Tribunal Regional Eleitoral-DF

REUNIÃO DA CSI
13/02/2025

Tópicos

Tribunal Regional Eleitoral-DF

- Pendências reunião de Agosto/2024
- Ações realizadas: 3º tri_2024 até o momento
- Atividades rotineiras: Status do ambiente
- Ações futuras
- Melhorias

Pendências Última Reunião

Tribunal Regional Eleitoral-DF

1. **Proposta para utilização do Whatsapp Web**

2. **Ativação do modo autônomo do Darktrace**

3. **Sugestão para modificações na rede Wi-Fi**

Pendência Última Reunião

Tribunal Regional Eleitoral-DF

Proposta para utilização do Whatsapp Web (0000650-22.2025.6.07.8100)

TRIBUNAL REGIONAL ELEITORAL DO DF

MINUTA DE PORTARIA - TRE-DF/PR/DG/STIC/COIE

Instituir Política de Acesso aos Recursos de TIC (PARTIC), no âmbito do Tribunal Regional Eleitoral do Distrito Federal – TRE/DF.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO DISTRITO FEDERAL, no uso de suas atribuições legais e regimentais, com fundamento no artigo 9º, Inciso II da Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral – TSE, e tendo em vista o contido no Processo Administrativo SEI 0000650-22.2025.6.07.8100.

CONSIDERANDO os princípios e diretrizes constantes da Política e do Sistema Nacional de Segurança do Poder Judiciário, instituídos pela Resolução CNJ nº 435, de 28/10/2021;

CONSIDERANDO os princípios e diretrizes constantes da Política de Segurança da Informação (PSI), no âmbito da Justiça Eleitoral, instituída pela Resolução TSE Nº 23.644, de 1º/07/2021;

CONSIDERANDO os princípios e diretrizes constantes da Política de Privacidade e Proteção de Dados Pessoais, no âmbito da Justiça Eleitoral, instituída pela Resolução TSE Nº 23.650, DE 15/09/2021;

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27001:2022, que estabelece boas práticas para gestão da segurança da informação, segurança cibernética e proteção à privacidade nas organizações;

CONSIDERANDO os princípios e diretrizes constantes da Política de Acesso aos Recursos de Tecnologia da Informação - PARTIC, instituída pela Portaria da Presidência do TRE-DF Nº 183/2024, de 31/07/2024; e

CONSIDERANDO a necessidade de atualizar as regras de controle, diretrizes de proteção e responsabilidades para uso de aplicativos de mensagens instantâneas internamente e externamente no âmbito do Tribunal Regional Eleitoral do Distrito Federal.

RESOLVE

Art. 1º Instituir no âmbito do Tribunal Regional do Eleitoral do Distrito Federal - TRE-DF a Política de Uso de Aplicativos de Mensageria Instantânea.

§ 1º O processo será executado e gerenciado em conformidade com o que dispõe o anexo desta Portaria.

§ 2º O anexo desta Portaria será atualizado, sem a necessidade de elaboração de nova portaria, mediante controle documental e versionamento.

§ 3º O anexo será revisado, pela área técnica responsável, sempre que necessário, devendo o processo de revisão ser certificado nos autos em que está editada a presente portaria.

§ 4º Quando verificada a necessidade de alteração do anexo pela área técnica responsável, as modificações serão propostas ao Comitê de Gestão de Tecnologia da Informação e Comunicação - CGTIC.

§ 5º As propostas de alteração deverão ser devidamente justificadas e processadas nos autos em que está editada a presente portaria.

§ 6º Após validadas pelo CGTIC, as propostas de alteração do anexo serão submetidas à aprovação da Comissão de Segurança da Informação - CSI.

§ 7º As novas versões, após aprovadas pelo CSI, deverão ser publicadas no sítio eletrônico deste Tribunal.

Art. 2º Esta portaria entra em vigor em até 01 ano a partir da data de sua publicação.

Pendência Última Reunião

Tribunal Regional Eleitoral-DF

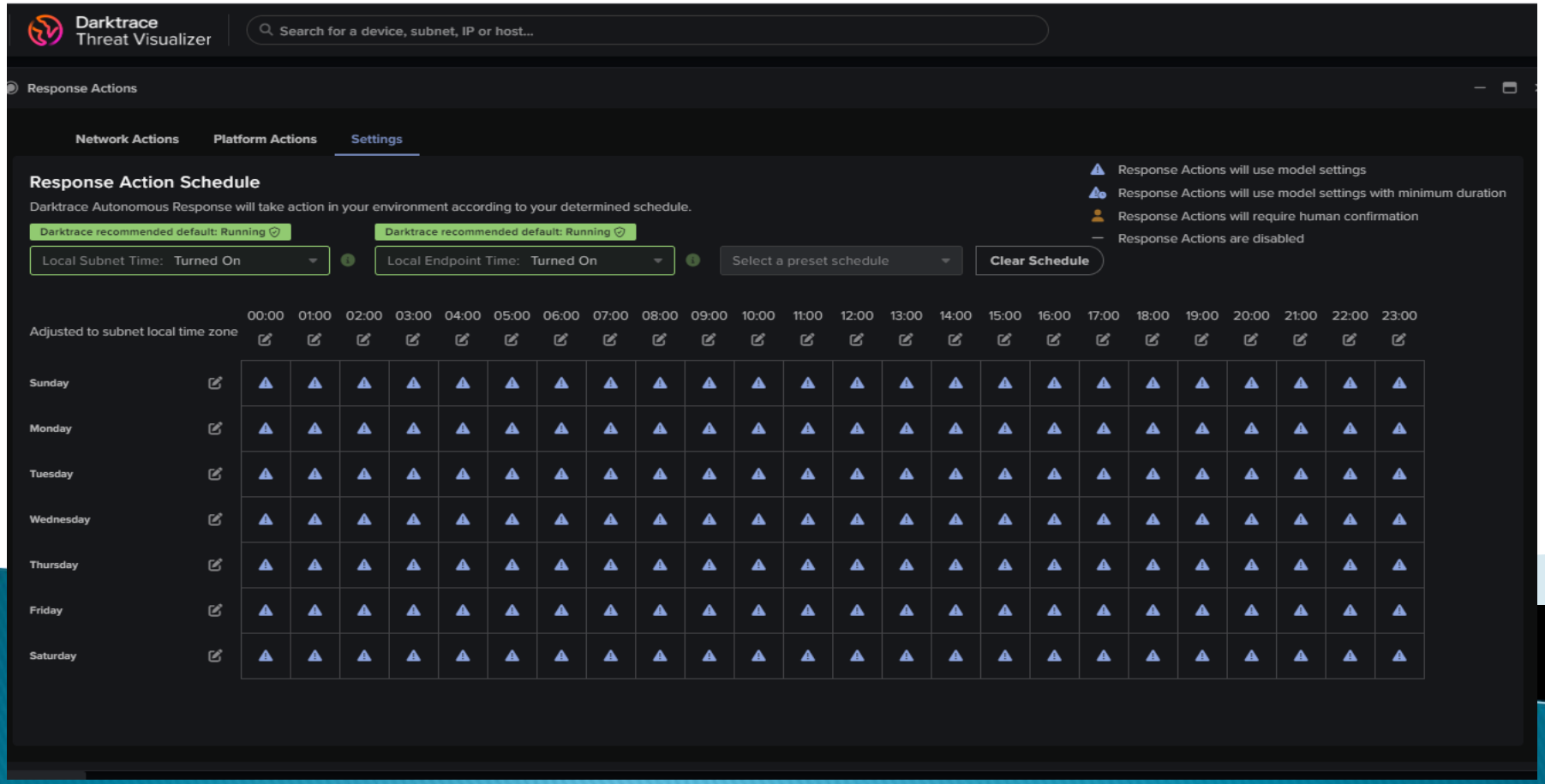
Proposta para utilização do Whatsapp Web (0000650-22.2025.6.07.8100)

