Tribunal Regional Eleitoral-DF

REUNIÃO DA CSI
01/08/2024

Tribunal Regional Eleitoral-DF

Tópicos

- Ações realizadas 2º trimestre/2024
- Atividades rotineiras: Status do ambiente
- Ações futuras
- Melhorias

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 2: Políticas e Normatização

2.1. Entrega dos protocolos de Cibersegurança

- PPINC - Prevenção de Incidentes Cibernéticos - antes: 37,84% - Set/2024: 58,58% - hoje: 64,29%
- PGCRC – Gerenciamento de Crises Cibernéticas – antes: 31,58% - Set/2024: 54,38% hoje: 42,11%
- PIILC – Investicação de Ilícitos Cibernéticos – antes: 20% - Set/2024: 46,66% hoje: 46,67%

2.2. Aprovada nova PARTIC – SEI: 0002966-52.2018.6.07.8100

2.3. Aprovado plano de ação do Manual de Gestão de ID e Controle de Acesso – https://bit.ly/3SudEwo

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 3: Ferramentas Automatizadas

Implementações 2º Tri/2024

1. Entrada em produção do Módulo de Threat Intel para e-mail – Darktrace Mail

2. Implementação do módulo de criptografia de DB ORACLE (TDE + NNE)

3. Implementação da solução Fortify - Desenvolvimento seguro

4. Execução do plano de uso do DUO – duplo fator de autenticação

Aquisições 2º Tri/2024

1. Modernização da solução de backup – SEI (0009132-27) - R$ 1.012.947,80 (estimado - 2024)

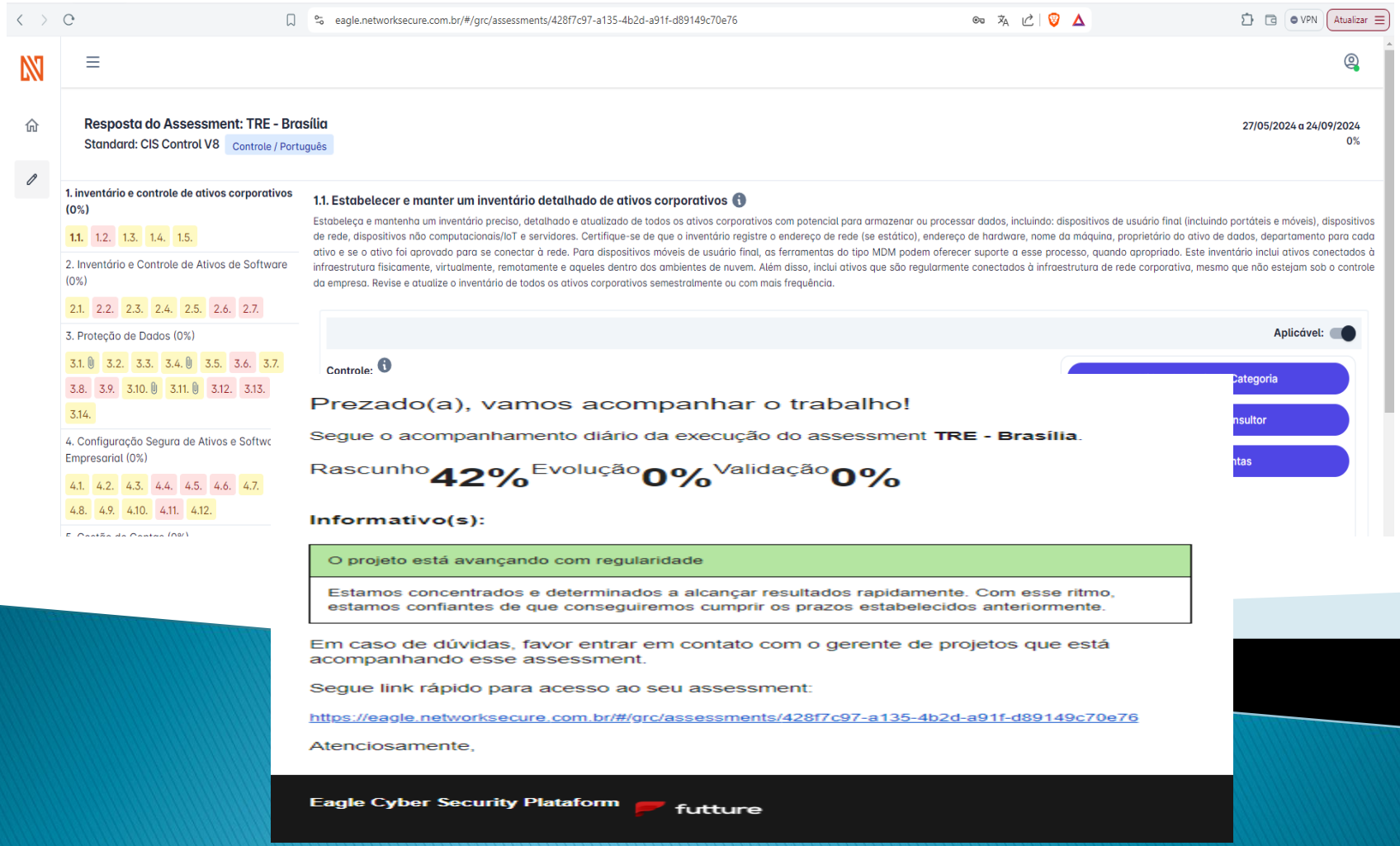
2. Aquisição de solução de GRC – SEI (0002922-23) – estimado em R$ 2.100.000,00 (Contratação TSE)

Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 4: Serviços Especializados

1. Análise da maturidade de gestão de SI – serviços nacionais de cibersegurança – TSE

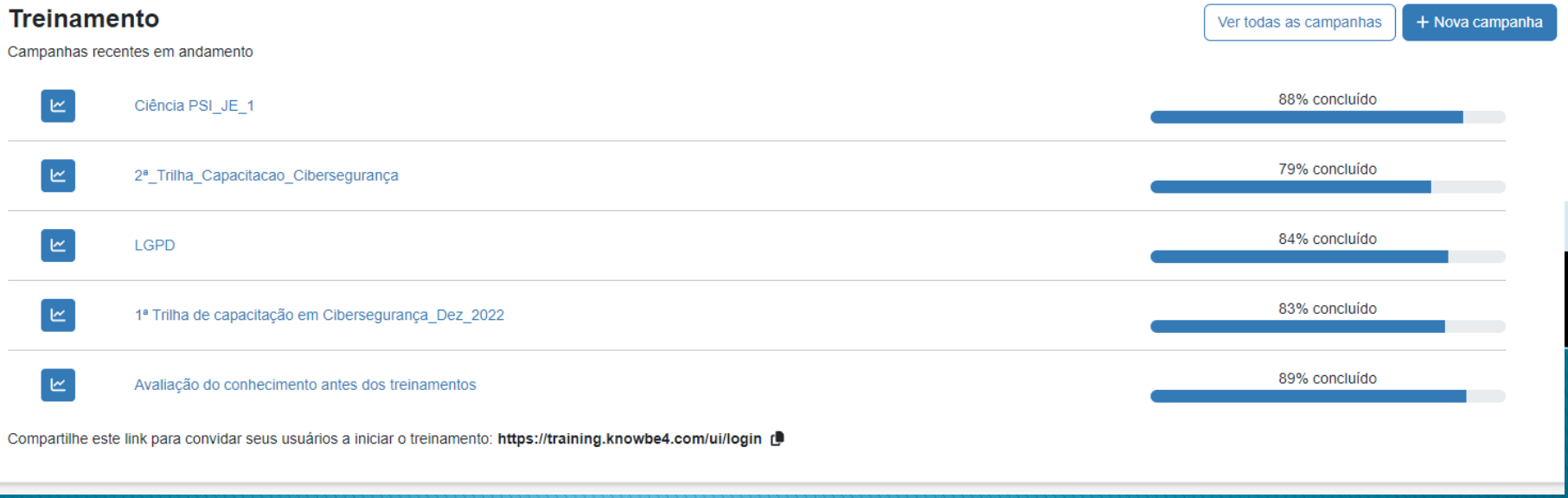


Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 5: Sensibilização e Consciêntização

