Tribunal Regional Eleitoral-DF

3ª REUNIÃO DA CSI

OUT/2025

Tópicos

Tribunal Regional Eleitoral-DF

- Pendências da última reunião
- Ações realizadas
- Ações futuras
- Propostas de Melhorias

Pendências Reuniões Anteriores

Tribunal Regional Eleitoral-DF

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

Tribunal Regional Eleitoral-DF

1. Monitorar ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...

2. Atuar preventivamente nos dispositivos

3. Tratar eventos reportados (canais de comunicação e relatórios)

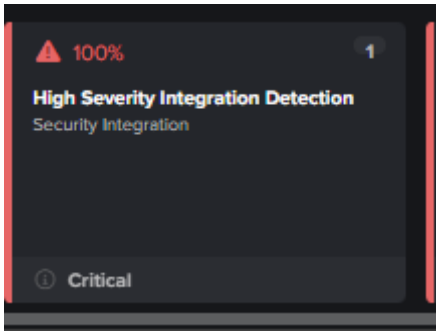
4. Solicitar atualização no ambiente (vulnerabilidades críticas)

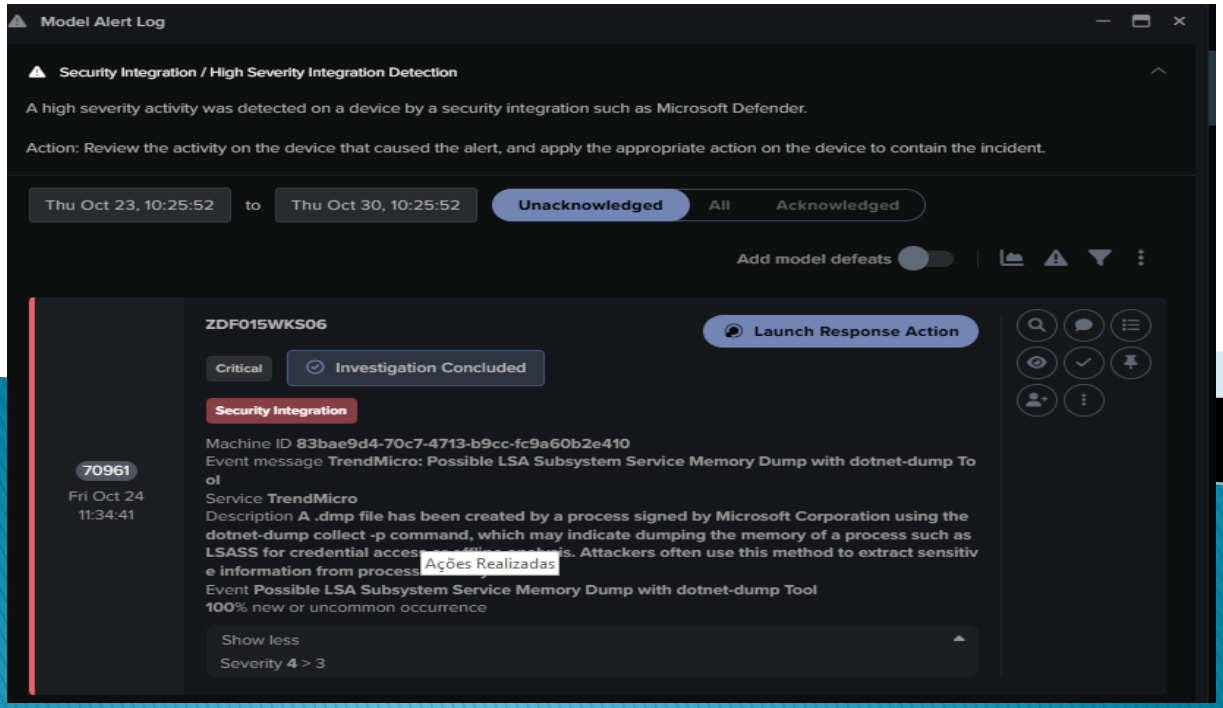
5. Propor ações de melhoria no ambiente

Ações Realizadas

Tribunal Regional Eleitoral-DF

