dmpemail1.com/?subject=unsubscribe,https://www4.dmp-voyamail.com/voyamarketingzone/dsc/collateral/Email_Banner_XLarge(3).jpg,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/voya_facebook.png,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/voya_youtube.png,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/footer_bar.png,https://www4.dmp-voyamail.com/voyamarketingzone/files/image_repository/email_templates/167037/logo.png],Sender:hasinfo@voya.com,P1Sender:www-data+voyamarketingzone@bounce.dmp-voyamail.com,P1SenderDomain:bounce.dmp-voyamail.com,SenderIP:208.82.211.28,P2Sender:hasinfo@voya.com,P2SenderDisplayName:Voya Health Account Solutions,P2SenderDomain:voya.com,ReceivedDate:2025-04-21T17:52:03,NetworkMessageId:555b55ef-20e6-45ac-dc12-08dd80fd36f3,InternetMessageId:,Subject:Update to Voya Health Account Solutions homepage,AntispamDirection:Inbound,DeliveryAction:DeliveredAsSpam,ThreatDetectionMethods:[MLModel],Language:en,DeliveryLocation:JunkFolder,OriginalDeliveryLocation:JunkFolder,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Fail},{Name:DMARC,Value:Fail},{Name:Comp Auth,Value:none}],SystemOverrides:[],Type:mailMessa	208.82.211.28	2025-04-22 12:10:41
780c4797-3714-4dd5-b213-f09dc14387b3	CARLOS.MEJIA2@THOMSONREUTERS.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-22T11:58:00Z,EndTimeUtc:2025-04-22T11:59:00Z,TimeGenerated:2025-04-22T11:59:20.1433333Z,ProcessingEndTime:2025-04-22T12:10:31.6629098Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:6f6b3c7e-f560-7657-2a2a-08dd819509c9,SystemAlertId:null,CorrelationKey:a70b3566-1a70-462b-b832-5b94db19ca1a,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=6f6b3c7e-f560-7657-2a2a-08dd819509c9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,Recipient:alyssaramirez@merchantsfleet.com,Sender:carlos.mejia2@thomsonreuters.com,P1Sender:carlos.mejia2@bouncebm.thomsonreuters.com,P1SenderDomain:bouncebm.thomsonreuters.com,SenderIP:65.110.55.248,P2Sender:carlos.mejia2@thomsonreuters.com,P2SenderDisplayName:Mejia Carlitos,P2SenderDomain:thomsonreuters.com,ReceivedDate:2025-04-21T20:44:42,NetworkMessageId:c33559bf-ffdf-4855-cfc7-08dd81155607,InternetMessageId:<4adb2df1a7674999a8b9cb999ea2bcd4@thomsonreuters.com>,Subject:Reaching out,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:30e379dc7abec44f19c1b6cd01977689,Source:OATP,FirstSeen:2025-04-22T12:08:25},{$id:4,MailboxPrimaryAddress:alyssaramirez@merchantsfleet.com,Upn:alyssaramirez@merchantsfleet.com,AadId:fd80b955-d567-457e-b975-4424e6fa04ee,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:2398da6da1a912e916cd863b90884969,Source:OATP,FirstSeen:2025-04-22T12:08:25}],LogCreationTime:2025-04-22T10:31:07.6785347Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	65.110.55.248	2025-04-22 12:10:41
bfadfdd0-93d3-4e01-92e0-1afd4a6750f1	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-22T11:59:00Z,EndTimeUtc:2025-04-22T12:00:00Z,TimeGenerated:2025-04-22T11:59:47.5266667Z,ProcessingEndTime:2025-04-22T12:05:24.6808051Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:f63e1966-9521-549d-f92d-08dd81952cfb,SystemAlertId:null,CorrelationKey:b8331958-fb13-417f-8cdf-c1d977ee17ae,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=f63e1966-9521-549d-f92d-08dd81952cfb,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-22T12:05:24.6808051Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-22 12:05:28
348907e1-cb1d-4af3-a4dd-09ed236d339e	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-22T11:58:00Z,EndTimeUtc:2025-04-22T11:59:00Z,TimeGenerated:2025-04-22T11:59:20.1433333Z,ProcessingEndTime:2025-04-22T12:05:23.3526901Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:6f6b3c7e-f560-7657-2a2a-08dd819509c9,SystemAlertId:null,CorrelationKey:41b673e8-20b3-4638-8664-b27169fcf9d4,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=6f6b3c7e-f560-7657-2a2a-08dd819509c9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-22T12:05:23.3526901Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-22 12:05:28
428bf356-5110-493c-86fc-5e26471d019b	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:f63e1966-9521-549d-f92d-08dd81952cfb,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:59:00.0000000Z,te:2025-04-22T12:00:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:e420ac93-3916-4ed3-17b7-08dd81952ed8,wsrt:2025-04-22T12:02:51,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-22 12:04:21
617ddf72-d9b1-4e6a-8fe9-4f3297a97618	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:6f6b3c7e-f560-7657-2a2a-08dd819509c9,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:58:00.0000000Z,te:2025-04-22T11:59:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:e756159b-cd9e-40e1-4445-08dd81950b2e,wsrt:2025-04-22T12:00:31,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-22 12:01:48