- Define 03 perfis: (Art. 3º)
  - Institucional (para uso em comunicação externa);
  - Interno (para uso interno institucional)
  - Pessoal (para uso pessoal, particular)
- Propõe a homologação das ferramentas pelo CSI (WhatsApp Web Bussiness / Google Chat) (Art. 6º)
- Define que o uso do Google Chat é permitido e obrigatório para todos usuários, e que a comunicação externa pelo mesmo, excepcionalmente será autorizado (Art. 7º)
- Garante o uso do WhatsApp Web a todos os usuários que em função do serviço precisem, bastando apresentar a justificativa (comunicação externa). Solicitações excepcionais serão analisadas pelo CSI. (Art. 8º e 9º)
- Define as informações que deverão constar no WhatsApp Web para comunicações externas (Art. 10º)
- Define em quais dispositivos poderá ser utilizado o Google Chat (Art. 11)
- Define as regras básicas estabelecidas para uso do Google Chat e do WhatsApp Web (Art. 12)
- Define responsabilidades para CSI, Gestores, STIC e usuários (Art. 17 a 21)

Pendência Última Reunião

Tribunal Regional Eleitoral-DF

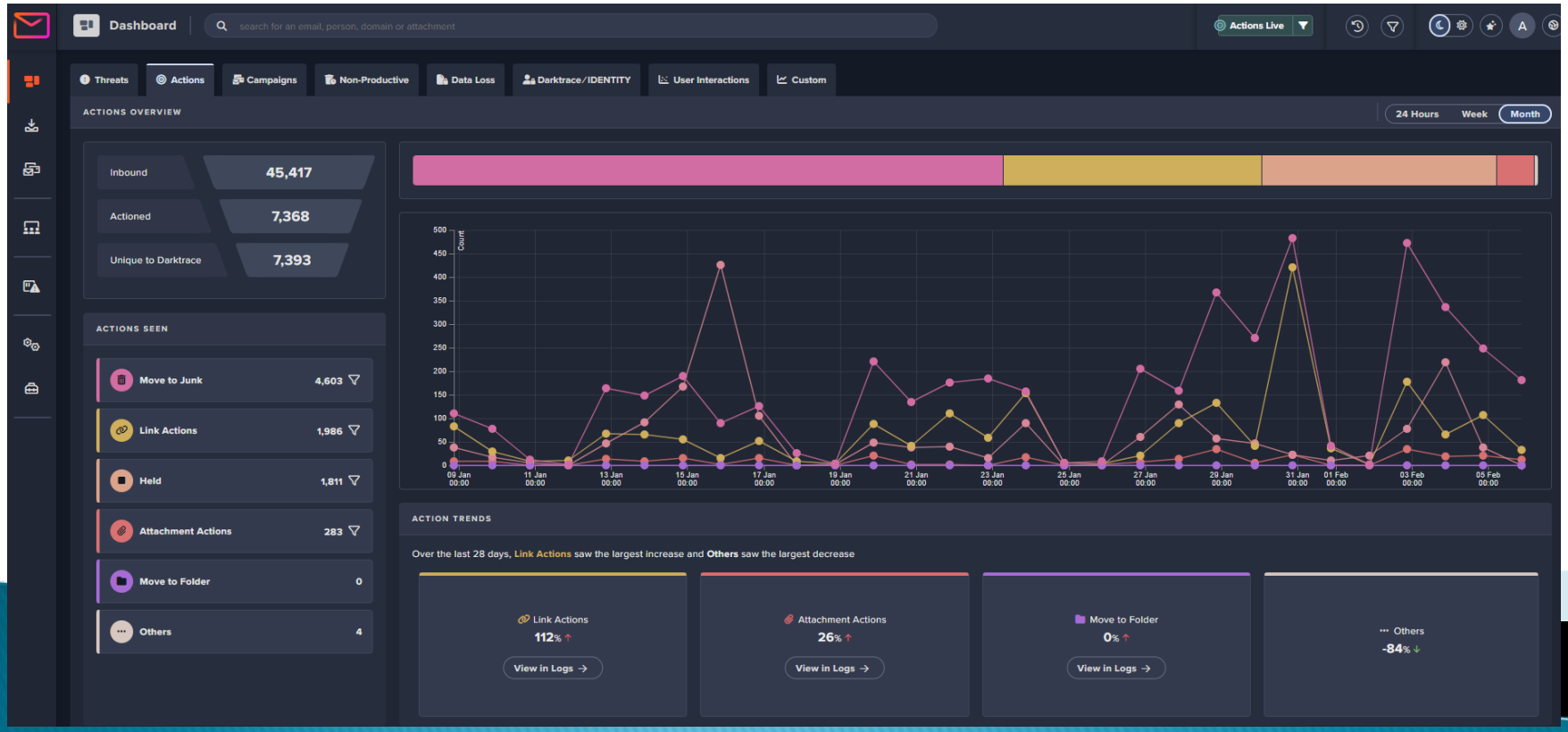
Ativação do modo autônomo do Darktrace (Threat Visualizer)



Pendência Última Reunião

Tribunal Regional Eleitoral-DF

Ativação do modo autônomo do Darktrace (Mail)