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

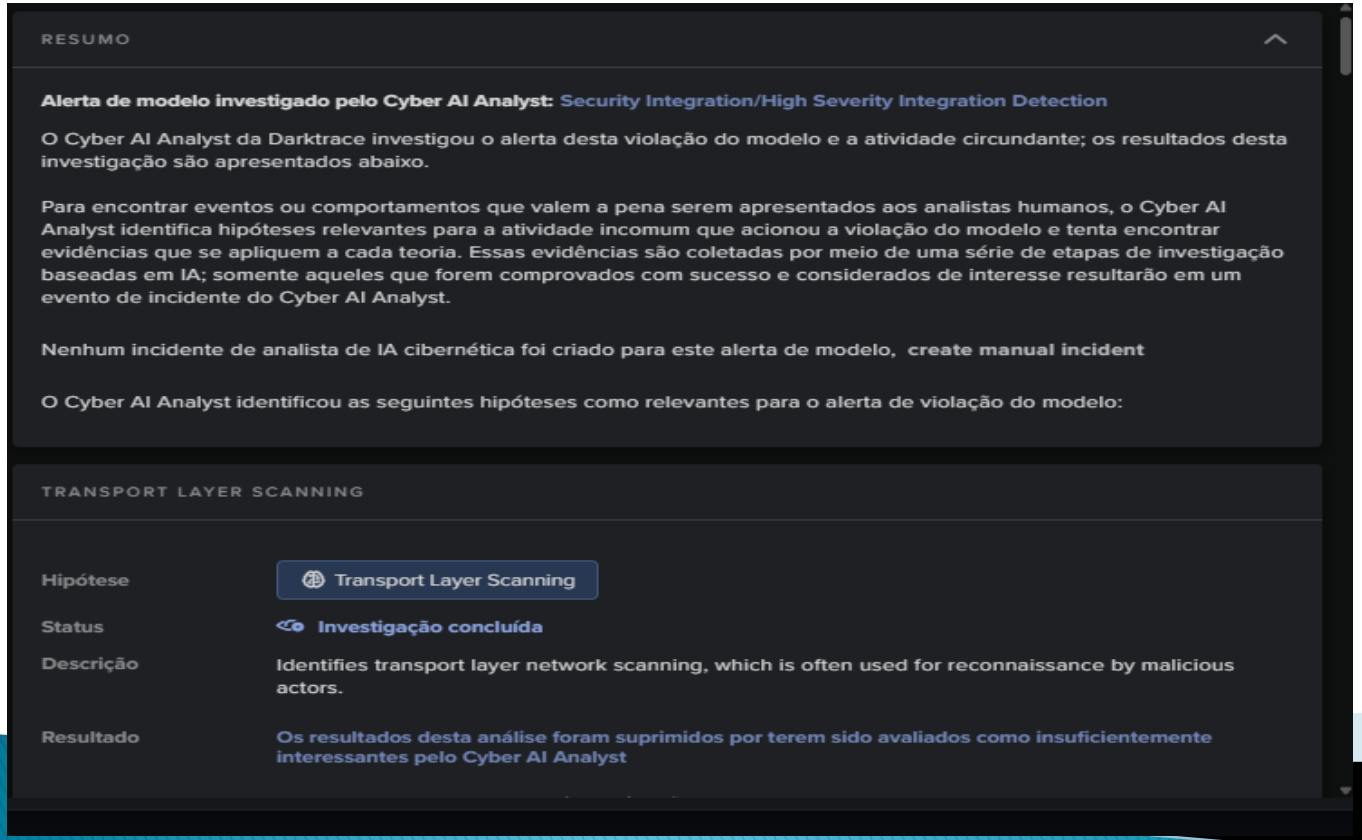




Ações Realizadas

Tribunal Regional Eleitoral-DF

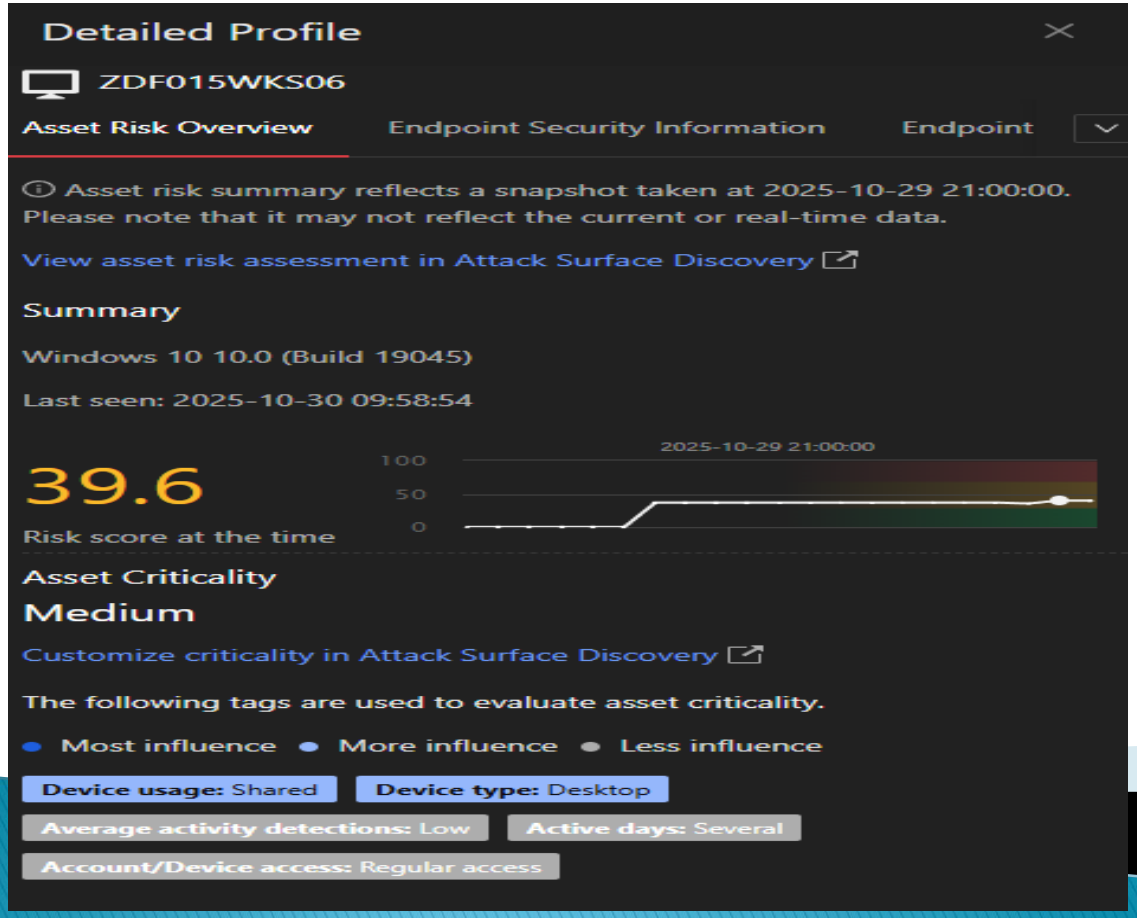
1. Monitora o ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...



Ações Realizadas

Tribunal Regional Eleitoral-DF

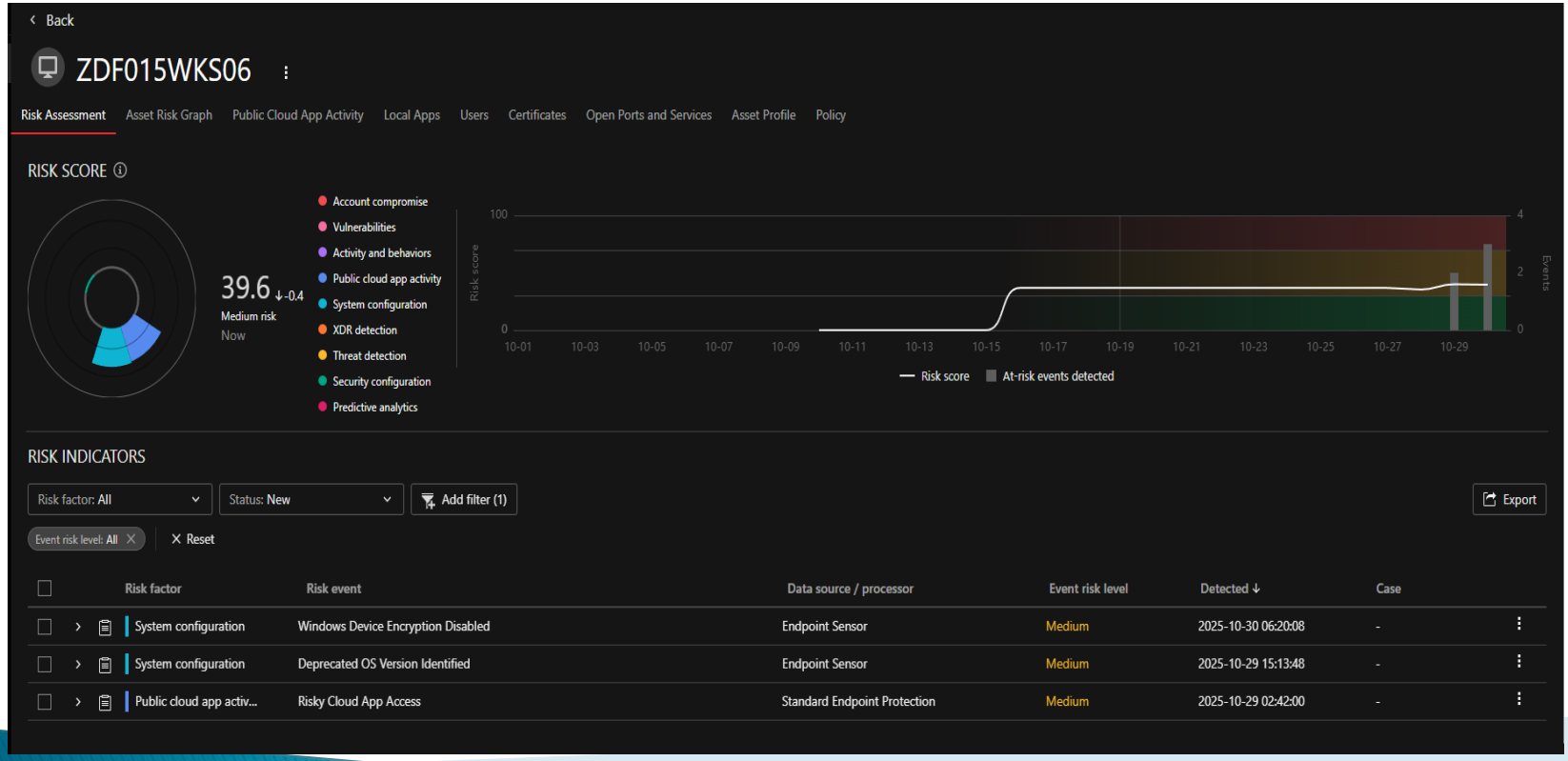
1. Monitora o ambiente (XDR, DARKTRACE, TENABLE, IVANTI, ...