557d2337-d996-47e9-8e1f-19a813855462	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:f63e1966-9521-549d-f92d-08dd81952cfb,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:59:00Z,te:2025-04-22T12:00:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:01cf4982-517a-4b2a-289a-08dd81952da0,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:78ae9e73eca649118bf5c9f3072bd531}	None	2025-04-22 12:00:09
abbd2a9e-dd02-4709-bb98-053a7aeb6c07	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:6f6b3c7e-f560-7657-2a2a-08dd819509c9,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:58:00Z,te:2025-04-22T11:59:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:0b09620e-519a-44d6-904f-08dd81950a47,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90}	None	2025-04-22 11:59:49
77f2df88-f7f9-4004-9244-dd26f97e5e75	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:f63e1966-9521-549d-f92d-08dd81952cfb,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:59:00.0000000Z,te:2025-04-22T12:00:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:01cf4982-517a-4b2a-289a-08dd81952da0,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-22 11:59:47
62467782-e7e6-4541-936e-5e08878b17de	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-22T11:59:47.2059546Z,te:2025-04-22T11:59:47.2059546Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:hasinfo@voya.com,sip:,imsgid:3d24b68f-2698-409a-b87c-465f8179b355@DM4PR11MB8225.namprd11.prod.outlook.com,srt:1,trc:alyssaramirez@merchantsfleet.com,ms:Update to Voya Health Account Solutions homepage,sid:01cf4982-517a-4b2a-289a-08dd81952da0,aii:555b55ef-20e6-45ac-dc12-08dd80fd36f3,md:2025-04-21T17:51:59.3510930Z,etps:SubmissionId:2453f47-867d-4f25-f92d-08dd81952cfb,lon:UserSubmission}	None	2025-04-22 11:59:47
5efe48c7-150b-4082-bff3-832e59c2e1b8	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:6f6b3c7e-f560-7657-2a2a-08dd819509c9,f3u:phishing@merchantsfleet.com,ts:2025-04-22T11:58:00Z,te:2025-04-22T11:59:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:0b09620e-519a-44d6-904f-08dd81950a47,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:e97d62a7df8bab43296b14979b7dee90}	None	2025-04-22 11:59:20
c0c2bc00-e6a9-47af-b451-c6d4b8aae84d	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-22T11:58:47.9050831Z,te:2025-04-22T11:58:47.9050831Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:Carlos.Mejia2@thomsonreuters.com,sip:,imsgid:6f3284b7-1058-4cb7-ba96-2d7b7aacdc38@DS0PR11MB8739.namprd11.prod.outlook.com,srt:1,trc:alyssaramirez@merchantsfleet.com,ms:Reaching out,sid:0b09620e-519a-44d6-904f-08dd81950a47,aii:c33559bf-ffdf-4855-cfc7-08dd81155607,md:2025-04-21T20:44:39.4127303Z,etps:SubmissionId:3175ec24-4824-4ca5-2a2a-08dd819509c9,lon:UserSubmission}	None	2025-04-22 11:59:20
98267208-cb86-459a-b889-11e4f67357c2	TAYLOR.SARAH@SQXFINANCIALDATA.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T19:34:00Z,EndTimeUtc:2025-04-21T19:35:00Z,TimeGenerated:2025-04-21T19:34:29.9066667Z,ProcessingEndTime:2025-04-21T20:04:44.7081322Z,Status:Resolved,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:9c63a142-ac6b-758a-85ad-08dd810b7b8e,SystemAlertId:null,CorrelationKey:ef715adf-a113-484d-8436-25b31cab89a,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=9c63a142-ac6b-758a-85ad-08dd810b7b8e,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:robertlewis@merchantsfleet.com,Upn:robertlewis@merchantsfleet.com,AadId:0cb67f6e-49b5-42ce-8bb0-1968079a2319,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:7293bfd666f00d1f573655429553c007,Source:OATP,FirstSeen:2025-04-21T19:39:35},{$id:4,Recipient:robertlewis@merchantsfleet.com,Sender:taylor.sarah@sqxfinancialdata.com,P1Sender:taylor.sarah@sqxfinancialdata.com,P1SenderDomain:sqxfinancialdata.com,SenderIP:2607:f8b0:4864:20::d44,P2Sender:taylor.sarah@sqxfinancialdata.com,P2SenderDisplayName:Sarah Taylor,P2SenderDomain:sqxfinancialdata.com,ReceivedDate:2025-04-21T18:06:35,NetworkMessageId:cce28b3e-a452-46cb-5a03-08dd80ff3963,InternetMessageId:,Subject:Re: quick question Robert,AntispamDirection:Inbound,DeliveryAction:DeliveredAsSpam,ThreatDetectionMethods:[MLModel],Language:en,DeliveryLocation:JunkFolder,OriginalDeliveryLocation:JunkFolder,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:51642e67e759678c5ca3e3946d2ecb68,Source:OATP,FirstSeen:2025-04-21T19:39:35},{$id:5,Address:2607:f8b0:4864:20::d44,Type:ip,Urn:urn:IPEntity:d9a5cbaf2d4edb6c27b569ae66e304e1,Source:OATP,FirstSeen:2025-04-21T19:42:48},{$id:6,NetworkMessageIds:[cce28b3e-a452-46cb-5a03-08dd80ff3963],CountByThreatType:{HighConfPhish:0,Phish:0,Malware:0,Spam:1},CountByProtectionStatus:{DeliveredAsSpam:1},CountByDeliveryLocation:{JunkFolder:1},Query:((((Subject:\Re: quick question Robert\)) AND ((SenderIp:\2607:f8b0:4864:20::d44\)) AND ((AntispamDirection:\1\)) AND ((ContentType: 1))) AND NOT(XmlIn	None	2025-04-21 20:06:55

