Tribunal Regional Eleitoral-DF

REUNIÃO EXTRAORDINÁRIA DA CSI 05/2025

Tópicos

Tribunal Regional Eleitoral-DF

- Reporte incidentes recentes
- Ações futuras e Melhorias

Reporte Incidentes Recentes

Tribunal Regional Eleitoral-DF

1. Usuário remoto com equipamento contaminado

2. Infecção por uso de mídia externa

3. Estagiários presos por aplicar golpes

Reporte Incidentes Recentes

Tribunal Regional Eleitoral-DF

1. Usuário remoto com equipamento contaminado

Data do incidente: 13/02/2025

Resumo do incidente: XDR – TrendMicro, identificou SEPAG-001, alerta alto de vírus, aplicativo WinVNC comprometido

Causa do incidente: Uso de pendrive contaminado, que infectou versão antiga do WinVNC com malware.

Ações realizadas:

1) Identificada usuário e IP da máquina;
2) Identificada fonte da contaminação (D:/);
3) Identificado arquivo contaminado (ferramenta de backdoor – hacktool.winvnc);
4) Laptop institucional recolhido para análise profunda;
5) Laptop formatado pela equipe da SEAPU;
6) Orientações quanto ao procedimento para uso de mídias.

Reporte Incidentes Recentes

Tribunal Regional Eleitoral-DF

2. Infecção por uso de mídia externa

Data do incidente: 12/03/2025

Resumo do incidente: XDR – TrendMicro, identificou ZDF001WKS36, alerta alto, 253 vírus.

Causa do incidente: Necessidade de cópia de mídias de processo para disponibilização para consulta pelas partes envolvidas

Ações realizadas:

1) Identificada usuária e IP da máquina;
2) Identificada fonte da contaminação (F:/);
3) Identificados arquivos contaminados (ferramentas de hacking, backdoor, exploit);
4) Desktop isolado da rede;
5) Identificamos contaminação lateral nas máquinas ZDF001WKS26 e ZDF001WKS24;
6) Senhas de todos os usuários das máquinas infectadas foram resetadas;
7) Todas as máquinas recolhidas e formatadas pela equipe da SEAPU;
8) Orientações quanto ao procedimento de cópia de mídias.
9) Instalação de equipamento específico para realização das cópias de mídias fora da rede;
10) Abertura de processo SEI relatando a ocorrência (0002195-30.2025.6.07.8100).

Reporte Incidentes Recentes

Tribunal Regional Eleitoral-DF

3. Estagiários presos por aplicar golpes

Data do incidente: 31/03/2025

Resumo do incidente: Estagiários do TRE-DF presos por aplicar golpes com documentos falsificados

Ações realizadas:

1) Contas no AD e no Google Workspace desativadas;
2) Verificados e-mails, google drive e demais serviços do Google Workspace;
3) Verificado logs dos acessos á rede e domínio do TRE-DF;