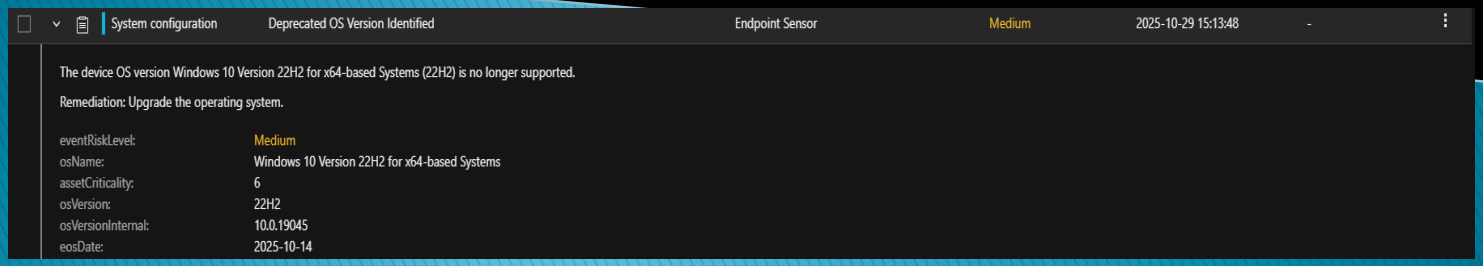


Ações Realizadas

Tribunal Regional Eleitoral-DF

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





Ações Realizadas

Tribunal Regional Eleitoral-DF

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

[TRE-DF] - Informativo diário - 28/10/2025 Externa Caixa de entrada ×

Resumir este e-mail

Maria Correa
para sesop, pcarvalho@tre-df.jus.br, fbatelli@tre-df.jus.br, carlos.ferreira@tre-df.jus.br, mim, Romulo, Projeto

Prezados, boa tarde.

Segue monitoramento realizado no ambiente TRE-DF na data de hoje: **28/10/2025.**

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/Endpoin...	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-I...	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-I...	C:\Users\THAYNARA.NAKAYAM...	Real-time Scan	gisela.seixas	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-insta...	C:\Users\soraya.marques\Deskt...	Scheduled Scan	soraya.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-insta...	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\soraya.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		STIC > COIE > HELPDESK		Em atendimento (atribuído)	Média	Médio	28-10-2025 18:06

Processo

Tribunal Regional Eleitoral-DF

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 Capitulo 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

Tribunal Regional Eleitoral-DF

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

Tribunal Regional Eleitoral-DF

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

Tribunal Regional Eleitoral-DF

Obrigado