bbe76909-d9fa-4579-b8fa-6cc748ea7db3	TAYLOR.SARAH@SQXFINANCIALDATA.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T19:34:00Z,EndTimeUtc:2025-04-21T19:35:00Z,TimeGenerated:2025-04-21T19:34:29.9066667Z,ProcessingEndTime:2025-04-21T19:40:44.2689925Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:9c63a142-ac6b-758a-85ad-08dd810b7b8e,SystemAlertId:null,CorrelationKey:be13474d-a7c3-4a27-8218-6ce5ca2a2eac,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=9c63a142-ac6b-758a-85ad-08dd810b7b8e,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:robertlewis@merchantsfleet.com,Upn:robertlewis@merchantsfleet.com,AadId:0cb67f6e-49b5-42ce-8bb0-1968079a2319,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:7293bfd666f00d1f57365542955 3c007,Source:OATP,FirstSeen:2025-04-21T19:39:35},{$id:4,Recipient:robertlewis@merchantsfleet.com,Sender:taylor.sarah@sqxfinancialdata.com,P1Sender:taylor.sarah@sqxfinancialdata.com,P1SenderDomain:sqxfinancialdata.com,SenderIP:2607:f8b0:4864:20::d44,P2Sender:taylor.sarah@sqxfinancialdata.com,P2SenderDisplayName:Sarah Taylor,P2SenderDomain:sqxfinancialdata.com,ReceivedDate:2025-04-21T18:06:35,NetworkMessageId:cce28b3e-a452-46cb-5a03-08dd80ff3963,InternetMessageId:,SubjectRe: quick question Robert,AntispamDirection:Inbound,DeliveryAction:Delivered,DeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:51642e67e759678c5ca3e3946d2ecb68,Source:OATP,FirstSeen:2025-04-21T19:39:35}],LogCreationTime:2025-04-21T19:40:44.2689925Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 19:40:45
a811b46a-9c0f-4a45-ba1f-fb074c24f941	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:9c63a142-ac6b-758a-85ad-08dd810b7b8e,f3u:phishing@merchantsfleet.com,ts:2025-04-21T19:34:00.0000000Z,te:2025-04-21T19:35:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:d164e7de-6515-4f7d-88bc-08dd810b7d48,wsrt:2025-04-21T19:36:40,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 19:39:51
e4176118-1deb-4e20-9d8a-f6b6b043d2f9	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T19:34:00Z,EndTimeUtc:2025-04-21T19:35:00Z,TimeGenerated:2025-04-21T19:34:29.9066667Z,ProcessingEndTime:2025-04-21T19:35:18.03694Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:9c63a142-ac6b-758a-85ad-08dd810b7b8e,SystemAlertId:null,CorrelationKey:7214ad0e-e640-431d-8bfe-6768f9ca794f,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=9c63a142-ac6b-758a-85ad-08dd810b7b8e,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T19:35:18.03694Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 19:35:19
a26ec24b-aa89-4245-aeb2-0229093 07bd0	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:9c63a142-ac6b-758a-85ad-08dd810b7b8e,f3u:phishing@merchantsfleet.com,ts:2025-04-21T19:34:00Z,te:2025-04-21T19:35:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:ffaa8d96-4051-4c40-9325-08dd810b7c13,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326}	None	2025-04-21 19:34:31
17812d60-96a2-4253-9f2e-2d6546009a34	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-21T19:34:08.2759461Z,te:2025-04-21T19:34:08.2759461Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:taylor.sarah@sqxfinancialdata.com,sip:,imsgid:764dc03c-d965-44dc-9a87-5f5aedb61818@LV2PR11MB5998.namprd11.prod.outlook.com,srt:1,trc:robertlewis@MerchantsFleet.com,ms:Re: quick question Robert,sid:ffaa8d96-4051-4c40-9325-08dd810b7c13,aii:cce28b3e-a452-46cb-5a03-08dd80ff3963,md:2025-04-21T18:06:22.4306691Z,etps:SubmissionId:035bf771-bed4-4535-85ad-08dd810b7b8e,lon:UserSubmission}	None	2025-04-21 19:34:29
cf02fb45-c4e3-4698-a7cf-9644c37a6548	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:9c63a142-ac6b-758a-85ad-08dd810b7b8e,f3u:phishing@merchantsfleet.com,ts:2025-04-21T19:34:00Z,te:2025-04-21T19:35:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:ffaa8d96-4051-4c40-9325-08dd810b7c13,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:d14358e8aa1409725a4b2ba04aa2a326}	None	2025-04-21 19:34:29
1306dd24-18f9-4b75-82d0-5d9c953f3583	NOREPLY@EMAIL.TEAMS.MICROSOFT.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T18:18:00Z,EndTimeUtc:2025-04-21T18:19:00Z,TimeGenerated:2025-04-21T18:18:08.14Z,ProcessingEndTime:2025-04-21T18:52:02.9106902Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:63e93678-2b9c-e35e-9218-08dd8100dd21,SystemAlertId:null,CorrelationKey:f14d9774-c957-4c47-8748-7f2ab2947822,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=63e93678-2b9c-e35e-9218-08dd8100dd21,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,Recipient:jordanwagner@merchantsfleet.com,Urls:[https://aka.ms/downloadteams,https://statics.teams.skype.com/icons/icn_apple.png,https://statics.teams.skype.com/icons/img_chat.png,https://statics.teams.skype.com/icons/img_tabs.png,https://statics.teams.skype.com/icons/icn_android.png,https://urlshortener.teams.cloud.microsoft/8DD810028912513-3-0,https://statics.teams.microsoft.com/evergreen-assets/emails/notification_bell.png,https://teams.microsoft.com/l/chat/19:2c1f87b08e014009a9be720e58515933@thread.v2/conversations?tenantId=74e16038-e7dd-4392-b38a-5a2b6d6e3a25,https://statics.teams.skype.com/icons/img_teams_channels.png,https://statics.teams.skype.com/icons/img_videocalling.png,https://teams.microsoft.com/downloads],Sender:noreply@email.teams.microsoft.com,P1Sender:noreply@email.teams.microsoft.com,P1SenderDomain:email.teams.microsoft.com,SenderIP:2a01:111:f403:2414::70f,P2Sender:noreply@email.teams.microsoft.com,P2SenderDisplayName:Microsoft