1. Evolução da capacitação dos usuários via Knowbe4



Ações Realizadas

Tribunal Regional Eleitoral-DF

EI - 5: Sensibilização e Consciêntização

2. Criação de nova campanha de treinamento no Knowbe4 – Início: 09/08 e Término: 09/11/2024

Nome	Grupos	Conteúdo	Duração total	conclusão	Ações
Criado 3ª Trilha de capacitação em Cibersegurança 09/08/2024 - 3 meses	Todos os usuários	Chatbots de IA: Compreenda os usos, riscos e limitações no local de trabalho Como evitar os golpes on-line Criminal Minds: Ransomware Criminal Minds: Social Media Códigos QR; escanear com segurança Jogo Identificador de phishing Ameaças comuns 2024 Coleta de credencial Como celebrar o fim de ano com segurança Como criar senhas fortes - Treinamento para conscientização em segurança Criminal Minds: Cloud Apps Criminal Minds: Mobile Applications Jogo de perguntas sobre conscientização de segurança The Inside Man: Temporada 2, Ep 01 - Uma melodia diferente (Dispositivos móveis) The Inside Man: Temporada 2, Ep 02 - Equipe em ruptura (O que você precisa saber) The Inside Man: Temporada 2, Ep 03 - Temos um encontro marcado (Dispositivos móveis) The Inside Man: Temporada 2, Ep 04 - O Santo Graal (Internet das Coisas/Dispositivos conectados) The Inside Man: Temporada 2, Ep 05 - Companheiros de cama nada prováveis (Phishing) The Inside Man: Temporada 2, Ep 06 - É complicado (Autenticação multifator/Phishing de telefone) The Inside Man: Temporada 2, Ep 07 - Mesa para dois (Senhas/Aplicativos de terceiros) The Inside Man: Temporada 2, Ep 08 - O cara por trás do Cara (Dispositivos externos e Acesso físico) The Inside Man: Temporada 2, Ep 09 - Atrás da cortina (Engenharia social) The Inside Man: Temporada 2, Ep 10 - Confronto final no curral de IA - Parte 1 (Engenharia social) The Inside Man: Temporada 2, Ep 11 - Confronto final no curral de IA. Parte 2 (Ameaças internas) The Inside Man: Temporada 2, Ep 12 - Um novo dia (Internet das Coisas/Dispositivos conectados)	3 hours 12 minutes	0% concluído	