Ações Futuras e Melhorias

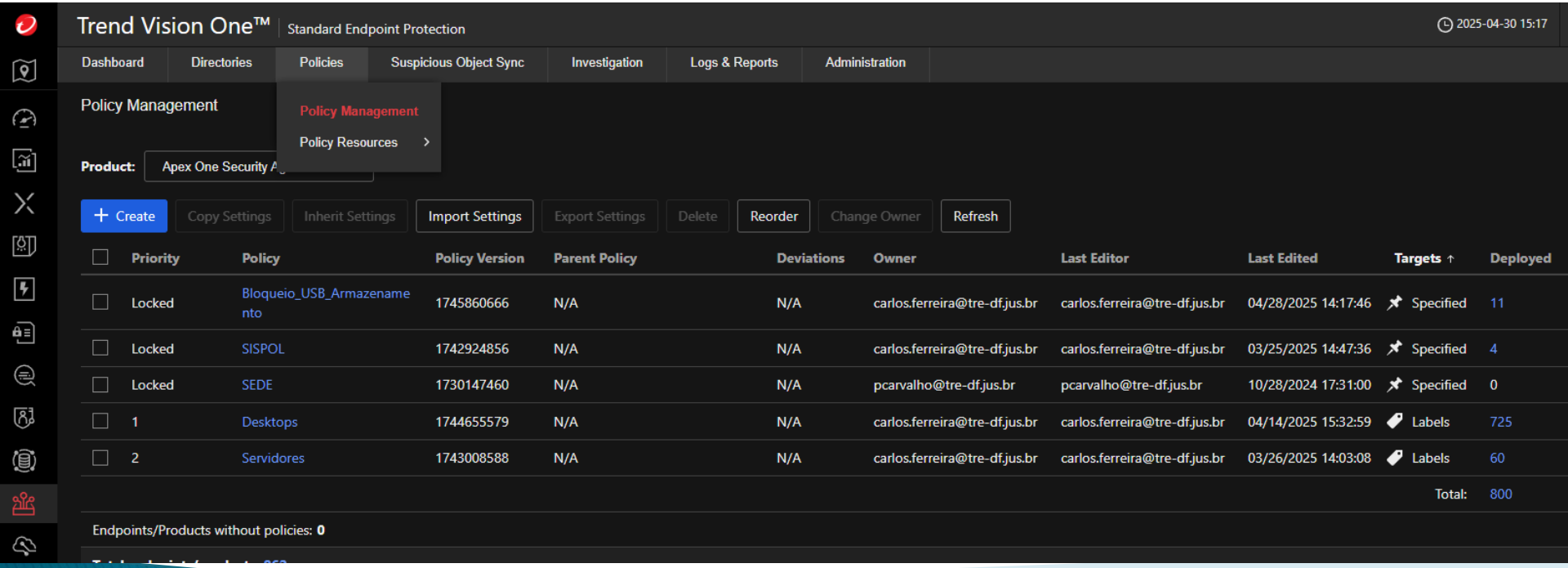
Tribunal Regional Eleitoral-DF

1. Ativação de bloqueio de dispositivo de armazenamento externo
2. Automação de isolamento de desktop da rede interna
3. Substituição do ILovePDF pelo STIRLING
4. Remoção dos links disponibilizado no Google Drive
5. Divulgação e publicidade para todos usuários antes das ativações

Ações Futuras e Melhorias

Tribunal Regional Eleitoral-DF

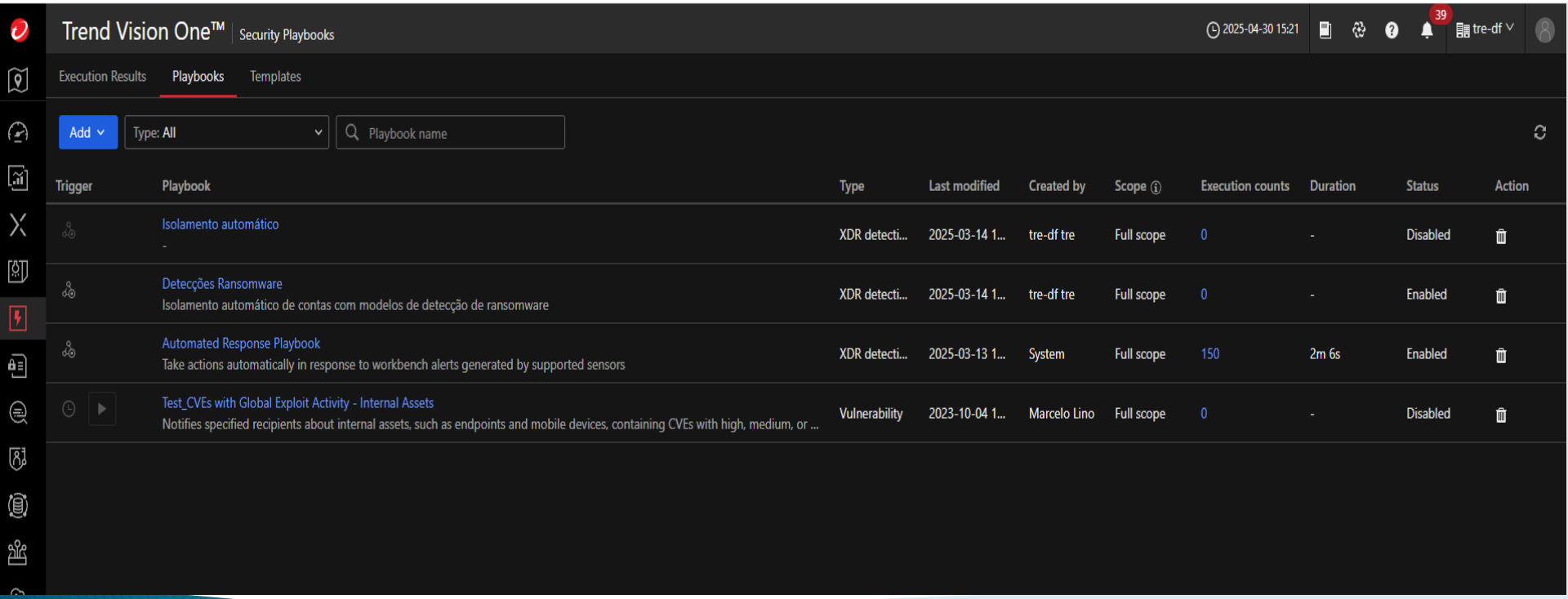
1. Ativação de bloqueio de dispositivo de armazenamento externo



