

REUNIÃO DA CSI

01/08/2024

Tópicos

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

Ações Realizadas

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

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

EI - 4: Serviços Especializados

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

The screenshot shows a web browser window displaying the Eagle Cyber Security Platform interface. The page title is "Resposta do Assessment: TRE - Brasília" with a standard of "CIS Control V8" and a language of "Português". The assessment progress is shown as 0% for the date range 27/05/2024 to 24/09/2024. The main content area is titled "1.1. Estabelecer e manter um inventário detalhado de ativos corporativos" and includes a detailed description of the control objective. A progress bar shows 42% completion for the "Rascunho" (Draft) phase, with 0% for "Evolução" (Evolution) and "Validação" (Validation). A green box contains the message: "O projeto está avançando com regularidade. Estamos concentrados e determinados a alcançar resultados rapidamente. Com esse ritmo, estamos confiantes de que conseguiremos cumprir os prazos estabelecidos anteriormente." Below this, there is a link to the assessment and a closing statement: "Atenciosamente,". The footer of the page includes the logos for "Eagle Cyber Security Platform" and "future".

Resposta do Assessment: TRE - Brasília
Standard: CIS Control V8 Controle / Português
27/05/2024 a 24/09/2024 0%

1. Inventário e controle de ativos corporativos (0%)
1.1. 1.2. 1.3. 1.4. 1.5.

2. Inventário e Controle de Ativos de Software (0%)
2.1. 2.2. 2.3. 2.4. 2.5. 2.6. 2.7.

3. Proteção de Dados (0%)
3.1. 3.2. 3.3. 3.4. 3.5. 3.6. 3.7.
3.8. 3.9. 3.10. 3.11. 3.12. 3.13.
3.14.

4. Configuração Segura de Ativos e Softw
Empresarial (0%)
4.1. 4.2. 4.3. 4.4. 4.5. 4.6. 4.7.
4.8. 4.9. 4.10. 4.11. 4.12.

5. Config de Contas (0%)

1.1. Estabelecer e manter um inventário detalhado de ativos corporativos ⓘ
Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.

Controle: ⓘ

Aplicável:

Prezado(a), vamos acompanhar o trabalho!
Segue o acompanhamento diário da execução do assessment TRE - Brasília.

Rascunho **42%** Evolução **0%** Validação **0%**

Informativo(s):

O projeto está avançando com regularidade

Estamos concentrados e determinados a alcançar resultados rapidamente. Com esse ritmo, estamos confiantes de que conseguiremos cumprir os prazos estabelecidos anteriormente.

Em caso de dúvidas, favor entrar em contato com o gerente de projetos que está acompanhando esse assessment.

Segue link rápido para acesso ao seu assessment:
<https://eagle.networksecure.com.br/#/grc/assessments/428f7c97-a135-4b2d-a91f-d89149c70e76>