Pendência Última Reunião

Tribunal Regional Eleitoral-DF

Proposta para modificações na rede Wi-Fi

- Assunto ainda em discussão
- Benchmark junto à outros órgãos da JE
- WiFi Corp desabilitado o SSID, implementado 802.1x e autenticação pelo AD, somente uso interno
- WiFi Eventos e Convidados utilizadas sob demanda
- WiFi TRE-DF utilizada somente para acesso externo (internet)

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 1: Pessoas e Unidades Organizacionais

Treinamentos Realizados (02 alunos)

- ❑ SECURITY + (RNP + COMPTIA) - Ago/2024 - 40h
- ❑ CIBERSEGURANÇA (RNP + ASCEND) - Out/2024 - 40h

Treinamentos à Realizar (Mar e Out/2025 - 0000570-58.2025.6.07.8100 - 02 alunos)

- ❑ Foundation of Incident Management – FIM (CERT.br)
- ❑ Advanced Topics in Incident Handling – ATIH (CERT.br)

Mestrado profissional em Ciber Segurança (UNB - 0007840-70.2024.6.07.8100 - 10 vagas)

Pessoas

- ❑ Analista Sênior de Cibersegurança/SI (Contrato nº 18/2024 - CTC)**

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 2: Política e Normatização

- Plano de Gestão de Riscos de SI (aprovação CSI)
- PPINC - Prevenção de Incidentes Cibernéticos - Antes: 64,29% - Hoje: 80%
- PGCRC – Gerenciamento de Crises Cibernéticas – Antes: 42,11% - Hoje: 50%
- PIILC – Investigação de Ilícitos Cibernéticos – Antes: 46,67% - Hoje: 70%
- Painel para apoio da monitoração das credenciais previsto na PARTIC

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 2: Política e Normatização

- Painel para apoio da monitoração das credenciais previsto na PARTIC

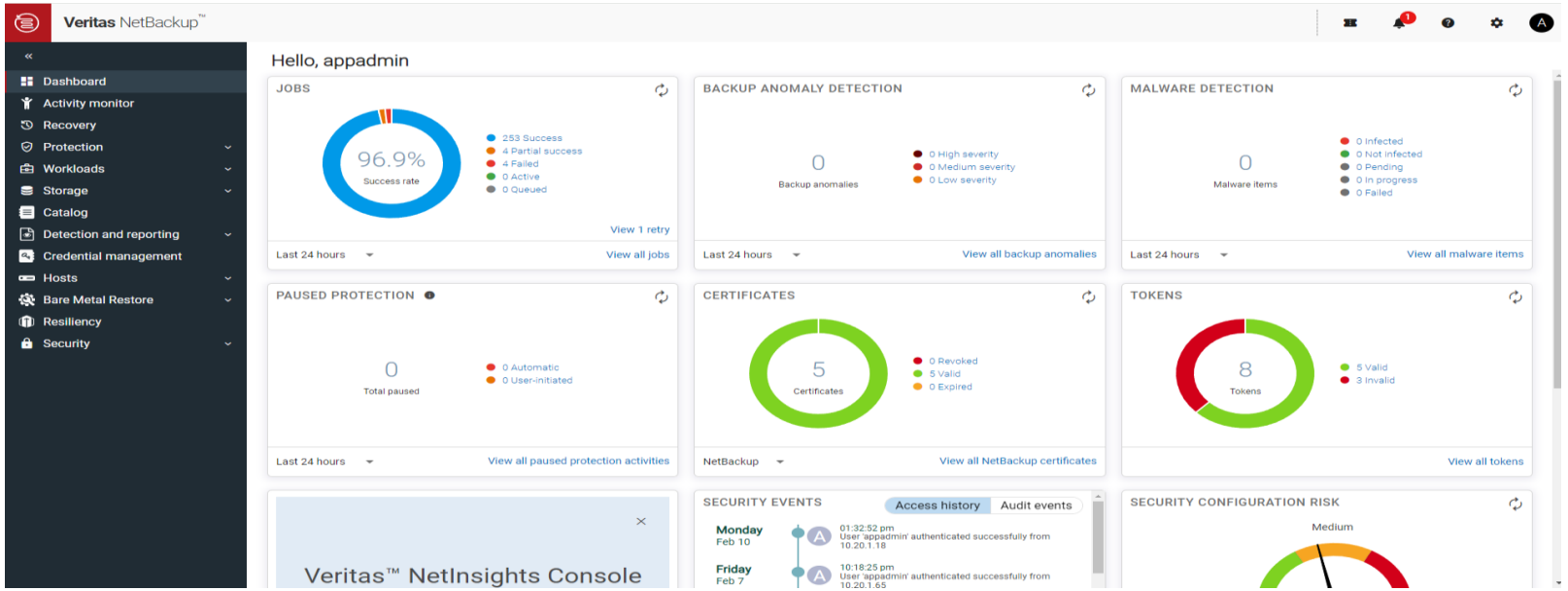
COIE_PARTIC

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 3: Ferramentas Automatizadas

- Implementação nova solução de backup (0009132-27.2023.6.07.8100)