Ações Futuras e Melhorias

Tribunal Regional Eleitoral-DF

2. Automação de isolamento de desktop da rede interna

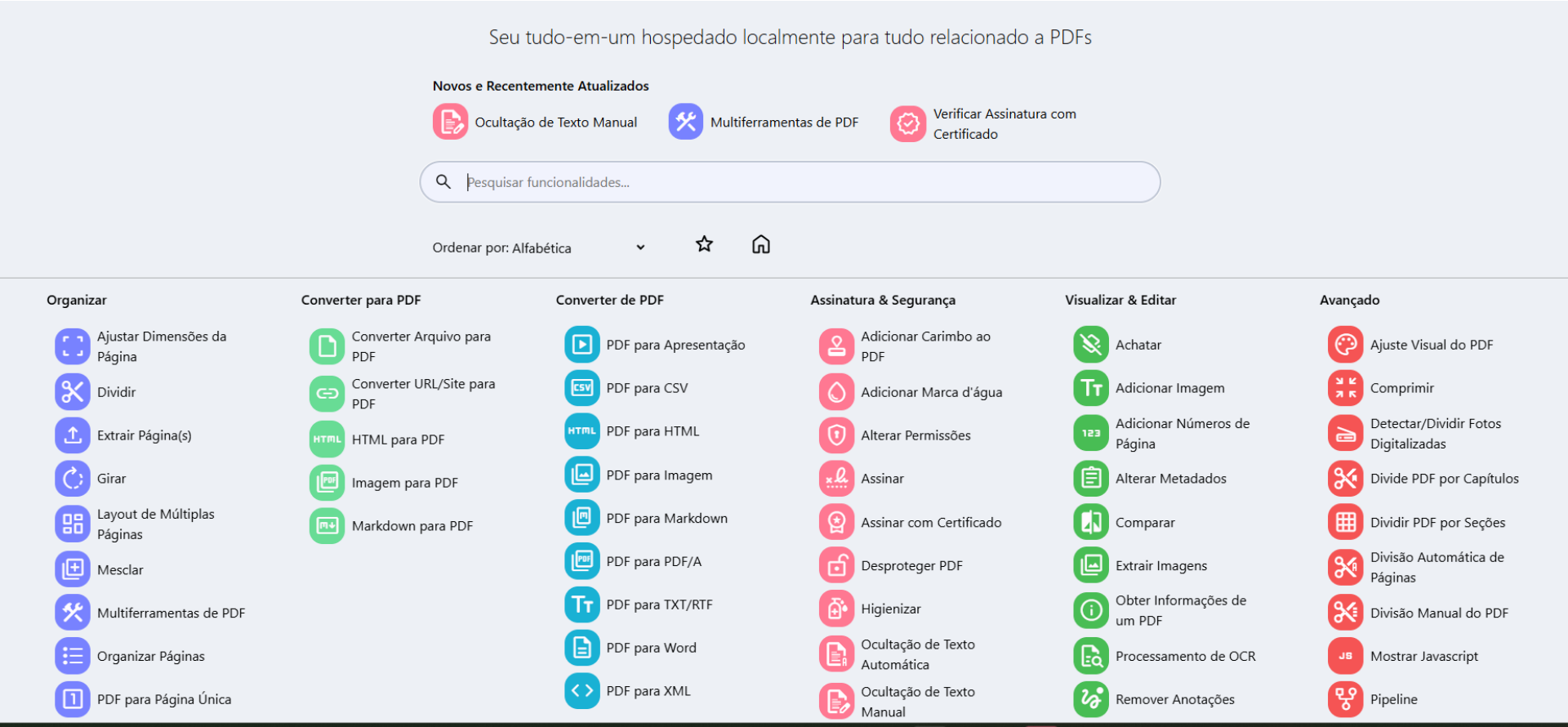


Ações Futuras e Melhorias

Tribunal Regional Eleitoral-DF

3. Substituição do ILovePDF pelo STIRLING

