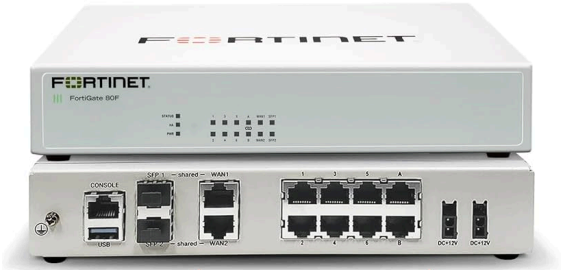
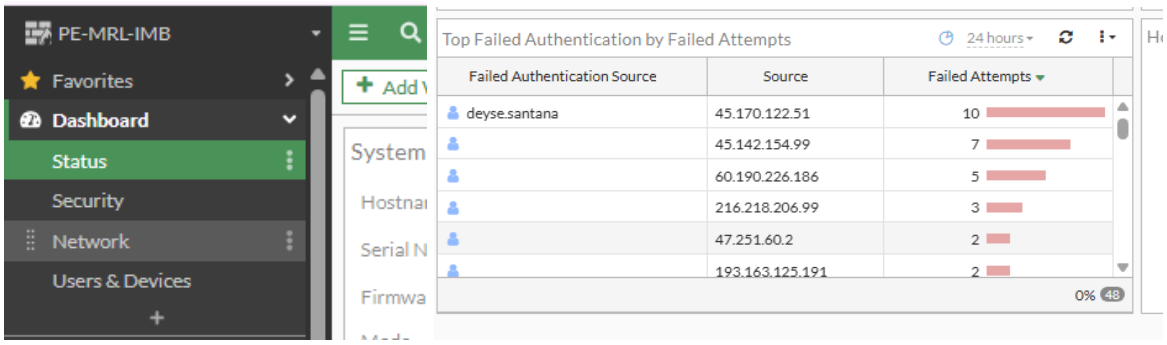
AUDITORIA DIÁRIA DE ATAQUES EXTERNOS

Procedimento de Verificação Diária de Incidentes de Segurança – Fortigate

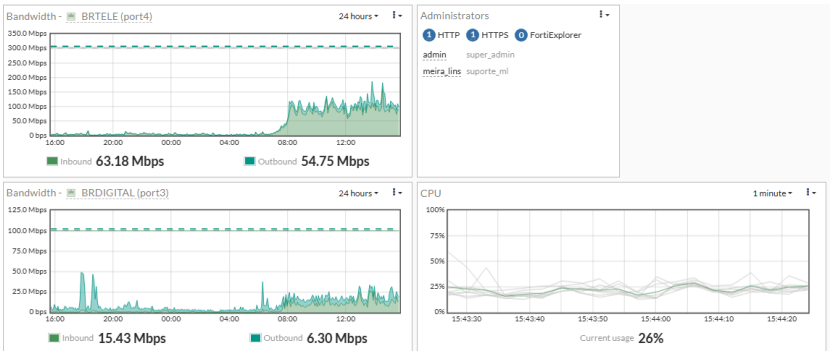
Este documento tem como objetivo a **verificação diária de possíveis ataques externos** à empresa, por meio da análise dos incidentes registrados na plataforma **Fortigate**. O procedimento deve ser executado **diariamente**, garantindo o monitoramento contínuo da segurança do ambiente.

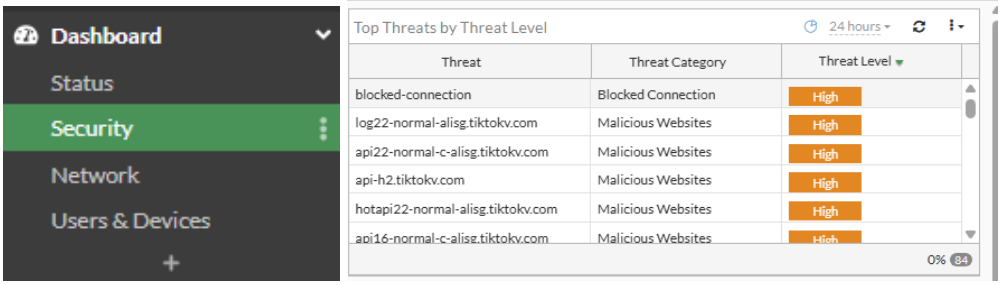


Passo a passo:

1. **Acesso à plataforma matriz do Fortigate**
   - Acesse o endereço: **https://10.81.6.1:4443/**
   - Realize o login com as credenciais necessárias. *(Você pode encontrar no nosso cofre de senhas)*
2. **Consulta de incidentes**
   - Em Dashboard>Status você pode consultar oscilações de tráfego de rede, memória, e tentativas de falhas de autenticação, que são importantíssimas para procurar por picos incomuns de volume, varreduras de portas (port scans) ou tentativas de acesso a serviços não usuais.
   - 

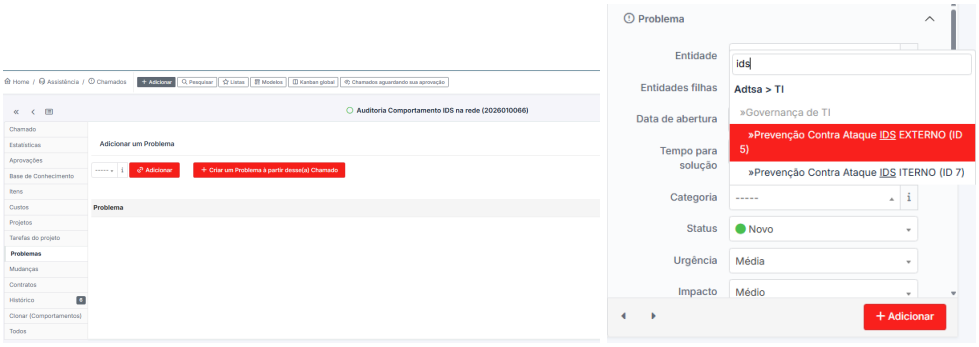
AUDITORIA DIÁRIA DE ATAQUES EXTERNOS

- 

- Em Dashboards>Security você encontrará as principais ameaças por nível, que precisam de uma atenção redobrada.
- 

- Em **Top Threats bt Threat level** você encontrará de forma mais detalhada as ameaças que são encontradas pelo Fortigate, porém, muitas delas podem ser falsos positivos, como propagandas, API's de sites de streaming usados pela equipe de marketing, Acessos remotos entre outros.
- **Análise dos resultados**
    - **Caso não haja incidentes registrados**:
        - Tire uma **print (captura de tela)** da tela sem resultados.
        - Anexe a evidência ao chamado correspondente no **GLPI**.
    - **Caso existam incidentes registrados**:
        - Acesse o chamado no GLPI.
        - Na aba **Problemas**, crie um **novo problema** relacionado ao chamado