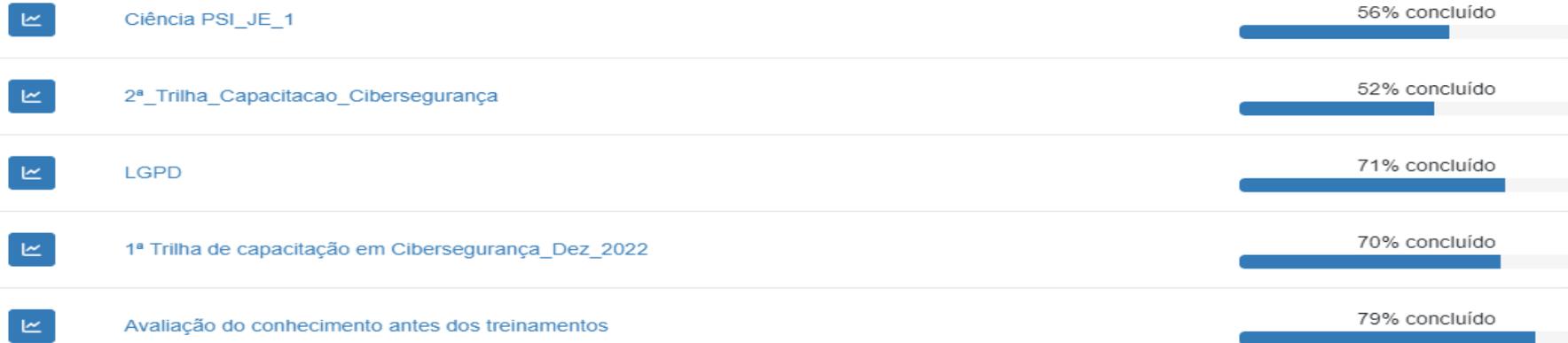
Atenciosamente,

Eagle Cyber Security Platform future

Ações Realizadas

EI - 5: Sensibilização e Consciência

1. Evolução da capacitação dos usuários via Knowbe4



Treinamento

Campanhas recentes em andamento

[Ver todas as campanhas](#)

[+ Nova campanha](#)



Compartilhe este link para convidar seus usuários a iniciar o treinamento: <https://training.knowbe4.com/ui/login>

Ações Realizadas

EI - 5: Sensibilização e Consciência

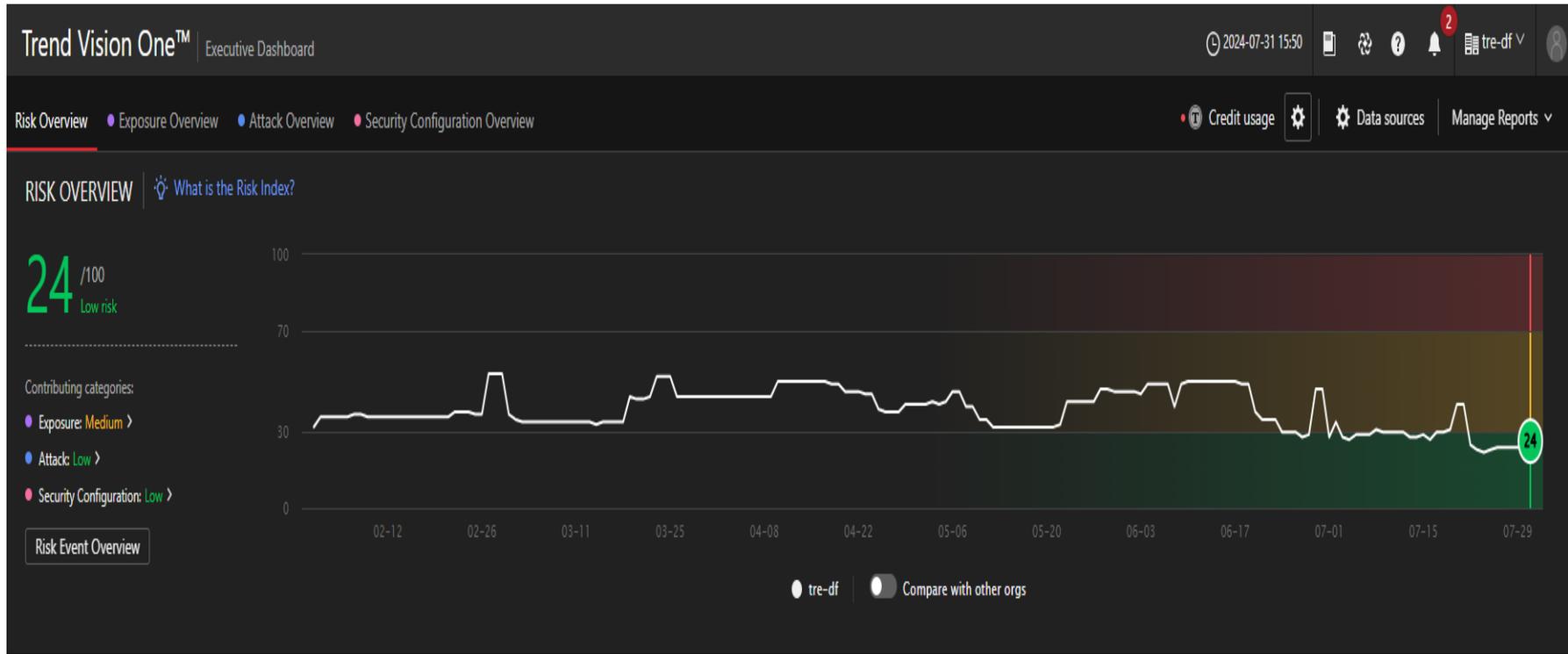
2. Criação de nova campanha de treinamento no Knowbe4 – Início: 09/08 e Término: 09/11/2024

