

3ª REUNIÃO DA CSI

OUT/2025

Tópicos

☐ Pendências da última reunião

☐ Ações realizadas

☐ Ações futuras

☐ Propostas de Melhorias

Pendências Reuniões Anteriores

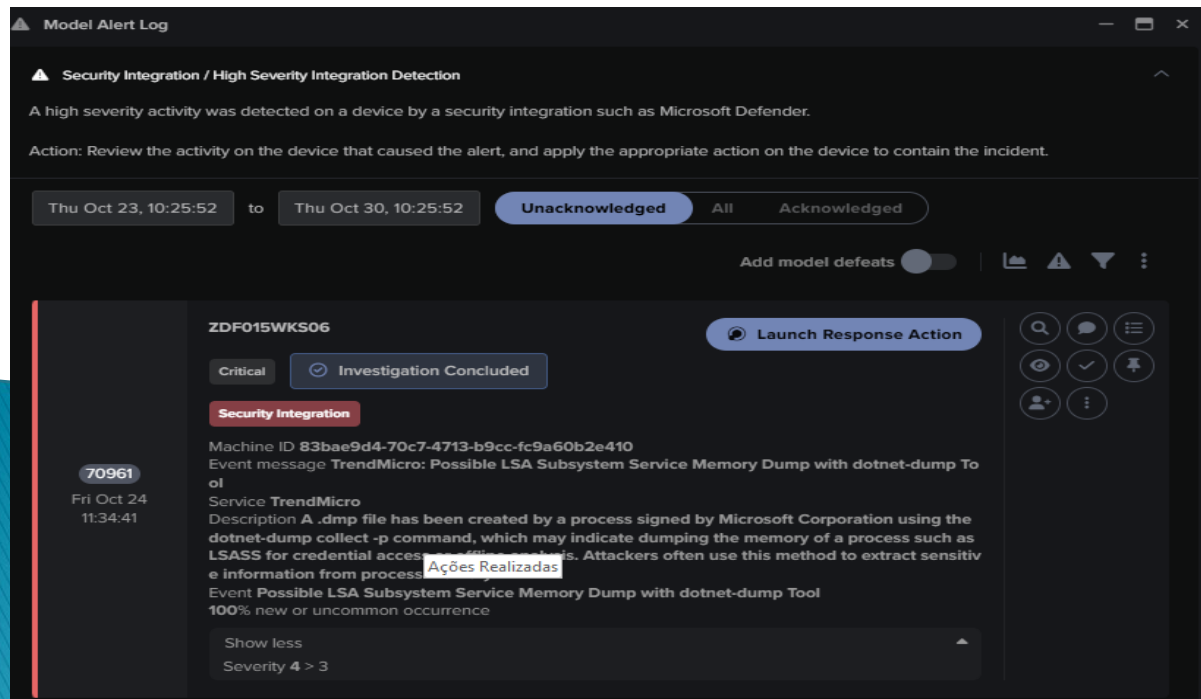
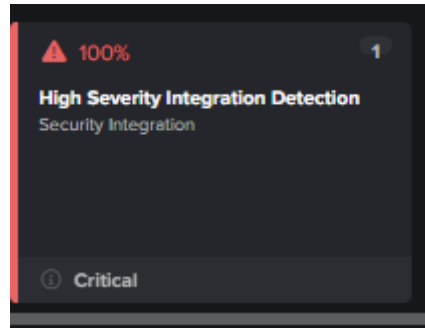
1. Ativação de bloqueio dos dispositivos de armazenamento externo
2. Ativação da automação no XDR TrendMICRO
3. Bloqueio do uso do WhatsApp Web

Ações Realizadas

1. Monitorar ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...)
2. Atuar preventivamente nos dispositivos
3. Tratar eventos reportados (canais de comunicação e relatórios)
4. Solicitar atualização no ambiente (vulnerabilidades críticas)
5. Propor ações de melhoria no ambiente

Ações Realizadas

1. Monitora o ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...)



Ações Realizadas

1. Monitora o ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...)

RESUMO

Alerta de modelo investigado pelo Cyber AI Analyst: Security Integration/High Severity Integration Detection

O Cyber AI Analyst da Darktrace investigou o alerta desta violação do modelo e a atividade circundante; os resultados desta investigação são apresentados abaixo.