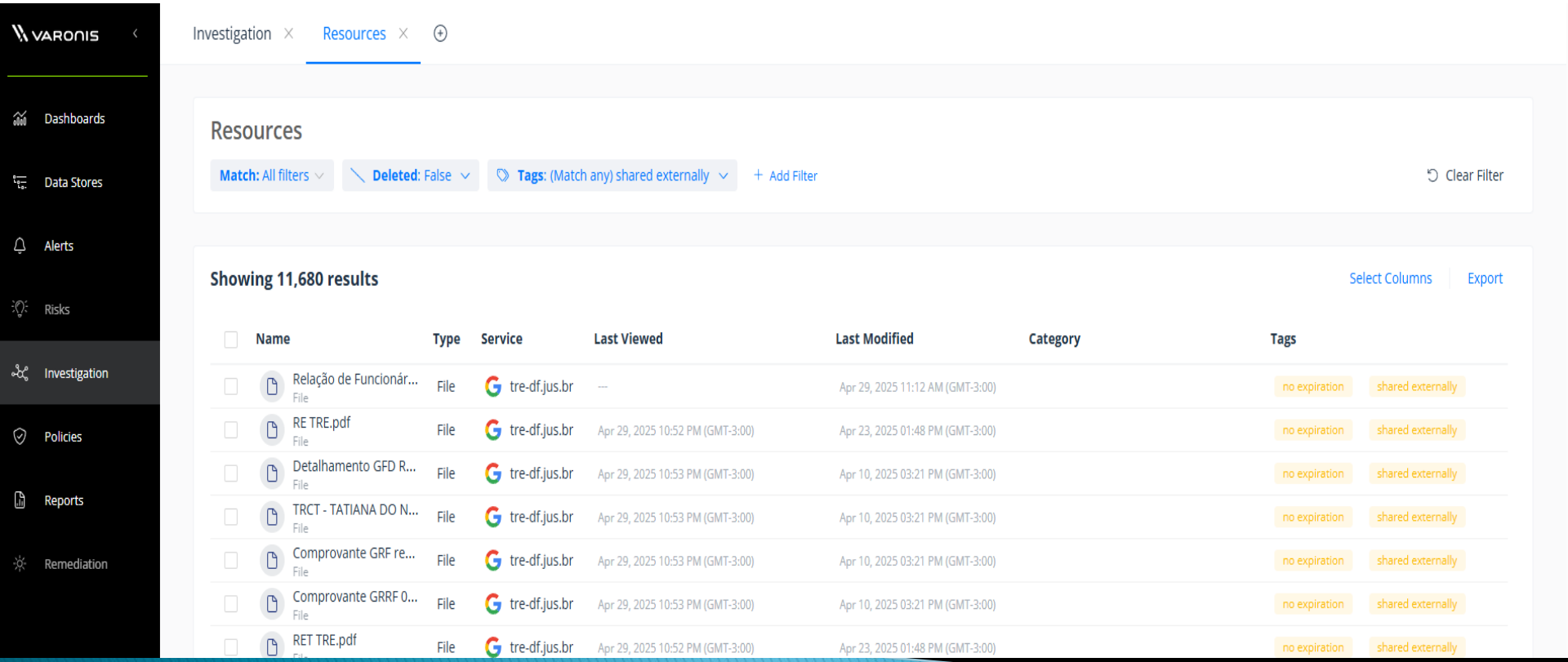
3. http://web-stirling-pdf.apps.ocp-hml.tre-df.jus.br/?lang=pt_BR



Ações Futuras e Melhorias

Tribunal Regional Eleitoral-DF

4. Remoção dos links disponibilizado no Google Drive



Tribunal Regional Eleitoral-DF

Obrigado