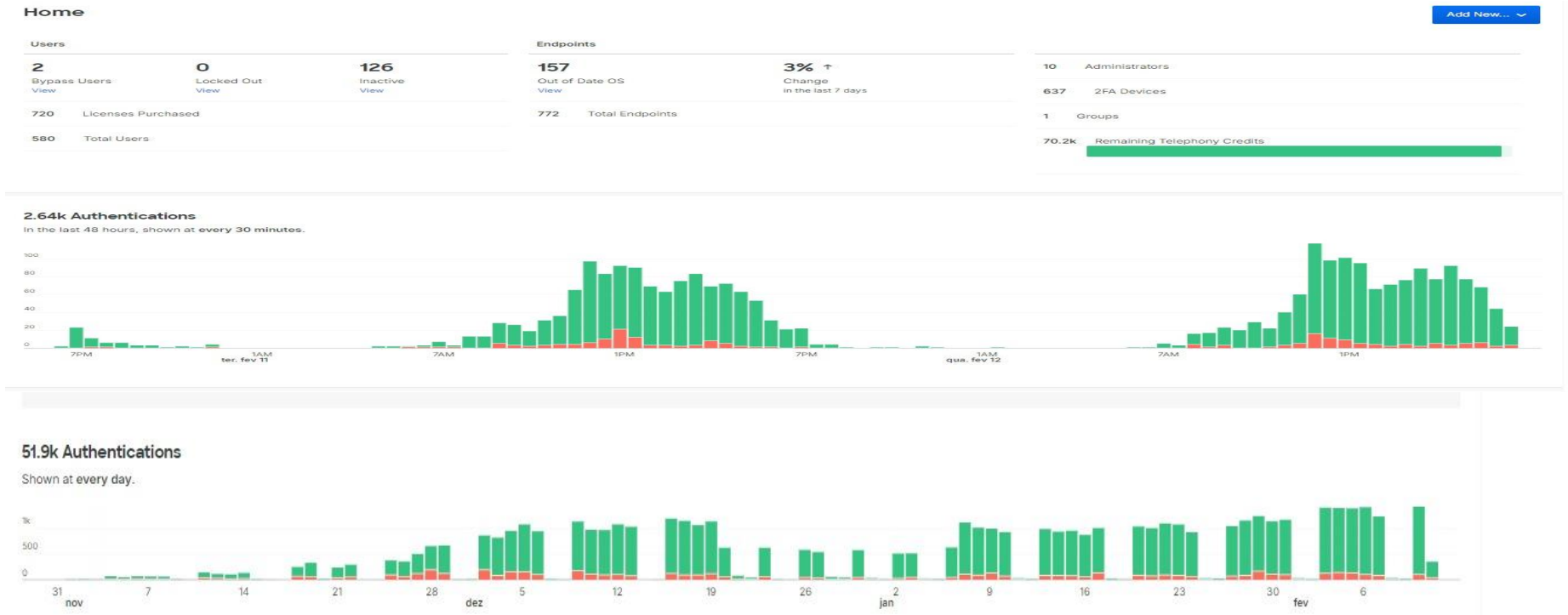


Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 3: Ferramentas Automatizadas

- Implementado duplo fator no login de rede



Usuários cadastrados: 580

Usuários utilizando: 453

Usuários pendentes: 127

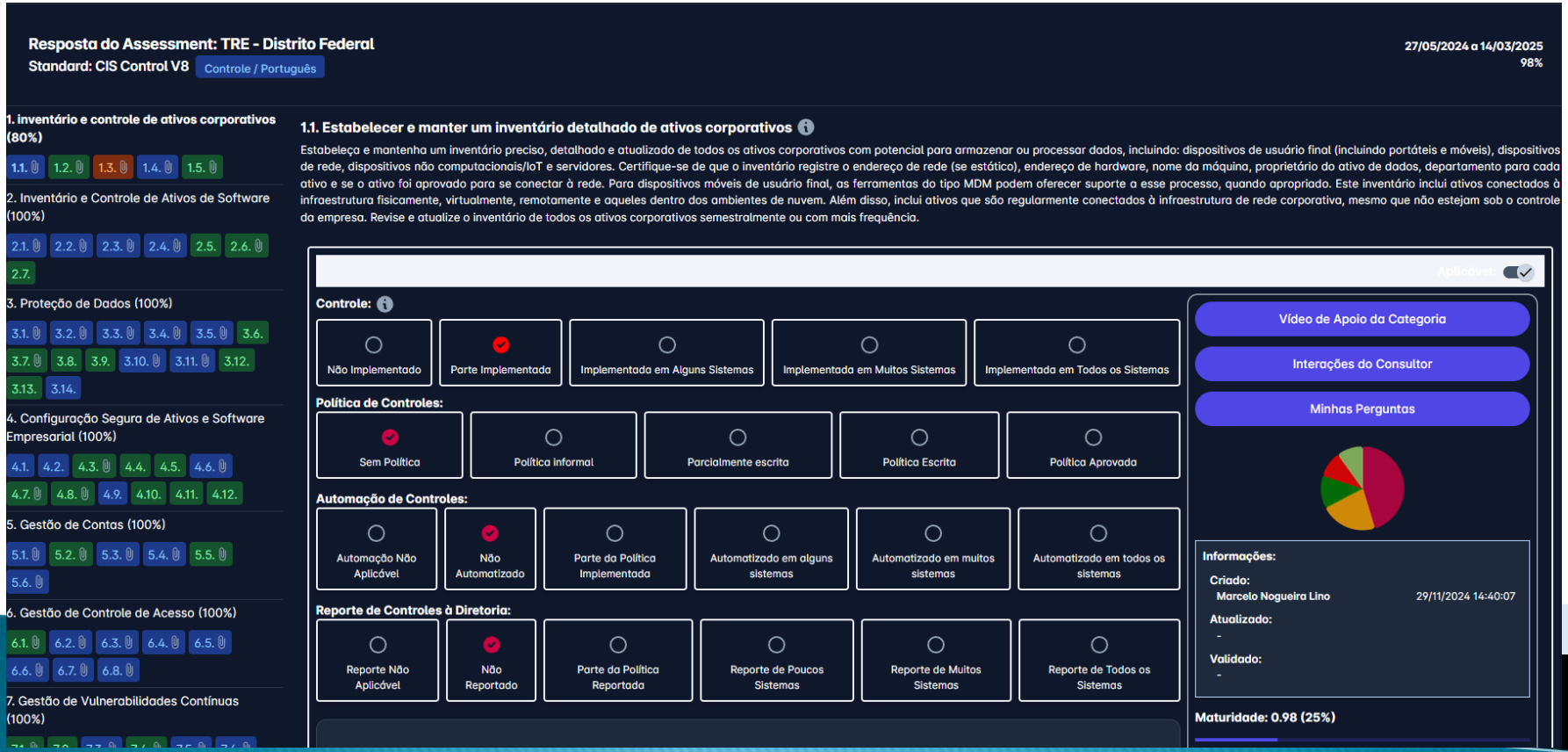
Quantidade de autenticações (último trimestre): 51.9K