Para encontrar eventos ou comportamentos que valem a pena serem apresentados aos analistas humanos, o Cyber AI Analyst identifica hipóteses relevantes para a atividade incomum que acionou a violação do modelo e tenta encontrar evidências que se apliquem a cada teoria. Essas evidências são coletadas por meio de uma série de etapas de investigação baseadas em IA; somente aqueles que forem comprovados com sucesso e considerados de interesse resultarão em um evento de incidente do Cyber AI Analyst.

Nenhum incidente de analista de IA cibernética foi criado para este alerta de modelo, [create manual incident](#)

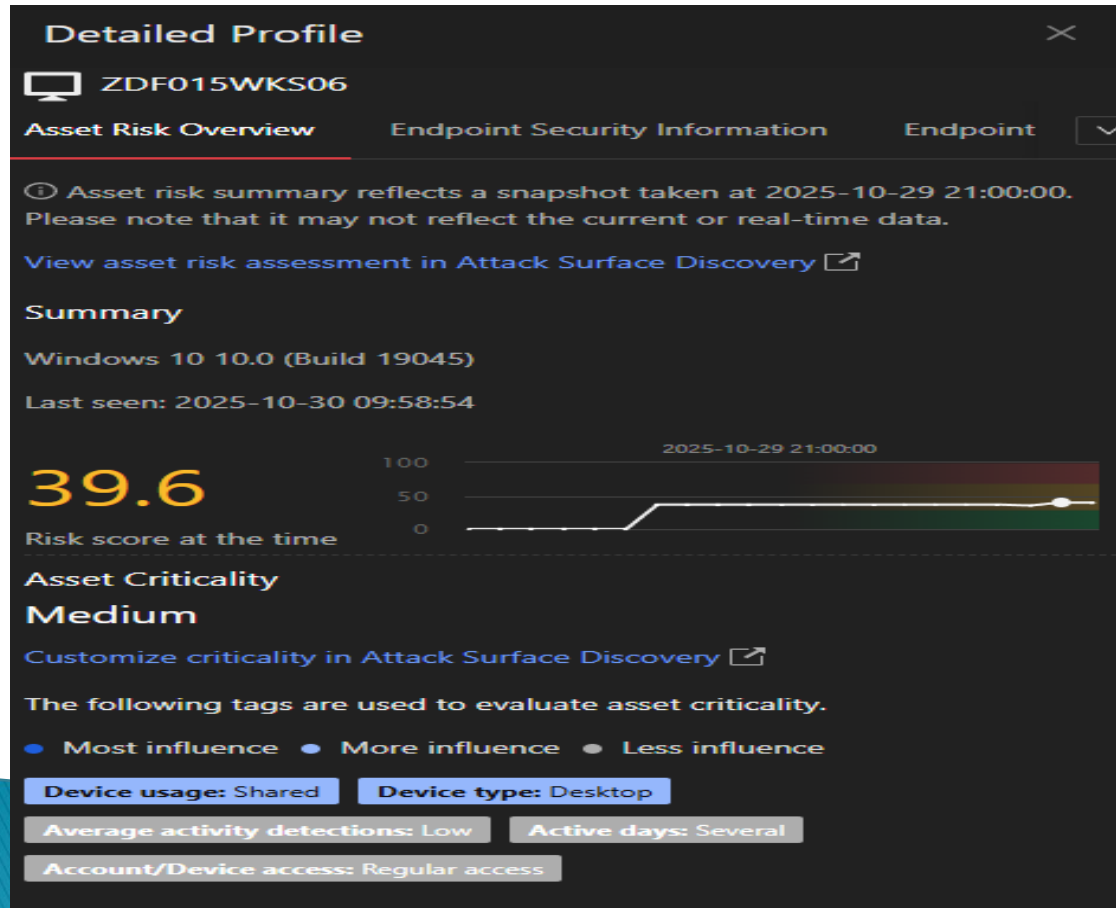
O Cyber AI Analyst identificou as seguintes hipóteses como relevantes para o alerta de violação do modelo:

TRANSPORT LAYER SCANNING

Hipótese	Transport Layer Scanning
Status	Investigação concluída
Descrição	Identifies transport layer network scanning, which is often used for reconnaissance by malicious actors.
Resultado	Os resultados desta análise foram suprimidos por terem sido avaliados como insuficientemente interessantes pelo Cyber AI Analyst

Ações Realizadas

1. Monitora o ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...)



**Tribunal
Regional
Eleitoral-DF**

[Back](#)

ZDF015WKS06

- Risk Assessment
- Asset Risk Graph
- Public Cloud App Activity
- Local Apps
- Users
- Certificates
- Open Ports and Services
- Asset Profile
- Policy

RISK SCORE ⓘ

The risk score is currently **39.6**, categorized as **Medium risk**. It has decreased by **0.4** from its previous value.