Nome	Grupos	Conteúdo	Duração total	conclusão	Ações
Criado 3ª Trilha de capacitação em Cibersegurança 09/08/2024 - 3 meses	Todos os usuários	<ul style="list-style-type: none">Chatbots de IA: Compreenda os usos, riscos e limitações no local de trabalhoComo evitar os golpes on-lineCriminal Minds: RansomwareCriminal Minds: Social MediaCódigos QR; escanear com segurançaJogo Identificador de phishingAmeaças comuns 2024Coleta de credencialComo celebrar o fim de ano com segurançaComo criar senhas fortes - Treinamento para conscientização em segurançaCriminal Minds: Cloud AppsCriminal Minds: Mobile ApplicationsJogo de perguntas sobre conscientização de segurançaThe 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

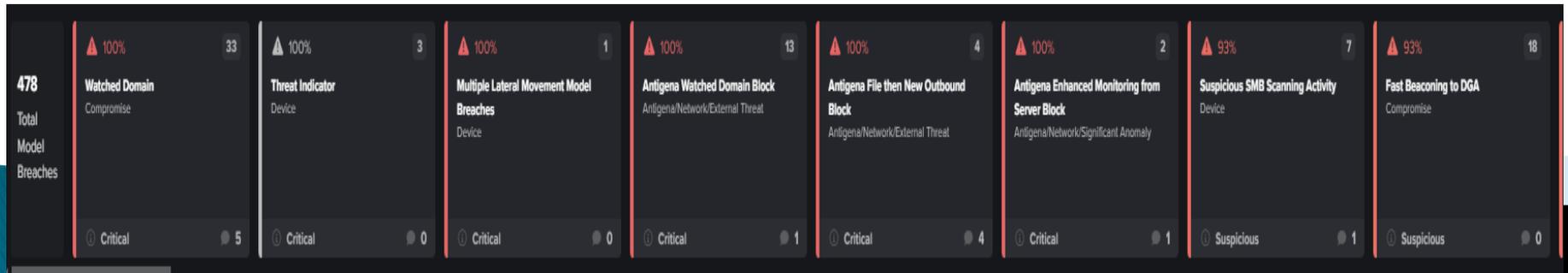
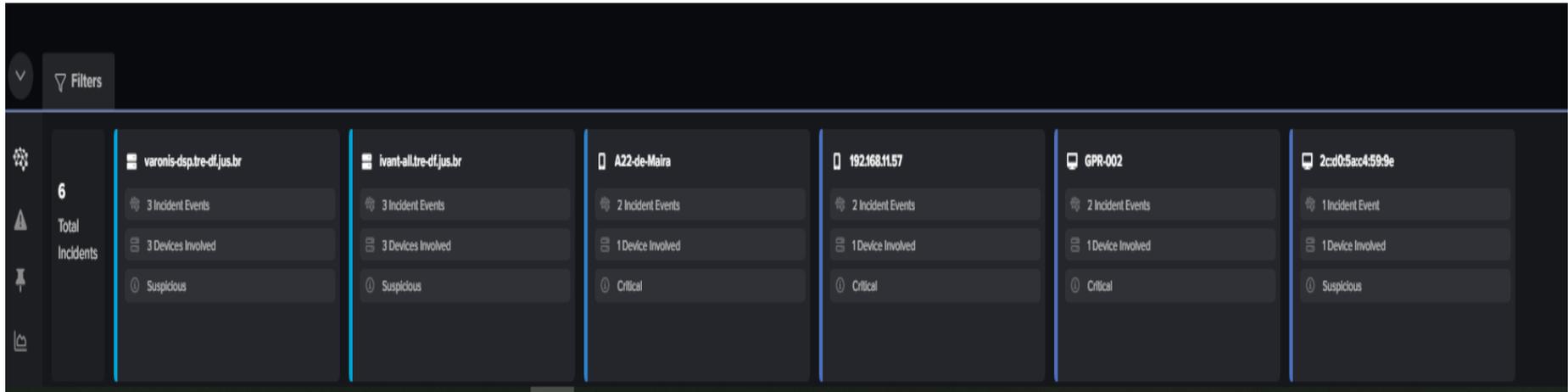
Solução de gestão de ativos (desktops + servidores) -