3. 3ª simulação de phishing controlado usando o Knowbe4 – Ago/2024

Atividades Rotineiras – Status

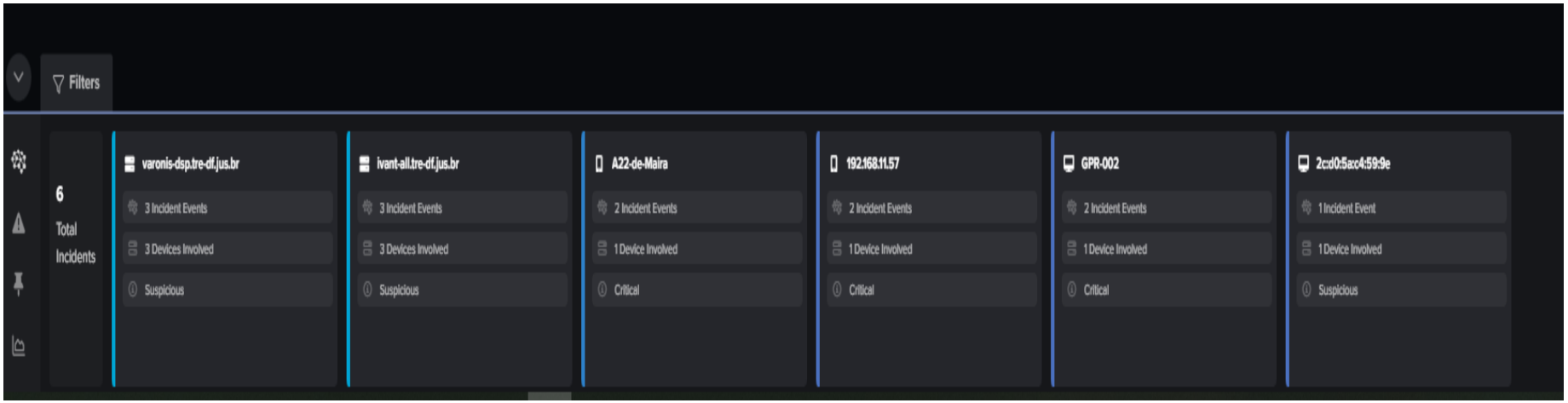
Tribunal Regional Eleitoral-DF

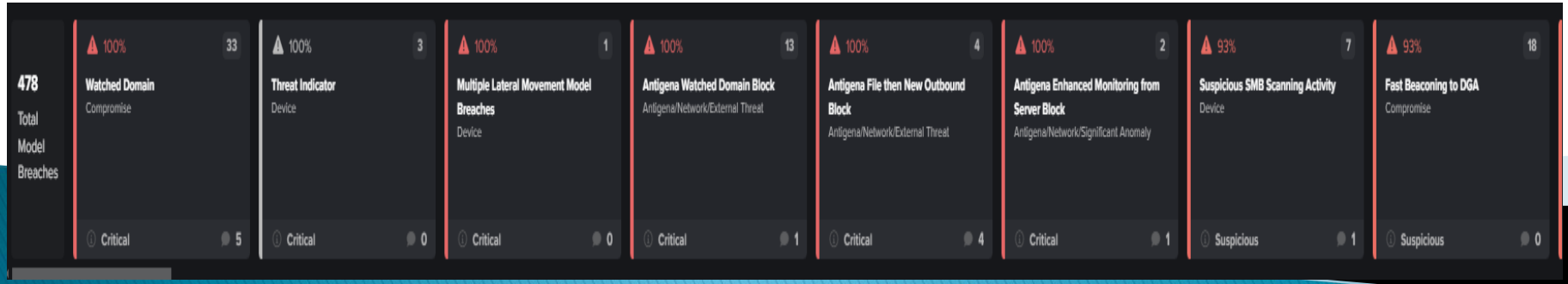
Solução de gestão de ativos (desktops + servidores) - Trend Vision One™

Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

Solução de análise avançada de cibersegurança - DARKTRACE



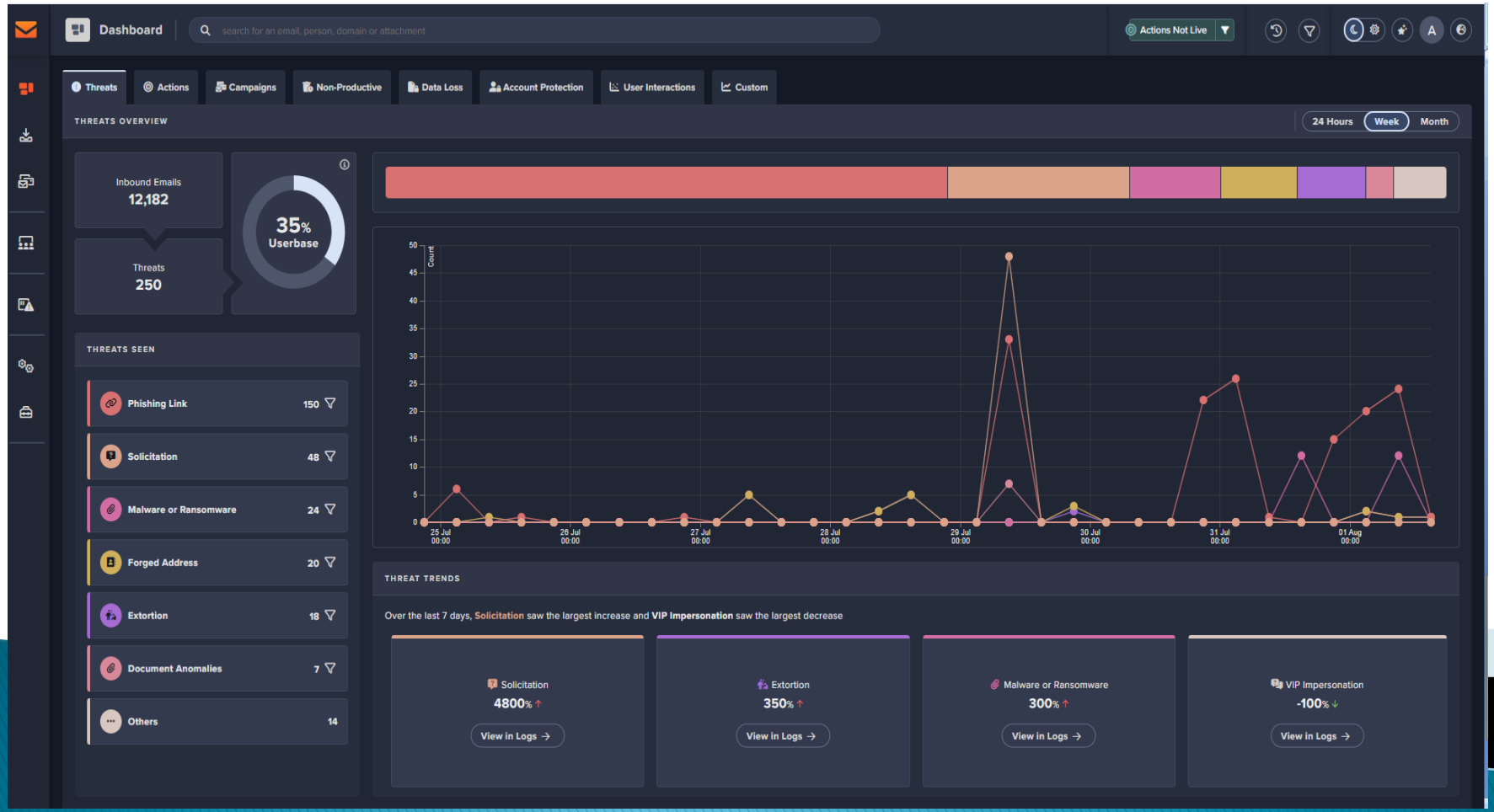


Nenhum confirmado

Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

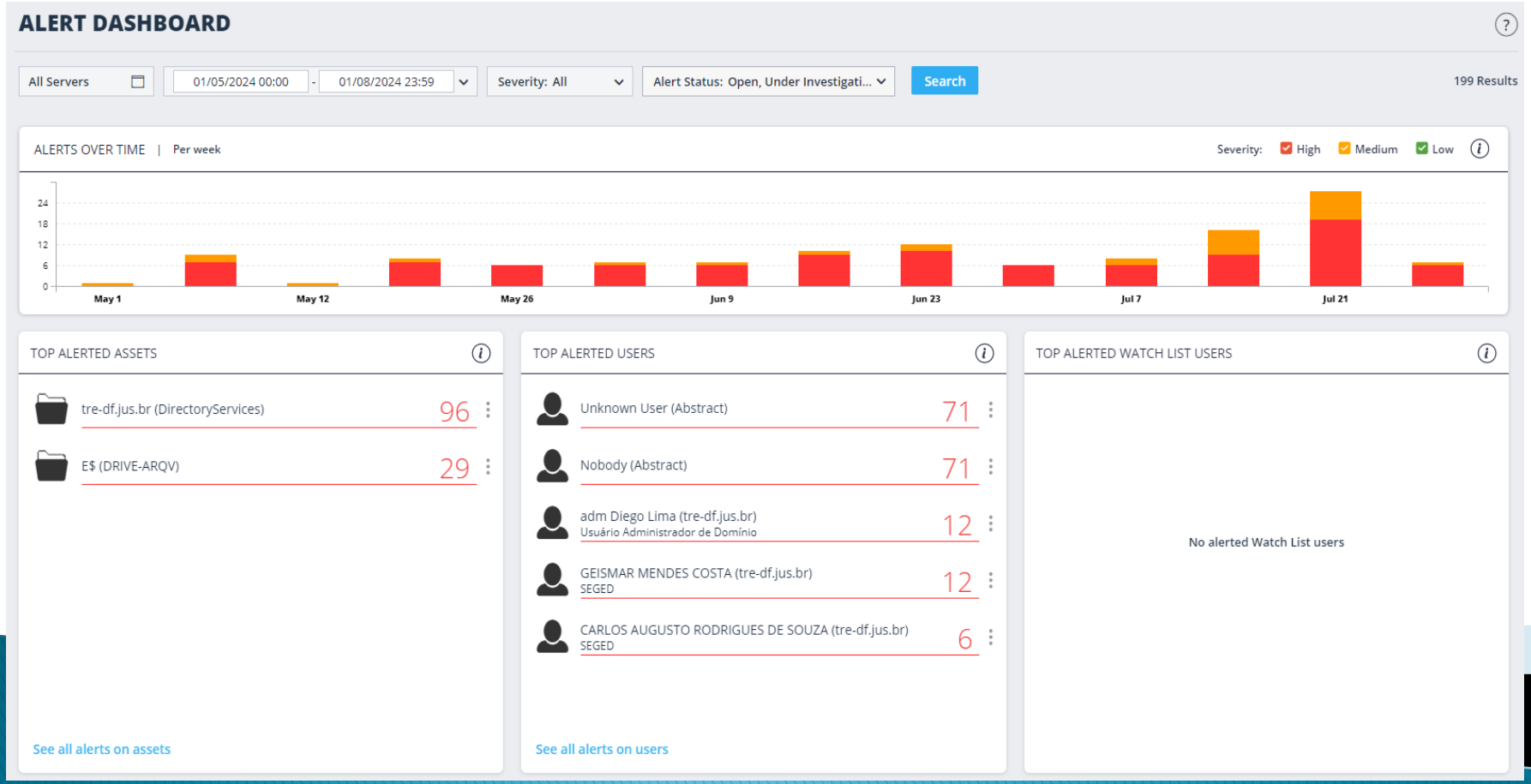
Solução de análise avançada de cibersegurança - DARKTRACE