Risk factors contributing to the score:

- Account compromise
- Vulnerabilities
- Activity and behaviors
- Public cloud app activity
- System configuration
- XDR detection
- Threat detection
- Security configuration
- Predictive analytics

Risk Score Timeline:

The timeline shows the risk score over time from October 1st to October 29th. The score remains low until around October 15th, where it rises sharply to approximately 39.6 and remains stable thereafter. A vertical line at October 19th indicates a significant event.

Date	Risk Score	At-risk events detected
10-01	~0	0
10-15	~0	0
10-19	~39.6	0
10-29	~39.6	~2

RISK INDICATORS

Risk factor: All | Status: New | Add filter (1) | Export

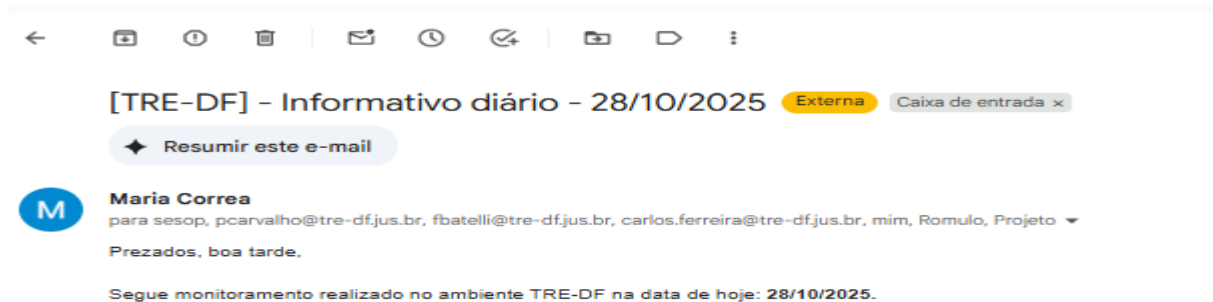
Event risk level: All | Reset

	Risk factor	Risk event	Data source / processor	Event risk level	Detected ↓	Case
< >	System configuration	Windows Device Encryption Disabled	Endpoint Sensor	Medium	2025-10-30 06:20:08	-
< >	System configuration	Deprecated OS Version Identified	Endpoint Sensor	Medium	2025-10-29 15:13:48	-
< >	Public cloud app activ...	Risky Cloud App Access	Standard Endpoint Protection	Medium	2025-10-29 02:42:00	-

System configuration		Deprecated OS Version Identified	Endpoint Sensor	Medium	2025-10-29 15:13:48	-	
		The device OS version Windows 10 Version 22H2 for x64-based Systems (22H2) is no longer supported. Remediation: Upgrade the operating system.					
eventRiskLevel:		Medium					
osName:		Windows 10 Version 22H2 for x64-based Systems					
assetCriticality:		6					
osVersion:		22H2					
osVersionInternal:		10.0.19045					
eosDate:		2025-10-14					

Ações Realizadas

1. Monitora o ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...)



Tipo de Violação: Spyware/Grayware

Informação: Se referem aos aplicativos ou arquivos não classificados como vírus ou cavalo de Troia, mas que podem afetar negativamente o desempenho dos endpoints na rede e introduzir riscos significantes legais, de segurança, de confidencialidade à organização.