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 4: Serviços Especializados

- 1. Finalizada Análise da maturidade de gestão de SI – TSE



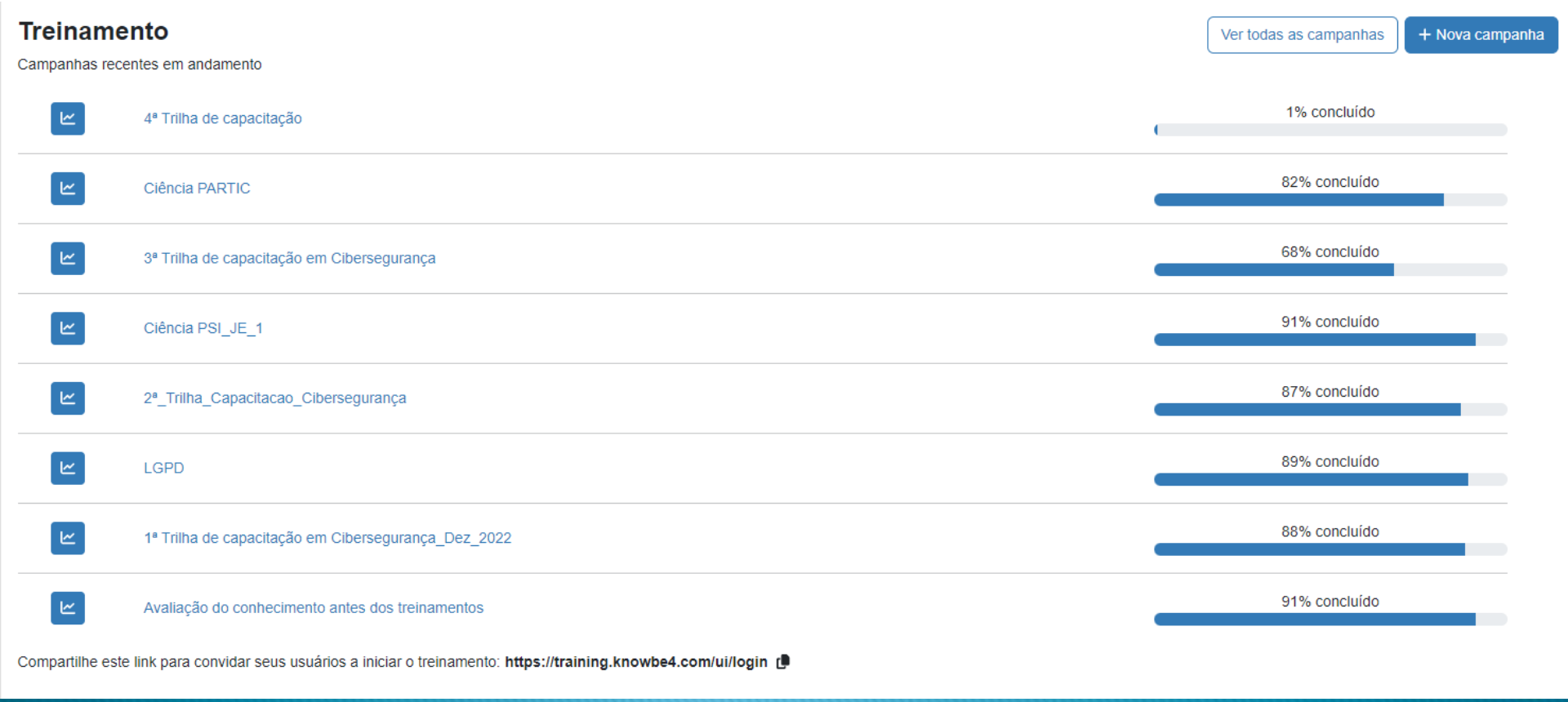
Network Secure

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 5: Sensibilização e Consciêntização

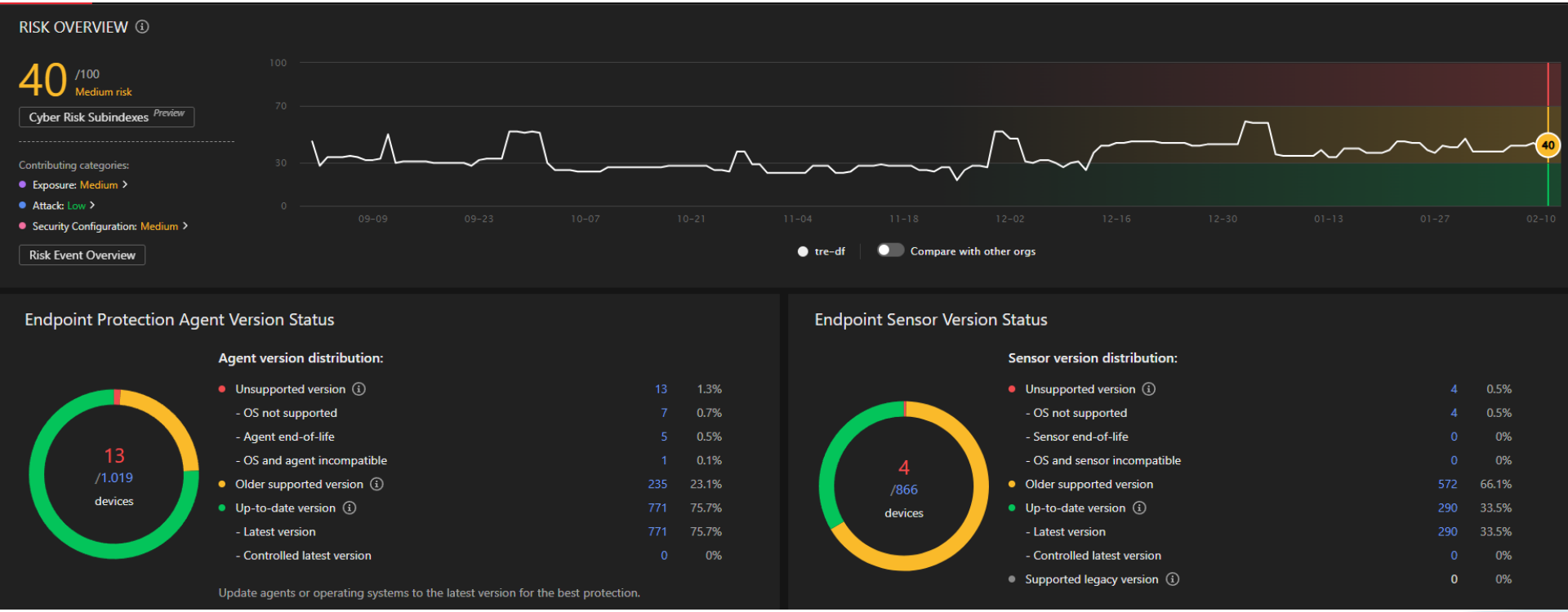
1. Evolução da capacitação dos usuários via Knowbe4



Atividades Rotineiras – Status

Tribunal Regional Eleitoral-DF

Solução de gestão de ativos (desktops + servidores) - Trend Vision One™



Endpoint Protection Agent Version Status

Agent version distribution:

Unsupported version	13	1.3%
- OS not supported	7	0.7%
- Agent end-of-life	5	0.5%
- OS and agent incompatible	1	0.1%
Older supported version	235	23.1%
Up-to-date version	771	75.7%
- Latest version	771	75.7%
- Controlled latest version	0	0%

Update agents or operating systems to the latest version for the best protection.