Atividades Rotineiras - Status

Tribunal Regional Eleitoral-DF

Solução de auditoria de dados não estruturados – VARONIS



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

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

1.1 Terceirização de equipe – Nova contratação Service Desk – 2024 (01 analista sênior – Edital publicado – Licitação 13/08/2024);

1.2 Reestruturação organizacional – AGSI (02 analistas) - 0008704-79.2022.6.07.8100;

1.3 Concurso TSE – (02 analistas) - PL 04/2024 Câmara dos Deputados. (https://bit.ly/3WwyRa3)

Ações Futuras

Tribunal Regional Eleitoral-DF

EI- 2: Políticas e Normatização

1. Gestão de Riscos de SI – Set/2024
2. Gestão de Vulnerabilidades e Padrões de Configuração – Nov/2024
3. Plano de Continuidade de Serviços Essenciais TI – Mar/2025
4. PPINC – 64,29% - Ago/2024
5. PGCRC – 42,11% - Nov/2024
6. PIILC – 46,67% - Ago/2024
7. Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital – Port. CNJ nº 162/2021 – Maio/2025
8. Plano de Ação para Implementação do Manual Gestão de Identidade e Controle de Acesso – Port. CNJ nº 162/2021 – Jul/2024 - https://bit.ly/3SudEwo
9. Implementar o indicador nº 09 do Plano de Gestão 2024-2026, que mede o aprimoramento da maturidade de segurança Cibernética do TRE-DF

Melhorias

Tribunal Regional Eleitoral-DF

1. Bloquear o 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

Comunicar usuários;
Quando: dia 09/08/2024;
Em qual horário: 24x7x365

Melhorias

Tribunal Regional Eleitoral-DF

DARKTRACE

2. Ativar ações automáticas Inteligência de Ameaças e E-mail

Principais Benefícios

Tomar a ação de bloqueio “on line”;
Aumento do poder de mitigação de riscos e explorações;
Grande redução do esforço operacional das equipes envolvidas;
Ambiente mais seguro;

Ações

Comunicar usuários e divulgar canal de comunicação;
Quando: dia 05/08/2024 Threat Intel – E-mail: Aguardar;
Em qual horário:

1. Inicialmente fora do expediente, das 20h às 09h;
2. Após 30 dias 24x7x365

Melhorias

Tribunal Regional Eleitoral-DF

3. Implementação do duplo fator de autenticação

Principais Benefícios

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

Ações

Comunicar usuários e divulgar cronograma;
Divulgar manual de implementação (whatsapp e Intranet);
Início: dia 07/07/2024 – Término: 19/08/2024;

Melhorias

Tribunal Regional Eleitoral-DF

4. 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;

Ações

Preparar cronograma e comunicação;
Liberar aplicações/sistemas de forma gradual;
Divulgar manual de acesso;
Reduzir acessos via VPN do FW;
Início: A definir – Término: Nov/2024;

Melhorias

Tribunal Regional Eleitoral-DF

RUCKUS COMMSCOPE

5. Reduzir redes Wifi disponíveis

Principais Benefícios

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

Ações

Fazer comunicação usuários;
Desabilitar wifi_visitante e wifi_tredf;
Início: A definir – Término: Nov/2024;

Tribunal Regional Eleitoral-DF

Obrigado