Generated	Received	Endpoint	Product/Endpoint	Spyware/Grayware	File Name	File Path	Scan Type	User	Action
10/28/2025 12:11:27	10/28/2025 12:11:56	ZDF018WKS25	10.49.28.165	PUA.Win32.Bundler.AN	PDF24-PDF-CREATOR-11.23.0-L...	C:\Users\MARCIANO.SILVA\Des...	Real-time Scan	marciano.silva	File cleaned
10/28/2025 10:19:13	10/28/2025 10:19:55	ZDF018WKS26	10.49.28.166	PUA.Win32.Bundler.AN	PDF24-PDF-CREATOR-11.23.0-L...	C:\Users\THAYNARA.NAKAYAMA...	Real-time Scan	giela.silva	File cleaned
10/28/2025 00:19:10	10/28/2025 00:19:42	ZDF018WKS23	10.49.28.163	PUA.Win32.Bundler.AN	pdf24-pdf-creator-11.23.0-inst...	C:\Users\sonaya.marques\Desk...	Scheduled Scan	sonaya.marques	File cleaned
10/28/2025 00:14:40	10/28/2025 00:15:42	ZDF018WKS31	10.49.28.235	PUA.Win32.Bundler.AN	pdf24-pdf-creator-11.23.0-inst...	C:\Users\lidiard.oliveira\Deskto...	Scheduled Scan	candice.naoum	File cleaned

Caminho(s) do(s) arquivo(s):

- C:\Users\MARCIANO.SILVA\Desktop\PDF24-PDF-CREATOR-11.23.0-INSTALLER_C-BEVE2.EXE
- C:\Users\THAYNARA.NAKAYAMA\Desktop\PDF24-PDF-CREATOR-11.23.0-INSTALLER_C-BEVE2.EXE
- C:\Users\sonaya.marques\Desktop\pdf24-pdf-creator-11.23.0-installer_C-bEve2.exe
- C:\Users\lidiard.oliveira\Desktop\pdf24-pdf-creator-11.23.0-installer_C-bEve2.exe

AÇÃO DA FERRAMENTA: Realizada a limpeza pelo sistema Trend Micro.

OBSERVAÇÃO: Indicada a varredura no endpoint citado.

Ações

☐	ID	TÍTULO	DESCRIÇÃO	DATA DE ABERTURA	LOCALIZAÇÃO	REQUERENTE - REQUERENTE	ATRIBUÍDO - TÉCNICO	ATRIBUÍDO - GRUPO TÉCNICO	TEMPO PARA SOLUÇÃO + PROGRESSO	STATUS	URGÊNCIA	IMPACTO	ÚLTIMA ATUALIZAÇÃO
☐	12 671	Alerta TrendVision	Prezados, Solicito a remoção urgente do aplicativo PDF24 Creator (versão 11.23.0) do DESKTOPS listados abaixo, por ser classificado como PUA (Potentially Unwanted Application) e representar risco à segurança. ZDF018 (...) 🗨️	28-10-2025 10:37	COIE - AGSI	Marcelo Nogueira Lino <i>i</i>		STIC > COIE > HELPDESK		Em atendimento (atribuído)	Média	Médio	28-10-2025 18:06

2. Atuar Preventivamente nos dispositivos

1. Monitorar

2. Identificar

3. Analisar

4. Tratar

5. Erradicar

Regramento Legal:

- ❑ **PARTIC (Art. 15, 20, 23, 28, 30, 33, 46, e Capítulo XVII)**
- ❑ **PSI TSE**
- ❑ **Res. 396/2021 do CNJ**
- ❑ **Portaria PR TRE-DF nº 69/2023 (Capítulos IV, VII e VIII)**

Ações Futuras

Propostas de Melhoria

1. Bloquear dispositivo de armazenamento externo (uso de USB).
2. Criar VLANS específicas para DEV, HOMOLOG e PROD.
3. Ampliar proteção de aplicações no F5 (Big IP).
4. Identificar e desabilitar placas WiFi nos desktops.
5. Atualizar solução de análise de vulnerabilidades (TENABLE).
6. Migrar solução VARONIS para nuvem (SaaS.)
7. Atualizar pacote Office.

OBS: Dependente de apoio das equipes da SETEL, SESOP e SEAPU

Ações Futuras

Propostas de Melhoria

8. Ampliar a replicação do backup (2026)

9. PPINC – 100%. (Dez/2025)

10. PGCRC – 100%. (Dez/2025)

11. PIILC – 100%. (Dez/2025)

12. Entregar BIA e PCN. (Dez/2025)

13. Projeto de solução de *ZTNA + *SWG + IGA e NGFW + Microseg.

SEI 0002653-81.2024.6.07.8100

Obrigado