Teams,P2SenderDomain:email.teams.microsoft.com,ReceivedDate:2025-04-21T18:11:05,NetworkMessageId:cd4bfdfa-9e85-41e0-e52e-08dd80ffde2d,InternetMessageId:,Subject:Matt Moore is trying to reach you in Microsoft Teams,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:a68314834ce97fd4ceb7f3825265d76c,Source:OATP,FirstSeen:2025-04-21T18:26:56},{$id:4,MailboxPrimaryAddress:jordanwagner@merchantsfleet.com,Upn:jordanwagner@merchantsfleet.com,AadId:0cb67f6e-49b5-42ce-8bb0-1968079a2319,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:7293bfd666f00d1f57365542955 3c007,Source:OATP,FirstSeen:2025-04-21T19:39:35},{$id:4,Recipient:robertlewis@merchantsfleet.com,Sender:taylor.sarah@sqxfinancialdata.com,P1Sender:taylor.sarah@sqxfinancialdata.com,P1SenderDomain:sqxfinancialdata.com,SenderIP:2607:f8b0:4864:20::d44,P2Sender:taylor.sarah@sqxfinancialdata.com,P2SenderDisplayName:Sarah Taylor,P2SenderDomain:sqxfinancialdata.com,ReceivedDate:2025-04-21T18:06:35,NetworkMessageId:cce28b3e-a452-46cb-5a03-08dd80ff3963,InternetMessageId:,SubjectRe: quick question Robert,AntispamDirection:Inbound,DeliveryAction:Delivered,DeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:51642e67e759678c5ca3e3946d2ecb68,Source:OATP,FirstSeen:2025-04-21T19:39:35}],LogCreationTime:2025-04-21T19:40:44.2689925Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 18:52:25
129e8d5b-e5f4-474f-9574-5f7922ef8763	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:63e93678-2b9c-e35e-9218-08dd8100dd21,f3u:phishing@merchantsfleet.com,ts:2025-04-21T18:18:00.0000000Z,te:2025-04-21T18:19:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:8f2300fd-5100-4c6a-676a-08dd8100deb7,wsrt:2025-04-21T18:20:46,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 18:52:02
732e13f9-999e-4f05-8845-bbba5526c641	NOREPLY@EMAIL.TEAMS.MICROSOFT.COM	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T18:18:00Z,EndTimeUtc:2025-04-21T18:19:00Z,TimeGenerated:2025-04-21T18:18:08.14Z,ProcessingEndTime:2025-04-21T18:29:22.8904084Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:63e93678-2b9c-e35e-9218-08dd8100dd21,SystemAlertId:null,CorrelationKey:686bb6bd-b564-43e4-81d4-df7444ac9af0,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=63e93678-2b9c-e35e-9218-08dd8100dd21,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:robdaziel@merchantsfleet.com,Upn:robdaziel@merchantsfleet.com,AadId:98a2b1a1-37e8-44e6-a1b1-ddc2e8130c6a,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:0eac492cf976f1e530ab9107ad8e7a94,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:image001.jpg,FileHashes:[{$id:6,Algorithm:SHA256,Value:47777C53EEA77034AE420A6CEBBD7FB76C5851551DE241004489DBB37662A972,Type:filehash}],Type:file,MalwareFamily:null},{$id:7,Name:image002.png,FileHashes:[{$id:8,Algorithm:SHA256,Value:961F9CF255B695BF4D4CF380F980AFEA80D4AB280AD7E8E11D3E6CB0A2E93B9C,Type:filehash}],Type:file,MalwareFamily:null},{$id:9,Name:Offers. M365 Copilot. .pdf,FileHashes:[{$id:10,Algorithm:SHA256,Value:F6E24BC7C71D73FBFCE5FA25FF2BD6FFE9B20382F96FFA290AAE9D33DDADD56B,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:richardalbrecht@merchantsfleet.com,Urls:[https://outlook.office.com/bookwithme/me],Sender:kimaura.broomfield@microsoft.com,P1Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:24:35,NetworkMessageId:0c659557-a318-4a05-94f2-08dd7d2ceba5,InternetMessageId:,Subject:Copilot/m365 offers,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Block	None	2025-04-21 18:29:34
a0c3a9bf-7a21-4124-9243-bb21dba07127	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T18:18:00Z,EndTimeUtc:2025-04-21T18:19:00Z,TimeGenerated:2025-04-21T18:18:08.14Z,ProcessingEndTime:2025-04-21T18:24:23.9863062Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:63e93678-2b9c-e35e-9218-08dd8100dd21,SystemAlertId:null,CorrelationKey:68f88e0b-8cb5-4a4d-b4a2-d5b2ef6d9f3c,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=63e93678-2b9c-e35e-9218-08dd8100dd21,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T18:24:23.9863062Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 18:24:31
14458756-7cf6-4f6b-82e0-deeebf005728	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T18:18:00Z,EndTimeUtc:2025-04-21T18:19:00Z,TimeGenerated:2025-04-21T18:18:08.14Z,ProcessingEndTime:2025-04-21T18:24:23.9863062Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:63e93678-2b9c-e35e-9218-08dd8100dd21,SystemAlertId:null,CorrelationKey:68f88e0b-8cb5-4a4d-b4a2-d5b2ef6d9f3c,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:3239e7efbe53fa83b8913758fdb17ec1],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=63e93678-2b9c-e35e-9218-08dd8100dd21,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T18:24:23.9863062Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 18:24:25
