URL blocked by SOPHOS EDR(30 DAYS)_2025-04-23_07-30-58.pdf

superadmin@eras

EVENT ID	ACCOUNT NAME	CREATION TIME	SOURCE USERNAME	IP ADDRESS	MESSAGE	WEEK
608ac09a-f2fb-4c54-b4fe-1b3c22 4eeaea	AIRINVESTIGATION	2025-04-20 16:20:39	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-20T16:16:00Z,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:[{Sid:1,Id:urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:513025ffa9e27a3e52fe3f0312ac0129],Intent:Probing,ResourceIdentifiers:[{Sid: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}	Week4(2025-04-14 to 2025-04-20)
7131d6cf-5f61-4bec-a977-f0e72f9b3bab	AIRINVESTIGATION	2025-04-18 17:39:35	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T17:33:00Z,EndTimeUtc:2025-04-18T17:34:00Z,TimeGenerated:2025-04-18T17:34:25.9933333Z,ProcessingEndTime:2025-04-18T17:39:26.7774149Z,Status:InProgress,Severity:Low,Confidence:Low,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e6be84ca-f31b-acca-8d59-08dd7e9f2e43,SystemAlertId:null,CorrelationKey:68b0ab31-8b4e-4463-83ed-adc492b3ede1,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:cfb77bfa24627f701bf490164ce9796d,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:cfb77bfa24627f701bf490164ce9796d],Intent:Probing,ResourceIdentifiers:[{Sid: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=e6be84ca-f31b-acca-8d59-08dd7e9f2e43,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T17:39:26.7774149Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
8ae50588-1769-40a5-96d6-4e666289b5ca	AIRINVESTIGATION	2025-04-18 11:59:32	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T11:54:00Z,EndTimeUtc:2025-04-18T11:55:00Z,TimeGenerated:2025-04-18T11:54:26.3166667Z,ProcessingEndTime:2025-04-18T11:59:32.4555505Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:cb30f50a-69a4-d091-a710-08dd7e6fb602,SystemAlertId:null,CorrelationKey:dcdf2f72-6171-4075-a6b5-b1af5c81399c,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:4c6ab0c6b43eeea8483e2fbc098ffb97,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:4c6ab0c6b43eeea8483e2fbc098ffb97],Intent:Probing,ResourceIdentifiers:[{Sid: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=cb30f50a-69a4-d091-a710-08dd7e6fb602,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T11:59:32.4555505Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
c91286b3-373a-47e8-b557-5c6bf94f8ba7	AIRINVESTIGATION	2025-04-18 19:22:13	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T19:17:00Z,EndTimeUtc:2025-04-18T19:18:00Z,TimeGenerated:2025-04-18T19:17:31.3933333Z,ProcessingEndTime:2025-04-18T19:21:59.9509779Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:8b46e28c-952d-34af-f880-08dd7eada965,SystemAlertId:null,CorrelationKey:33bbe689-121e-4edd-b66c-62bec5c9f00d,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:1fd8075391b862835e81bc8c7c9c3779,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:1fd8075391b862835e81bc8c7c9c3779],Intent:Probing,ResourceIdentifiers:[{Sid: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=8b46e28c-952d-34af-f880-08dd7eada965,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T19:21:59.9509779Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
4d5f8c2a-670a-4dff-9541-1cd66c068263	AIRINVESTIGATION	2025-04-18 19:22:04	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T19:17:00Z,EndTimeUtc:2025-04-18T19:18:00Z,TimeGenerated:2025-04-18T19:17:31.3933333Z,ProcessingEndTime:2025-04-18T19:21:59.9509779Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:8b46e28c-952d-34af-f880-08dd7eada965,SystemAlertId:null,CorrelationKey:33bbe689-121e-4edd-b66c-62bec5c9f00d,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:1fd8075391b862835e81bc8c7c9c3779,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:1fd8075391b862835e81bc8c7c9c3779],Intent:Probing,ResourceIdentifiers:[{Sid: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=8b46e28c-952d-34af-f880-08dd7eada965,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T19:21:59.9509779Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
fbf48e27-7b10-4c18-8379-83e25a100954	AIRINVESTIGATION	2025-04-18 19:12:02	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T19:06:00Z,EndTimeUtc:2025-04-18T19:07:00Z,TimeGenerated:2025-04-18T19:06:52.9666667Z,ProcessingEndTime:2025-04-18T19:11:59.5644998Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:4e4a63c0-3848-b7fd-d362-08dd7eac0e4a,SystemAlertId:null,CorrelationKey:ec6dc112-79c3-4878-8692-6bf48f85247e,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:5ae6a41ab4688f8c4ef6f2428edc3db4,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:5ae6a41ab4688f8c4ef6f2428edc3db4],Intent:Probing,ResourceIdentifiers:[{Sid: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=4e4a63c0-3848-b7fd-d362-08dd7eac0e4a,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T19:11:59.5644998Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