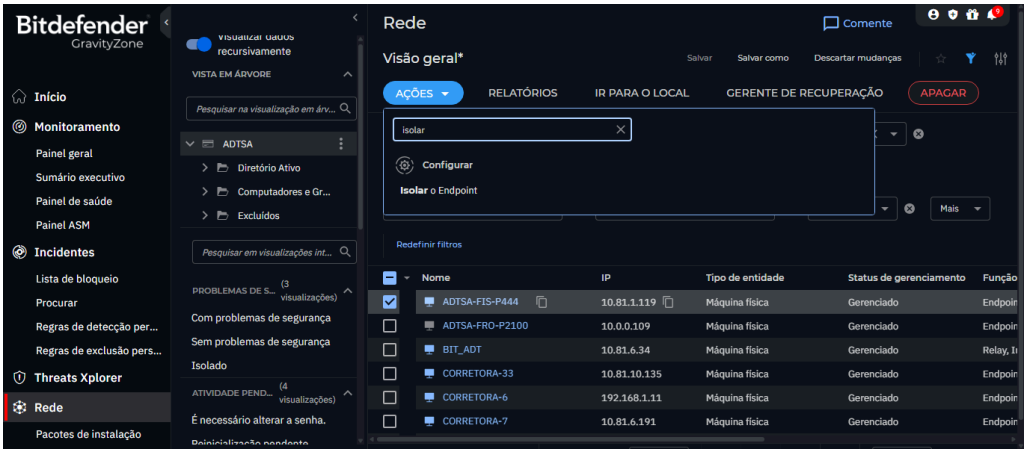
AUDITORIA DIÁRIA DE ATAQUES EXTERNOS



3. Tratativa dos incidentes

- Após a criação do problema:
  - Analise a **causa do incidente** (origem, tipo de ameaça, ativo impactado).
  - Realize as ações necessárias para a tratativa **e mitigação** do problema, conforme os procedimentos de segurança definidos.
  - Caso seja identificado que seja um problema real e não um falso positivo, é **OBRIGATÓRIO** que a máquina seja colocada em isolamento, para evitar replicação da contaminação.
  - Na aba de Rede, selecione o computador infectado e clique em **Isolar.**

AUDITORIA DIÁRIA DE ATAQUES EXTERNOS

- 

- **AVISE A EQUIPE DE ATENDIMENTO DE PRIMEIRO NÍVEL DA SITUAÇÃO! Solicite a transferência da ligação para o analista de rede disponível e dê início às tratativas necessárias.**

4. Encerramento

- Após o tratamento da não conformidade na estrutura:
  - Encerre o **problema** criado no GLPI.
  - Encerre o **chamado** correspondente, seguindo o seguinte padrão:

Na verificação diária dos eventos de segurança gerados pelo **Fortigate** foi identificada uma **não conformidade** e, seguindo as orientações do **PROC TI 001 – V – Verificar diariamente os eventos gerados pelas ferramentas de segurança da informação, tomando as providências necessárias para prevenção e mitigação de incidentes**, venho relatar o seguinte:

DESCRIÇÃO

1. Quando aconteceu ?
Dia, expediente, hora
Dia **{DD/MM/AA}**, por volta das **{HH:MM}**

AUDITORIA DIÁRIA DE ATAQUES EXTERNOS

2. Onde aconteceu ?

Local, sala, equipamento, fornecedor

Sala de TI, **{Unidade/Local}**, console **Fortigate**, endpoint **{hostname}**, IP **{IP}**

3. O que aconteceu

(Efeito, tipo de atividade, tipo de equipamento em uso, pessoas)

Durante o monitoramento dos eventos de segurança, o **Fortigate** identificou uma **detecção de ameaça/atividade suspeita**, classificada como **{tentativa de intrusão / comportamento malicioso / tráfego anômalo}**, originada do processo **{nome do processo}** no endpoint **{hostname}**.

4. Por que aconteceu ?

Não conformidade

A não conformidade ocorreu devido à **execução de software não autorizado**, **vulnerabilidade no sistema**, **configuração inadequada de política de segurança** ou **comportamento atípico do usuário**, acionando os mecanismos de detecção do GravityZone.

5. Qual o risco envolvido

(Consequência da não conformidade)

A não tratativa adequada dos alertas gerados pelo **Fortigate** pode resultar em **comprometimento do endpoint**, **propagação de malware na rede**, **exposição de dados sensíveis** e impactos diretos na **segurança da informação e continuidade do negócio**.

Orientação imediata:

FAZER O REGISTRO DESSA NÃO CONFORMIDADE ATRAVÉS DA ABERTURA DE UM CHAMADO DE PROBLEMA NO GLPI, para acompanhamento e controle através do **painel de indicadores do COMPLIANCE**, item **{X} – Eventos de segurança detectados e tratados pelo Bitdefender GravityZone**.

- **Acesse o grafana**
  - **Acesse o Grafana e vá em Menu>Dashboards>Complience>Complience backup e segurança**

AUDITORIA DIÁRIA DE ATAQUES EXTERNOS

-