Endpoint Sensor Version Status

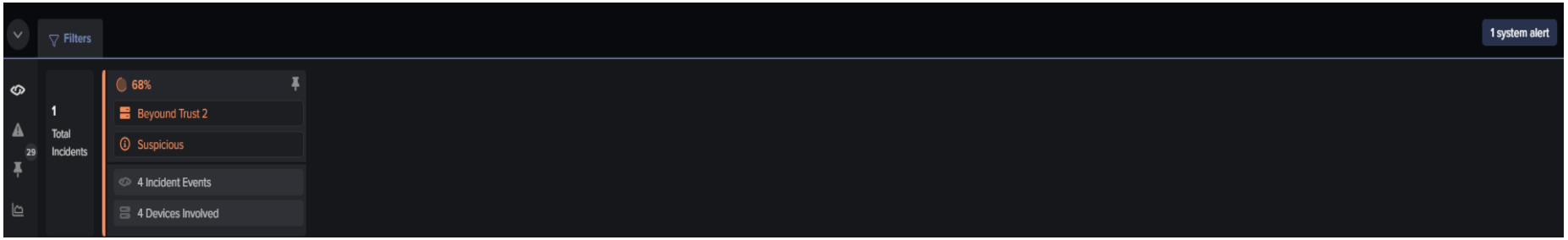
Sensor version distribution:

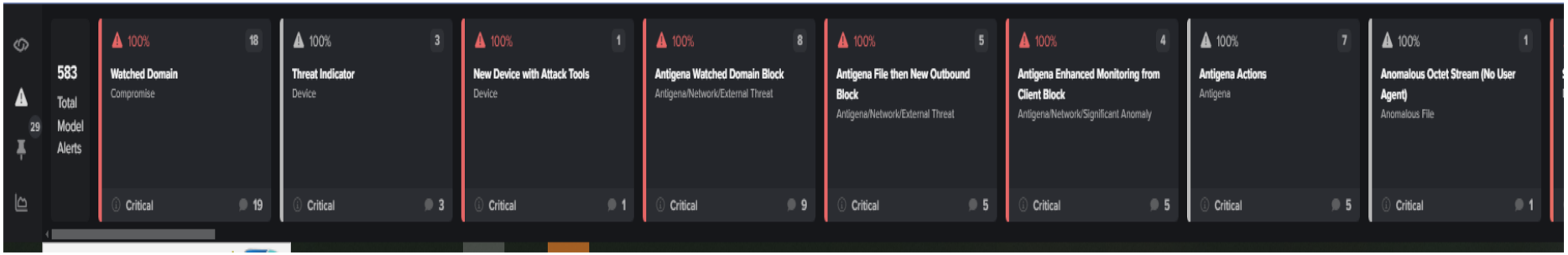
Unsupported version	4	0.5%
- OS not supported	4	0.5%
- Sensor end-of-life	0	0%
- OS and sensor incompatible	0	0%
Older supported version	572	66.1%
Up-to-date version	290	33.5%
- Latest version	290	33.5%
- Controlled latest version	0	0%
Supported legacy version	0	0%

Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

Solução de análise avançada de cibersegurança - Darktrace Threat Visualizer



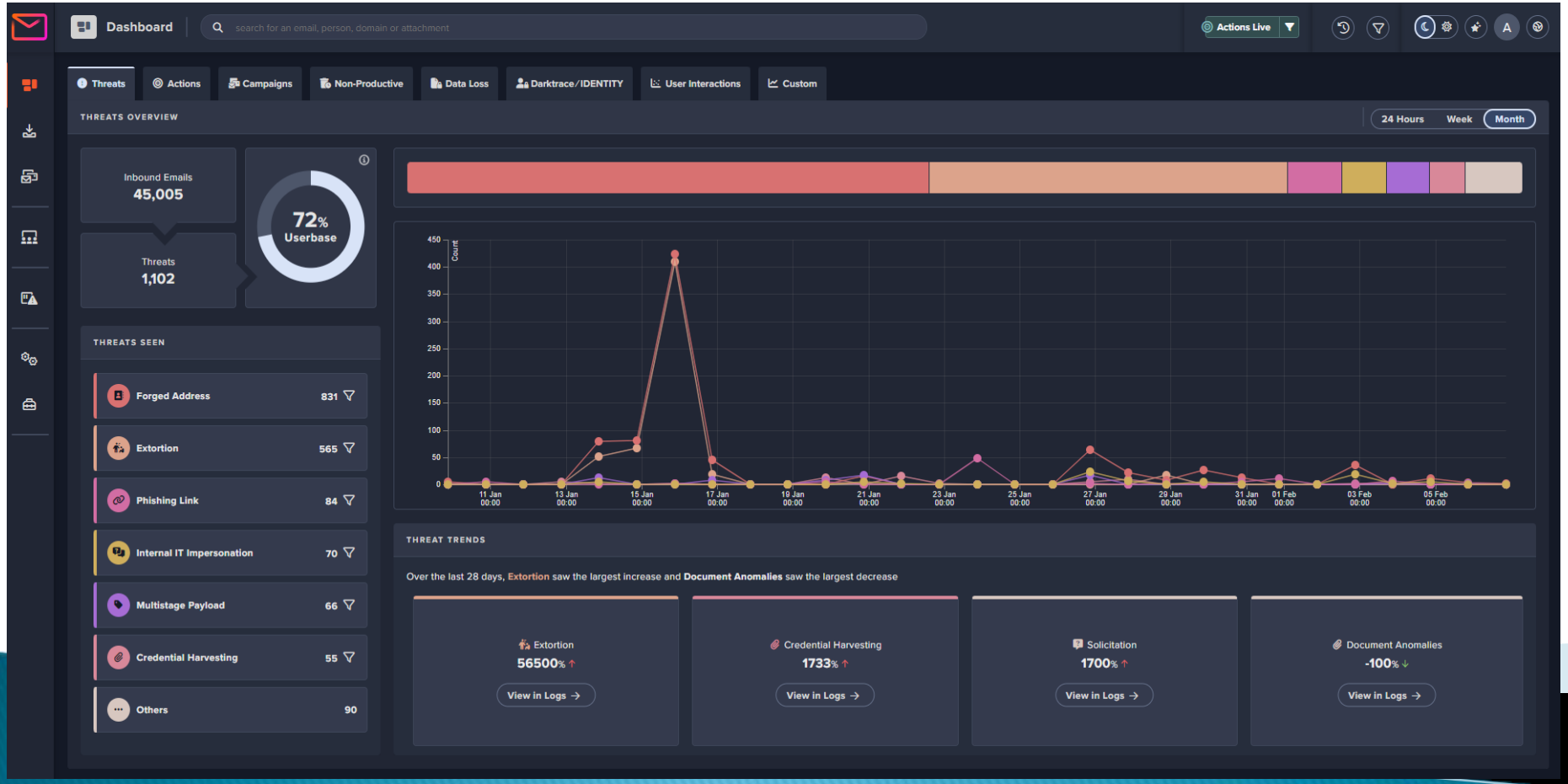


Nenhum confirmado

Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

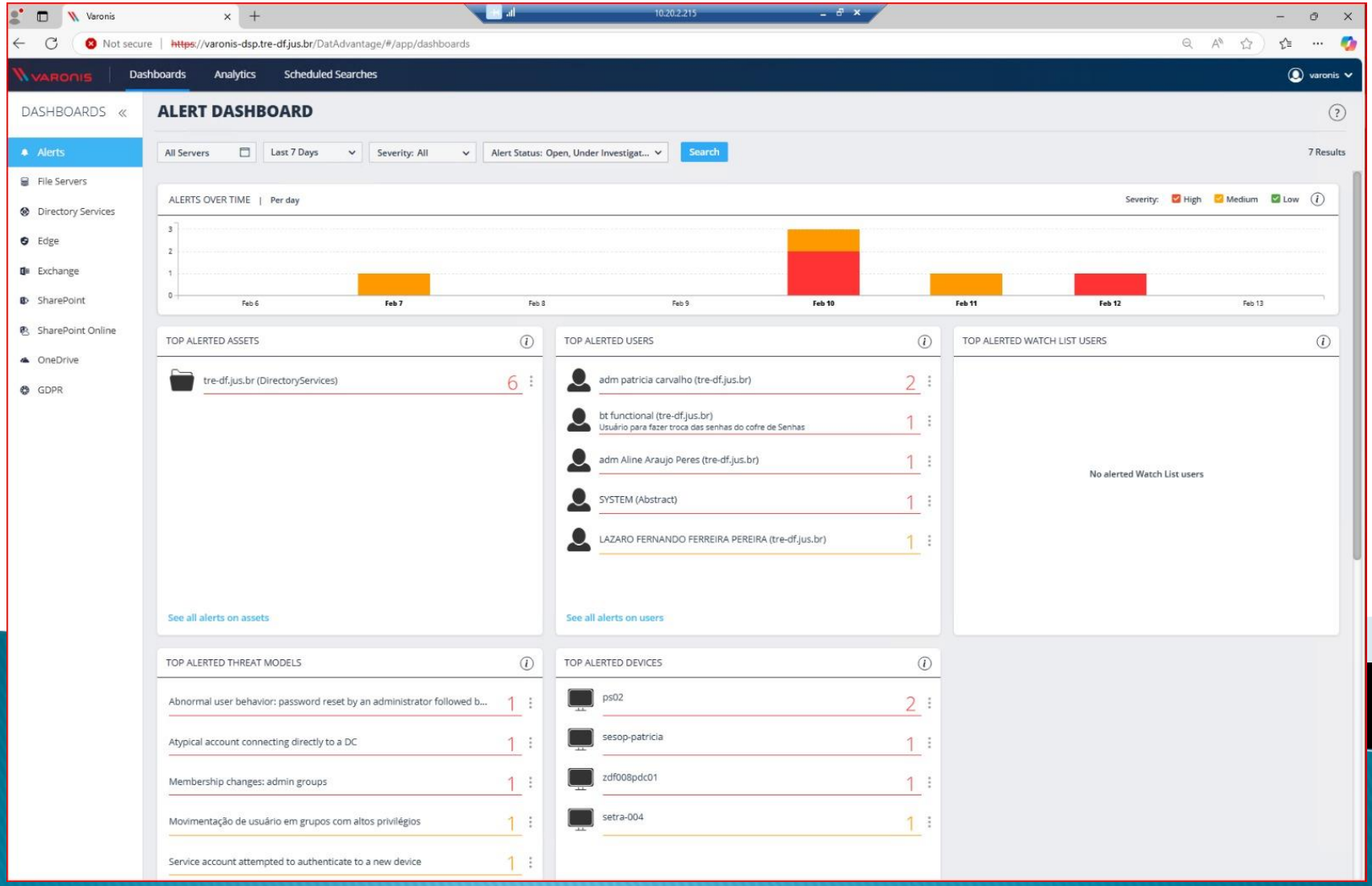
Solução de análise avançada de cibersegurança nos E-mails -



Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

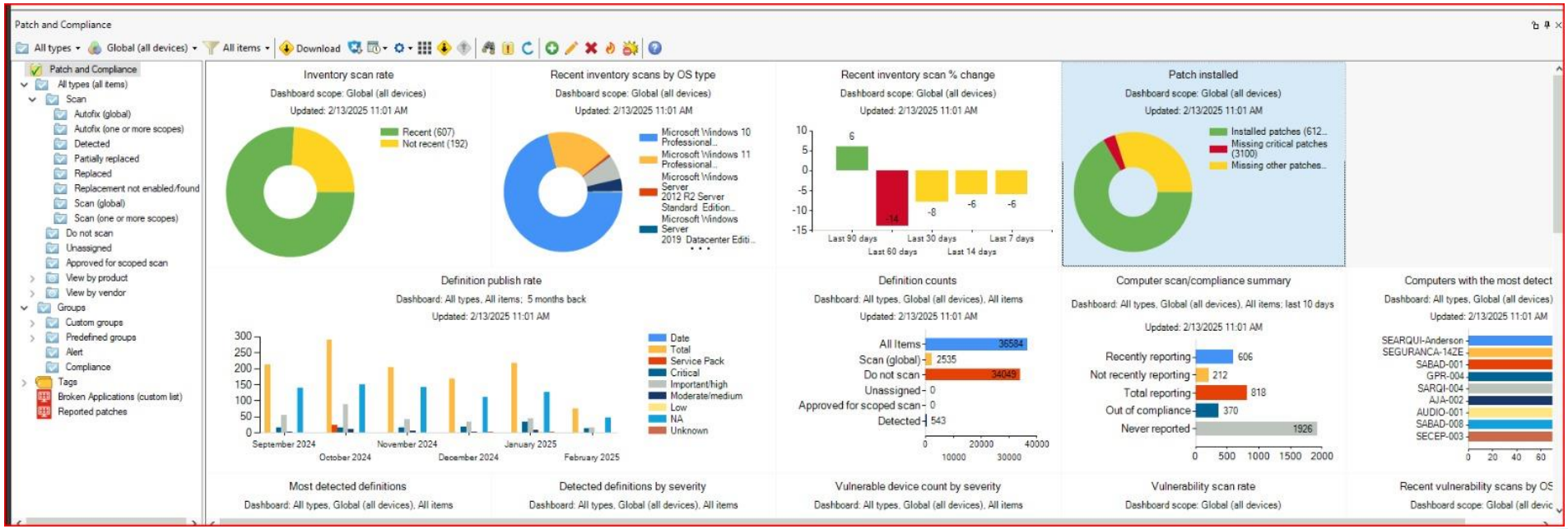
Solução de auditoria de dados não estruturados – VARONIS



Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

Solução de aplicação de patchs e atualização de aplicativos – ivanti



Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

Solução de análise de vulnerabilidades – tenable Security Center Plus

Vulnerability Summary

Vulnerability Summary

Mitigated | Cumulative

Vulnerabilities | Web App Scanning | Queries | Events | Mobile

72 Result(s) | Go to Vulnerability Detail | Export | Save | More

1 to 50 of 72 | Page 1 of 2

PlugIn ID	Name	Family	Severity	VPR	Total
172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	CRITICAL	6.7	8
201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	Web Servers	CRITICAL	6.0	7
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	CRITICAL	5.2	6
193421	Apache 2.4.x < 2.4.54 Authentication Bypass	Web Servers	CRITICAL	6.7	6
134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	CRITICAL	9.0	5
168496	Apache Solr 7.4.0 <= 7.7.3 / 8.0.0 <= 8.11.0 RCE	CGI abuses	CRITICAL	10.0	5

Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

Ferramentas administradas regularmente

LUMINAR DASHBOARD

KnowBe4 Human error. Conquered.

DARKTRACE

BeyondTrust

tenable Security Center Plus

F5

Trend Vision One™

ivanti

DUO CISCO

VARONIS

Ações Futuras

Tribunal Regional Eleitoral-DF

EI- 1: Pessoas e Unidades Administrativas

Implementar a estrutura técnica mínima da equipe de ETIR (03 servidores)

- Reestruturação organizacional – AGSI (02 analistas) - 0008704-79.2022.6.07.8100;
- Concurso TSE – (02 analistas) - PL 04/2024 Câmara dos Deputados. (https://bit.ly/3WwyRa3);
- Aditivar contrato 18/2024 (Connectcom) - Analista de SI e Cibersegurança

Ações Futuras

Tribunal Regional Eleitoral-DF

EI- 2: Políticas e Normatizações

1. Gestão de Riscos de SI – Fev/2025 **(Aprovação do CSI)**
2. Gestão de Vulnerabilidades - Ago/2025
3. Padrões de Configuração – Nov/2025
4. Plano de Continuidade de Serviços Essenciais TI – Maio/2025
5. PPINC – 100% - Dez/2025
6. PGCRC – 100% - Dez/2025
7. PIILC – 100% - Dez/2025
8. Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital – Port. CNJ nº 162/2021 – Jun/2025
9. Atender ao IE 07. Aprimorar a maturidade de segurança cibernética do TRE-DF
10. Definir normativo para realização de ações para preservação de provas em casos de incidentes

Ações Futuras

Tribunal Regional Eleitoral-DF

EI- 2: Políticas e Normatizações

Atender ao IE 07. Aprimorar a maturidade de segurança cibernética do TRE-DF

Próximos

IE 07. Aprimorar a maturidade de segurança cibernética do TRE-DF Plano de Gestão 2024-2026 (TRE-DF)

- MN JR +1 07.11 Manual de Gestão de Identidade e Controle de Acesso - Port. CNJ 162 Mais Dom 1º fev, 2026 - Qua 1º abr, 2026
- MN JR +1 07.08 Atingir nível do PPINC em 100% Mais Seg 1º dez - Qua 31º dez 80%
- MN JR +1 07.09 Atingir nível do PGCRC em 100% Mais Seg 1º dez - Qua 31º dez 50%
- MN JR +1 07.10 Atingir nível do PIILC em 100% Mais Seg 1º dez - Qua 31º dez 70%
- MN JR +1 07.07 Elaboração do Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança ... Mais Ter 1º abr - Seg 30º jun

Iniciado

IE 07. Aprimorar a maturidade de segurança cibernética do TRE-DF Plano de Gestão 2024-2026 (TRE-DF)

- MN JR +1 07.05 Atingir nível do PGCRC em 55% Mais Dom 1º dez, 2024 - Ter 31º dez, 2024 4 80%
- MN JR +1 07.03 Revisão Plano de Continuidade de Serviços Essenciais de TIC Mais Dom 1º set, 2024 - Seg 31º mar
- MN JR +1 07.02 Elaboração do Plano de Gestão de Vulnerabilidades e Padrões de configuração Mais Seg 1º jul, 2024 - Sáb 30º nov, 2024 1
  - Subtarefa MN JR +1 07.02.01 Plano de gestão da vulnerabilidade Seg 1º jul, 2024 - Sáb 30º nov, 2024
  - Subtarefa MN JR +1 07.02.02 Plano de padrões de configuração Seg 1º jul, 2024 - Sáb 30º nov, 2024
- MN JR +1 07.01 Elaboração do Plano de Gestão de Riscos de Segurança da Informação Mais Sáb 1º jun, 2024 - Seg 30º set, 2024 3 90%

Ações Futuras

Tribunal Regional Eleitoral-DF

EI- 3: Ferramentas Automatizadas

Contratações à realizar em 2025

1. Solução de ZTNA + IGA
2. Solução de NGWF + Inspeção de SSL/HTTPS e Distribuição de fluxo de dados
3. Renovação do contrato de VARONIS (Contrato nº 39/2023)
4. Renovação do contrato do DARKTRACE (Contrato nº 37/2023 - Operação assistida

Melhorias

Tribunal Regional Eleitoral-DF

Proposta para normatização do uso do Whatsapp web na rede interna

Principais Riscos

Exposição de informações sensíveis;
Vazamento de conversas e arquivos compartilhados;
Dispositivos comprometidos, podem permitir acesso não autorizado;
Informações pessoais e dados de contatos podem ser comprometidos;
Comprometimento de dispositivo por uso indevido;
Comprometimento da rede interna por uso indevido.

Ações

Aprovação da proposta da minuta pelo CSI;
Publicação, divulgação e implementação em até 12 meses

Melhorias

Tribunal Regional Eleitoral-DF

Implementação e liberação de portal de acesso remoto (portal.tre-df.jus.br)

Principais Benefícios

Aumento do poder de mitigação de riscos e explorações;
Redução da superfície de ataque;
Ambiente mais seguro;
Duplo fator implementado.

Ações

Preparar cronograma e comunicação;
Liberar aplicações/sistemas de forma gradual e corrigir erros;
Divulgar manual de acesso;
Reduzir acessos via VPN do FW;
Início: Em andamento – Término: MAR/2025;

Tribunal
Regional
Eleitoral-DF

Obrigado