1692a5cb-3a53-49d9-bc6f-154ef2172357	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:63e93678-2b9c-e35e-9218-08dd8100dd21,f3u:phishing@merchantsfleet.com,ts:2025-04-21T18:18:00.0000000Z,te:2025-04-21T18:19:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:8f2300fd-5100-4c6a-676a-08dd8100deb7,wsrt:2025-04-21T18:20:46,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 18:22:28
3dfd6bb5-38f5-4ab1-b25b-2670cb6e7f056	KIMAURA.BROOMFIELD@MICROSOFT.COM	None	image001.jpg	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:55:09.6433333Z,ProcessingEndTime:2025-04-21T17:19:22.8662669Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,SystemAlertId:null,CorrelationKey:4c2ac015-e1db-4e9f-b5e8-b491c2d9ab52,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,Recipient:jordanwagner@merchantsfleet.com,Upn:robdaziel@merchantsfleet.com,AadId:98a2b1a1-37e8-44e6-a1b1-ddc2e8130c6a,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:0eac492cf976f1e530ab9107ad8e7a94,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:image001.jpg,FileHashes:[{$id:6,Algorithm:SHA256,Value:47777C53EEA77034AE420A6CEBBD7FB76C5851551DE241004489DBB37662A972,Type:filehash}],Type:file,MalwareFamily:null},{$id:7,Name:image002.png,FileHashes:[{$id:8,Algorithm:SHA256,Value:961F9CF255B695BF4D4CF380F980AFEA80D4AB280AD7E8E11D3E6CB0A2E93B9C,Type:filehash}],Type:file,MalwareFamily:null},{$id:9,Name:Offers. M365 Copilot. .pdf,FileHashes:[{$id:10,Algorithm:SHA256,Value:F6E24BC7C71D73FBFCE5FA25FF2BD6FFE9B20382F96FFA290AAE9D33DDADD56B,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:richardalbrecht@merchantsfleet.com,Urls:[https://outlook.office.com/bookwithme/me],Sender:kimaura.broomfield@microsoft.com,P1Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:24:35,NetworkMessageId:0c659557-a318-4a05-94f2-08dd7d2ceba5,InternetMessageId:,Subject:Copilot/m365 offers,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Block	None	2025-04-21 17:19:43
ac6b3656-0f60-4ae9-9f54-b46ac5ad65fc	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:55:00.0000000Z,te:2025-04-21T15:56:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:ccb9d934-7932-4c1a-4a50-08dd80ece587,wsrt:2025-04-21T15:57:01,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 17:19:22

f79da6df-0bc2-4b37-be08-4b0c65758b60	KIMAURA.BROOMFIELD@MICROSOFT.COM	None	copilot & security.pdf	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:54:48.17Z,ProcessingEndTime:2025-04-21T16:27:23.4962627Z,Status:Resolved,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,SystemAlertId:null,CorrelationKey:afb174cc-da6b-49bc-b53c-f822b3124671,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=bf607b0f-fe53-5c48-1248-08dd80ecd6ab,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:haitamzoubir@merchantsfleet.com,Upn:haitamzoubir@merchantsfleet.com,AadId:4e0ff750-e770-4cc1-a7eb-b1e04818da06,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:a8c789045eb57ae4753e1c1c28353ed2,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:copilot & security.pdf,FileHashes:[{$id:6,Algorithm:SHA256,Value:BF8A0B38F841F74DB7C8AE1DC6764C6C7F2D89490D263B7EC041EE0A64B2A1B8,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:jenraimer@merchantsfleet.com,Sender:kimaura.broomfield@microsoft.com,P1Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:25:19,NetworkMessageId:9e04fe9b-5601-4204-17f5-08dd7d2d0aff,InternetMessageId:,Subject:}Copilot and security ,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Blocked domain),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:736689930d52e554a60be63ce4d8f822,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:7,MailboxPrimaryAddress:jenraimer@merchantsfleet.com,Upn:jenraimer@merchantsfleet.com,AadId:c6e30cae-0d87-4f93-aae8-aa975b1f680e,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:f1e7c14d203812707e89ddb42bb50081,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:8,Address	None	2025-04-21 16:27:42
492723b8-670c-47fb-ad48-b132a0704351	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:55:00.0000000Z,te:2025-04-21T15:56:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:9c3a3751-fedd-4d94-5ec1-08dd80ece040,wsrt:2025-04-21T15:57:01,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 16:27:23