Atividades Rotineiras - Status

Solução de análise avançada de cibersegurança -

DARKTRACE

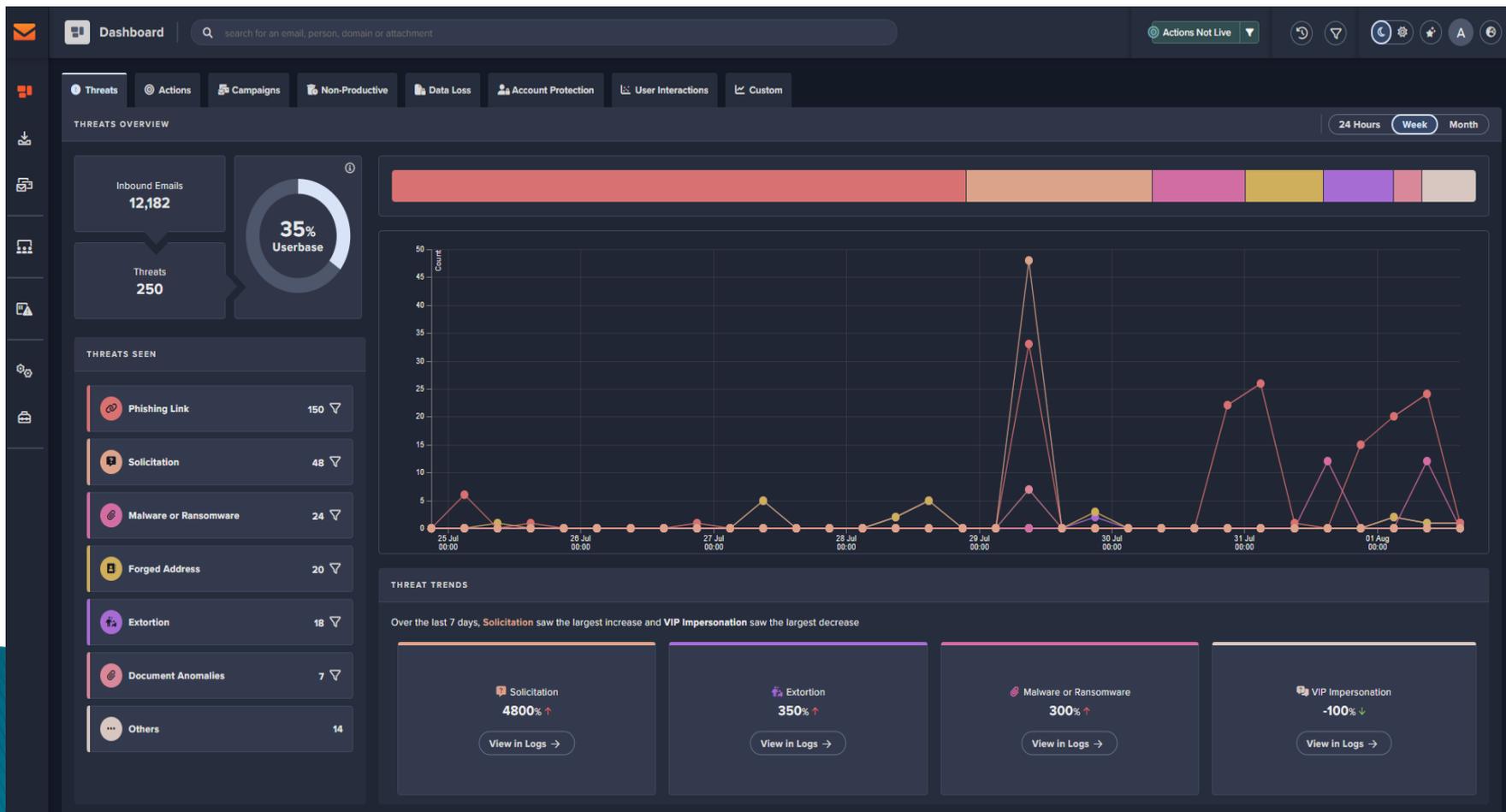


Nenhum confirmado

Atividades Rotineiras - Status

Solução de análise avançada de cibersegurança -

DARKTRACE



Atividades Rotineiras - Status

Solução de auditoria de dados não estruturados –



ALERT DASHBOARD



All Servers

01/05/2024 00:00

01/08/2024 23:59

Severity: All

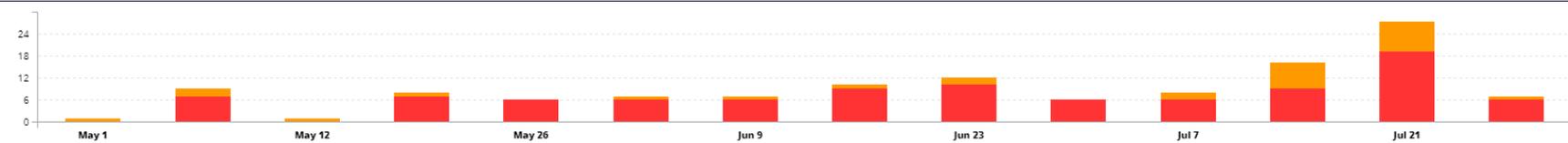
Alert Status: Open, Under Investigati...

Search

199 Results

ALERTS OVER TIME | Per week

Severity: High Medium Low



TOP ALERTED ASSETS

tre-df.jus.br (DirectoryServices)	96
E\$ (DRIVE-ARQV)	29

[See all alerts on assets](#)

TOP ALERTED USERS

Unknown User (Abstract)	71
Nobody (Abstract)	71
adm Diego Lima (tre-df.jus.br) Usuário Administrador de Domínio	12
GEISMAR MENDES COSTA (tre-df.jus.br) SEGED	12
CARLOS AUGUSTO RODRIGUES DE SOUZA (tre-df.jus.br) SEGED	6

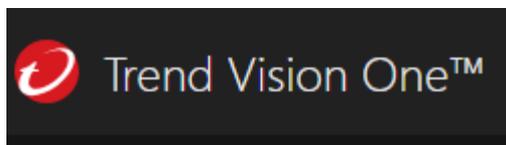
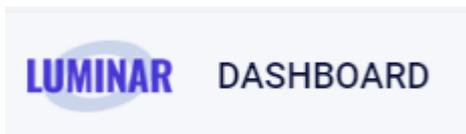
[See all alerts on users](#)

TOP ALERTED WATCH LIST USERS

No alerted Watch List users

Atividades Rotineiras - Status

Ferramentas administradas regularmente



Ações Futuras

El- 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

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



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



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



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



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



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;

Obrigado