6376dd89-3080-409d-8ba9-6648616887cd	AIRINVESTIGATION	2025-04-18 18:09:31	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T18:06:00Z,EndTimeUtc:2025-04-18T18:07:00Z,TimeGenerated:2025-04-18T18:06:54.05Z,ProcessingEndTime:2025-04-18T18:09:29.842023Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:3888fb66-c680-88b8-f1e2-08dd7ea3cbdb,SystemAlertId:null,CorrelationKey:74f65dd2-aae2-447b-b324-949de3492778,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:ee46721bdc4c00729a54939f3bc0cc1b,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:ee46721bdc4c00729a54939f3bc0cc1b],Intent:Probing,ResourceIdentifiers:[{Sid: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=3888fb66-c680-88b8-f1e2-08dd7ea3cbdb,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T18:09:29.842023Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
126f02e5-c808-4068-bf30-1659251d6777	AIRINVESTIGATION	2025-04-18 17:44:36	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T17:33:00Z,EndTimeUtc:2025-04-18T17:34:00Z,TimeGenerated:2025-04-18T17:34:25.9933333Z,ProcessingEndTime:2025-04-18T17:44:28.228123Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e6be84ca-f31b-acca-8d59-08dd7e9f2e43,SystemAlertId:null,CorrelationKey:bae632eb-9752-4265-9a42-740fece61eff,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:cfb77bfa24627f701bf490164ce9796d,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:cfb77bfa24627f701bf490164ce9796d],Intent:Probing,ResourceIdentifiers:[{Sid: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=e6be84ca-f31b-acca-8d59-08dd7e9f2e43,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T17:44:28.228123Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
2c10bd44-203f-4009-bee2-b0f545b47064	AIRINVESTIGATION	2025-04-18 17:39:29	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T17:33:00Z,EndTimeUtc:2025-04-18T17:34:00Z,TimeGenerated:2025-04-18T17:34:25.9933333Z,ProcessingEndTime:2025-04-18T17:39:26.7774149Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:e6be84ca-f31b-acca-8d59-08dd7e9f2e43,SystemAlertId:null,CorrelationKey:68b0ab31-8b4e-4463-83ed-adc492b3ede1,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:cfb77bfa24627f701bf490164ce9796d,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:cfb77bfa24627f701bf490164ce9796d],Intent:Probing,ResourceIdentifiers:[{Sid: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=e6be84ca-f31b-acca-8d59-08dd7e9f2e43,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T17:39:26.7774149Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
6b8f48d7-e96a-4737-86db-b1e453f21ffb	AIRINVESTIGATION	2025-04-18 13:26:38	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T13:22:00Z,EndTimeUtc:2025-04-18T13:23:00Z,TimeGenerated:2025-04-18T13:22:18.64Z,ProcessingEndTime:2025-04-18T13:26:38.0689648Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:056d858d-ab7b-c8a2-8a3e-08dd7e7c0ab9,SystemAlertId:null,CorrelationKey:c4e66037-56a3-4fcb-8f5d-eacfbbc3aecf,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:684743c96171eb0672b03cd3d8a99c6d,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:684743c96171eb0672b03cd3d8a99c6d],Intent:Probing,ResourceIdentifiers:[{Sid: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=056d858d-ab7b-c8a2-8a3e-08dd7e7c0ab9,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T13:26:38.0689648Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)
c72dc39c-950b-4d62-b5c5-7859ca5a5ec0	AIRINVESTIGATION	2025-04-18 12:55:59	AirInvestigation	None	{Version:3.0,VendorName:Microsoft,ProviderName:OATP,AlertType:b26a5770-0c38-434a-9380-3a3c2c27bbb3,StartTimeUtc:2025-04-18T12:52:00Z,EndTimeUtc:2025-04-18T12:53:00Z,TimeGenerated:2025-04-18T12:52:09.43Z,ProcessingEndTime:2025-04-18T12:55:59.4278594Z,Status:InProgress,Severity:Low,ConfidenceLevel:Unknown,ConfidenceScore:1.0,IsIncident:false,ProviderAlertId:c33bf8c0-39f7-7669-8f59-08dd7e77d3c8,SystemAlertId:null,CorrelationKey:fd2c8989-58f4-444f-8a35-7b9b5977f007,Investigations:[{Sid:1,Id:urn:SubmissionInvestigation:84b06f53494e7eb07bef4e168565dbd1,InvestigationStatus:Running}],InvestigationIds:[urn:SubmissionInvestigation:84b06f53494e7eb07bef4e168565dbd1],Intent:Probing,ResourceIdentifiers:[{Sid: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=c33bf8c0-39f7-7669-8f59-08dd7e77d3c8,Category:null,Label:alert,Type:webLink}],Metadata:{CustomApps:null,GenericInfo:null},LogCreationTime:2025-04-18T12:55:59.4278594Z,MachineName:BN8NAM12BG402,SourceTemplateType:Activity_Single,Category:ThreatManagement,SourceAlertType:System}	Week4(2025-04-14 to 2025-04-20)