f5ce503f-0c4f-4b7b-acc6-386e5d43a307	KIMAURA.BROOMFIELD@MICROSOFT.COM	None	copilot & security.pdf	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:54:48.17Z,ProcessingEndTime:2025-04-21T16:03:18.3929019Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,SystemAlertId:null,CorrelationKey:479c15db-da09-4776-84c7-92c0b592e1dc,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=bf607b0f-fe53-5c48-1248-08dd80ecd6ab,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:haitamzoubir@merchantsfleet.com,Upn:haitamzoubir@merchantsfleet.com,AadId:4e0ff750-e770-4cc1-a7eb-b1e04818da06,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:a8c789045eb57ae4753e1c1c28353ed2,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:copilot & security.pdf,FileHashes:[{$id:6,Algorithm:SHA256,Value:BF8A0B38F841F74DB7C8AE1DC6764C6C7F2D89490D263B7EC041EE0A64B2A1B8,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:jenraimer@merchantsfleet.com,Sender:kimaura.broomfield@microsoft.com,P1Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:25:19,NetworkMessageId:9e04fe9b-5601-4204-17f5-08dd7d2d0aff,InternetMessageId:,Subject:}Copilot and security ,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Blocked domain),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:736689930d52e554a60be63ce4d8f822,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:7,MailboxPrimaryAddress:jenraimer@merchantsfleet.com,Upn:jenraimer@merchantsfleet.com,AadId:c6e30cae-0d87-4f93-aae8-aa975b1f680e,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:f1e7c14d203812707e89ddb42bb50081,Source:OATP,FirstSeen:2025-04-21T16:03:04},LogCreati	None	2025-04-21 16:04:48
02fdb6b2-c2b2-482f-abdb-2f9f3484e2a8	KIMAURA.BROOMFIELD@MICROSOFT.COM	None	image001.jpg	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:55:09.6433333Z,ProcessingEndTime:2025-04-21T16:03:19.9710174Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,SystemAlertId:null,CorrelationKey:0de7d985-85a9-4f69-8a79-4d32ebad340b,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:robdaziel@merchantsfleet.com,Upn:robdaziel@merchantsfleet.com,AadId:98a2b1a1-37e8-44e6-a1b1-ddc2e8130c6a,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:0eac492cf976f1e530ab9107ad8e7a94,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:image001.jpg,FileHashes:[{$id:6,Algorithm:SHA256,Value:47777C53EEA77034AE420A6CEBBD7FB76C5851551DE24100448 9DB37662A972,Type:filehash}],Type:file,MalwareFamily:null}],{$id:7,Name:image002.png,FileHashes:[{$id:8,Algorithm:SHA256,Value:961F9CF555B695BF4D4CF380F980AFEA80D4AB280AD7E8E11D3E6CB0A2E93B9C,Type:filehash}],Type:file,MalwareFamily:null},{$id:9,Name:Offers. M365 Copilot. .pdf,FileHashes:[{$id:10,Algorithm:SHA256,Value:F6E24BC7C71D73FBFCE5FA25FF2BD6FFE9B20382F96FFA290AAE9D33DDADD56B,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:richardalbrecht@merchantsfleet.com,Urls:[https://outlook.office.com/bookwithme/me],Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:24:35,NetworkMessageId:0c659557-a318-4a05-94f2-08dd7d2ceba5,InternetMessageId:,Subject:Copilot/m365 offers,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Blocked domain),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:736689930d52e554a60be63ce4d8f822,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:7,MailboxPrimaryAddress:jenraimer@merchantsfleet.com,Upn:jenraimer@merchantsfleet.com,AadId:c6e30cae-0d87-4f93-aae8-aa975b1f680e,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:f1e7c14d203812707e89ddb42bb50081,Source:OATP,FirstSeen:2025-04-21T16:03:04},LogCreati	None	2025-04-21 16:04:48
8216dfcf-1ff2-44b7-b66f-b31183d47e49	KIMAURA.BROOMFIELD@MICROSOFT.COM	None	copilot & security.pdf	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:54:48.17Z,ProcessingEndTime:2025-04-21T16:03:18.3929019Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,SystemAlertId:null,CorrelationKey:479c15db-da09-4776-84c7-92c0b592e1dc,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=bf607b0f-fe53-5c48-1248-08dd80ecd6ab,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:haitamzoubir@merchantsfleet.com,Upn:haitamzoubir@merchantsfleet.com,AadId:4e0ff750-e770-4cc1-a7eb-b1e04818da06,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:a8c789045eb57ae4753e1c1c28353ed2,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:copilot & security.pdf,FileHashes:[{$id:6,Algorithm:SHA256,Value:BF8A0B38F841F74DB7C8AE1DC6764C6C7F2D89490D263B7EC041EE0A64B2A1B8,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:jenraimer@merchantsfleet.com,Sender:kimaura.broomfield@microsoft.com,P1Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:25:19,NetworkMessageId:9e04fe9b-5601-4204-17f5-08dd7d2d0aff,InternetMessageId:,Subject:}Copilot and security ,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Blocked domain),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:736689930d52e554a60be63ce4d8f822,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:7,MailboxPrimaryAddress:jenraimer@merchantsfleet.com,Upn:jenraimer@merchantsfleet.com,AadId:c6e30cae-0d87-4f93-aae8-aa975b1f680e,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:f1e7c14d203812707e89ddb42bb50081,Source:OATP,FirstSeen:2025-04-21T16:03:04},LogCreati	None	2025-04-21 16:04:28
e7045b31-e9b1-4d82-b906-852066c41464	KIMAURA.BROOMFIELD@MICROSOFT.COM	None	image001.jpg	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:55:09.6433333Z,ProcessingEndTime:2025-04-21T16:03:19.9710174Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,SystemAlertId:null,CorrelationKey:0de7d985-85a9-4f69-8a79-4d32ebad340b,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,MailboxPrimaryAddress:robdaziel@merchantsfleet.com,Upn:robdaziel@merchantsfleet.com,AadId:98a2b1a1-37e8-44e6-a1b1-ddc2e8130c6a,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:0eac492cf976f1e530ab9107ad8e7a94,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:4,Files:[{$id:5,Name:image001.jpg,FileHashes:[{$id:6,Algorithm:SHA256,Value:47777C53EEA77034AE420A6CEBBD7FB76C5851551DE24100448 9DB37662A972,Type:filehash}],Type:file,MalwareFamily:null}],{$id:7,Name:image002.png,FileHashes:[{$id:8,Algorithm:SHA256,Value:961F9CF555B695BF4D4CF380F980AFEA80D4AB280AD7E8E11D3E6CB0A2E93B9C,Type:filehash}],Type:file,MalwareFamily:null},{$id:9,Name:Offers. M365 Copilot. .pdf,FileHashes:[{$id:10,Algorithm:SHA256,Value:F6E24BC7C71D73FBFCE5FA25FF2BD6FFE9B20382F96FFA290AAE9D33DDADD56B,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:richardalbrecht@merchantsfleet.com,Urls:[https://outlook.office.com/bookwithme/me],Sender:kimaura.broomfield@microsoft.com,P1SenderDomain:microsoft.com,SenderIP:2a01:111:f403:c105::5,P2Sender:kimaura.broomfield@microsoft.com,P2SenderDisplayName:Kimaura Broomfield,P2SenderDomain:microsoft.com,ReceivedDate:2025-04-16T21:24:35,NetworkMessageId:0c659557-a318-4a05-94f2-08dd7d2ceba5,InternetMessageId:,Subject:Copilot/m365 offers,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Pass},{Name:DKIM,Value:Pass},{Name:DMARC,Value:Pass},{Name:Comp Auth,Value:pass}],SystemOverrides:[{Source:Tenant,Result:Allow,Details:Sender domain list (Safe domain / Blocked domain),FinalOverride:Yes}],Type:mailMessage,Urn:urn:MailEntity:736689930d52e554a60be63ce4d8f822,Source:OATP,FirstSeen:2025-04-21T16:03:04},{$id:7,MailboxPrimaryAddress:jenraimer@merchantsfleet.com,Upn:jenraimer@merchantsfleet.com,AadId:c6e30cae-0d87-4f93-aae8-aa975b1f680e,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:f1e7c14d203812707e89ddb42bb50081,Source:OATP,FirstSeen:2025-04-21T16:03:04},LogCreati	None	2025-04-21 16:04:28
1e79ab61-69fa-483c-bd4d-b02100a4ad87	SERGIO@SIGNZOO.COM	None	74048_Proof.jpg	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:23:00Z,EndTimeUtc:2025-04-21T15:24:00Z,TimeGenerated:2025-04-21T15:23:22.71Z,ProcessingEndTime:2025-04-21T16:01:57.3620149Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,SystemAlertId:null,CorrelationKey:21d85cfc-886b-4c18-9cba-e2e3256a5ac9,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4,InvestigationStatus:Benign}],InvestigationIds:[urn:SubmissionInvestigation:c351ca77a0fdcec78288f55ad08ab5c4],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},Entities:[{$id:3,Files:[{$id:4,Name:74048_Proof.jpg,FileHashes:[{$id:5,Algorithm:SHA256,Value:0DBD63BCA63B361EF12CA93EE75B2A8A227521D68EA63C3A4795DF1FCDE0118A,Type:filehash}],Type:file,MalwareFamily:null}],Recipient:kevingrant@merchantsfleet.com,Urls:[https://www.signzoo.com/,https://sarasotawebsites.com/clients/sz/facebook.png,https://sarasotawebsites.com/clients/sz/LinkedIn.png,https://sarasotawebsites.com/clients/sz/Instagram.png,https://www.facebook.com/SignZoo,https://sarasotawebsites.com/clients/sz/SignZoo_Mascot.png,https://www.instagram.com/SignZoo,https://www.linkedin.com/company/SignZoo],Sender:sergio@signzoo.com,P1Sender:sergio@signzoo.com,P1SenderDomain:signzoo.com,SenderIP:2a00:1450:4864:20::12a,P2Sender:sergio@signzoo.com,P2SenderDisplayName:Sergio Vippolis,P2SenderDomain:signzoo.com,ReceivedDate:2025-04-21T15:14:03,NetworkMessageId:1b8c2729-6e2a-4759-b834-08dd80e71e6c,InternetMessageId:,Subject:WO#74048 - Proof,AntispamDirection:Inbound,DeliveryAction:Delivered,Language:en,DeliveryLocation:Inbox,OriginalDeliveryLocation:Inbox,AdditionalActionsAndResults:[OriginalDelivery: [N/A]],AuthDetails:[{Name:SPF,Value:Soft fail},{Name:DKIM,Value:Pass},{Name:DMARC,Value:None},{Name:Comp Auth,Value:pass}],SystemOverrides:[],Type:mailMessage,Urn:urn:MailEntity:2f485efb4d6f678f6ee2e4b48d915e74,Source:OATP,FirstSeen:2025-04-21T15:30:35},{$id:6,MailboxPrimaryAddress:kevingrant@merchantsfleet.com,Upn:kevingrant@merchantsfleet.com,AadId:a715bb7-b57d-420d-b50b-edc3e3c4331a,RiskLevel:None,Type:mailbox,Urn:urn:UserEntity:90a97e88de98268e46dc93288c2e02c4,Source:OATP,FirstSeen:2025-04-21T15:30:35},{$id:7,Address:2a00:1450:4864:20::12a,Type:ip,Urn:urn:IPEntity:81f664e2438c06c3ec300	None	2025-04-21 16:02:31
a88f8b4d-055a-42ce-a963-012691b8b3a09	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:1d3d4c8c-fe22-d423-f9b8-08dd80e8726b,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:23:00.0000000Z,te:2025-04-21T15:24:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:013f16e8-102f-422f-e2c4-08dd80e87b2a,wsrt:2025-04-21T15:26:34,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 16:01:57
f953c0db-6b34-429f-b6d4-da831c636c3d	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:54:48.17Z,ProcessingEndTime:2025-04-21T15:58:13.9418239Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,SystemAlertId:null,CorrelationKey:0173877f-5c5c-4c09-8ecd-1332e45815c2,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=bf607b0f-fe53-5c48-1248-08dd80ecd6ab,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T15:58:13.9418239Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 15:58:18
8226962a-3995-46c7-b6eb-649e2ec0388a	AIRINVESTIGATION	None	None	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-21T15:55:00Z,EndTimeUtc:2025-04-21T15:56:00Z,TimeGenerated:2025-04-21T15:55:09.6433333Z,ProcessingEndTime:2025-04-21T15:58:14.6918177Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,SystemAlertId:null,CorrelationKey:04bd19f0-a506-4511-85a3-e6c29556390e,Investigations:[{$id:1,Id:urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214],Intent:Probing,ResourceIdentifiers:[{$id:2,AadTenantId:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,Type:AAD}],AzureResourceId:null,WorkspaceId:null,WorkspaceSubscriptionId:null,WorkspaceResourceGroup:null,AgentId:null,AlertDisplayName:Email reported by user as malware or phish,Description:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,ExtendedLinks:[{Href:https://security.microsoft.com/viewalerts?id=b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-21T15:58:14.6918177Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	None	2025-04-21 15:58:18
101015a1-ca94-46c7-be30-1004a67b864a	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:55:00.0000000Z,te:2025-04-21T15:56:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:ccb9d934-7932-4c1a-4a50-08dd80ece587,wsrt:2025-04-21T15:57:01,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 15:57:09

d5ec70fb-47c5-4554-8bbf-d6a3506e4f7b	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:55:00.0000000Z,te:2025-04-21T15:56:00.0000000Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:9c3a3751-fedd-4d94-5ec1-08dd80ece040,wsrt:2025-04-21T15:57:01,mdt:Audit,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low}	None	2025-04-21 15:57:09
03352e10-a768-4e1b-954f-392aecffbf55	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:55:00Z,te:2025-04-21T15:56:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:e04de8c4-0aad-46ad-a591-08dd80ece4a2,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214}	None	2025-04-21 15:55:16
03534bf4-5cf4-4c97-ab79-157d331496f6	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:b80f4cf8-66d4-fee1-5e24-08dd80ece3bd,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:55:00Z,te:2025-04-21T15:56:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:e04de8c4-0aad-46ad-a591-08dd80ece4a2,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:f215a16379052a42d5579a3e7dd65214}	None	2025-04-21 15:55:09
765a0e66-aef5-4b9a-bca8-57070b382cfa	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-21T15:55:09.2980113Z,te:2025-04-21T15:55:09.2980113Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:Kimaura.Broomfield@microsoft.com,sip:,imsgid:7c8abd01-7dd0-46e3-9adb-555c56b88816@SJ5PPF1EED2E381.namprd11.prod.outlook.com,srt:1,trc:elainepaquet@MerchantsFleet.com,ms:Copilot/m365 offers,sid:e04de8c4-0aad-46ad-a591-08dd80ece4a2,aii:0c659557-a318-4a05-94f2-08dd7d2ceba5,md:2025-04-16T21:23:24.2008818Z,etps:SubmissionId:dc18b5cd-d25b-4d3f-5e24-08dd80ece3bd,lon:UserSubmission}	None	2025-04-21 15:55:09
fc48099d-f388-4185-a1d8-7552eaacb201	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{aig:bf607b0f-fe53-5c48-1248-08dd80ecd6ab,f3u:phishing@merchantsfleet.com,ts:2025-04-21T15:54:00Z,te:2025-04-21T15:55:00Z,op:UserSubmission,wl:SecurityComplianceCenter,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,tdc:1,reid:0f917fc4-07a8-428c-e346-08dd80ecd7da,wsrt:0001-01-01T00:00:00,mdt:u,rid:5e109db2-f860-4d79-8faf-aed562f1d58d,cid:b26a5770-0c38-434a-9380-3a3c2c27bbb3,ad:This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.3,lon:UserSubmission,an:Email reported by user as malware or phish,sev:Low,ail:https://security.microsoft.com/mtp-investigation/urn:SubmissionInvestigation:96e701744abbfa4095ecec79a78c34e3}	None	2025-04-21 15:54:56
51542583-ec2c-4bd7-b32e-95dff370d0be	PHISHING@MERCHANTSFLEET.COM	None	None	Low	{etype:User,eid:phishing@merchantsfleet.com,tid:74e16038-e7dd-4392-b38a-5a2b6d6e3a25,ts:2025-04-21T15:54:47.8562118Z,te:2025-04-21T15:54:47.8562118Z,op:UserSubmission,tdc:1,suid:phishing@merchantsfleet.com,ut:Regular,ssic:0,tsd:Kimaura.Broomfield@microsoft.com,sip:,imsgid:816fd45d-9197-4042-8346-20f43b644040@DS0PR11MB7560.namprd11.prod.outlook.com,srt:1,trc:elainepaquet@MerchantsFleet.com,ms:}Copilot and security,sid:0f917fc4-07a8-428c-e346-08dd80ecd7da,aii:9e04fe9b-5601-4204-17f5-08dd7d2d0aff,md:2025-04-16T21:24:16.7968757Z,etps:SubmissionId:4215de63-58e9-48ec-1248-08dd80ecd6ab,lon:UserSubmission}	None	2025-04-21 15:54:48