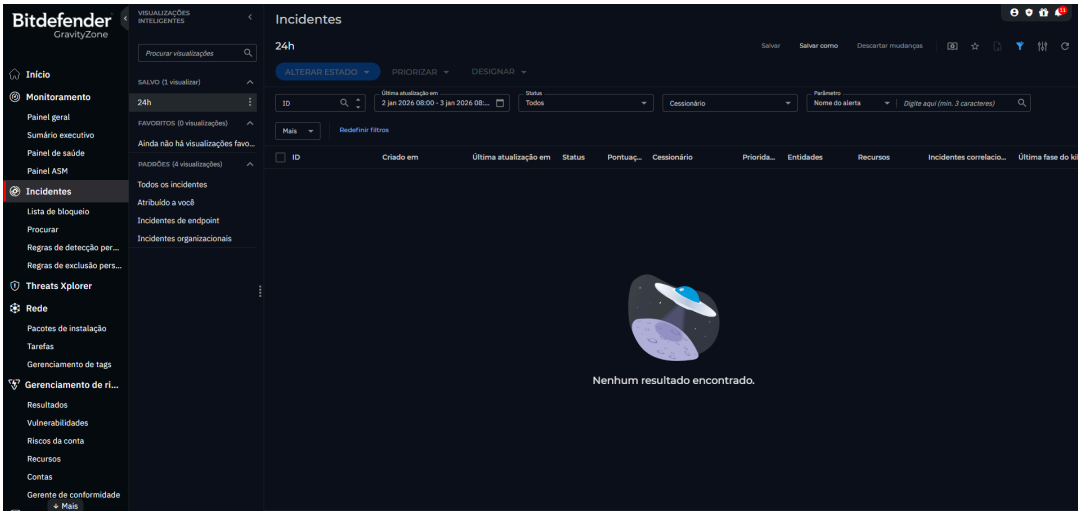
# AUDITORIA DIÁRIA DE ATAQUE INTERNO

## Procedimento de Verificação Diária de Incidentes de Segurança – Bitdefender

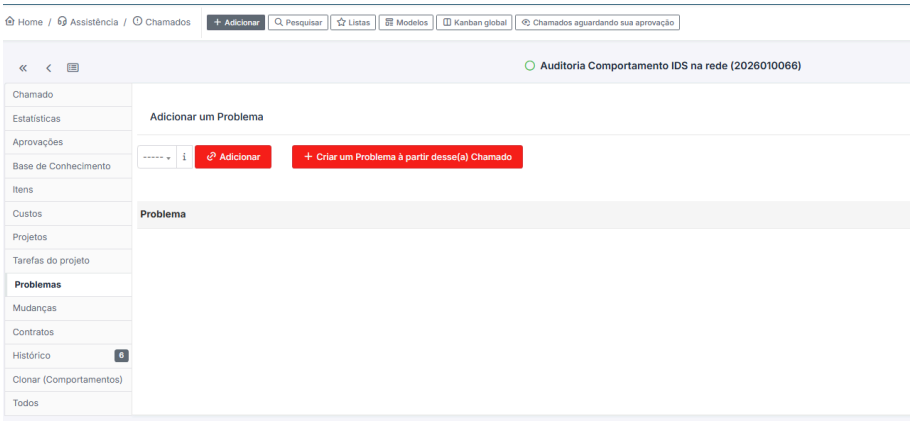
Este documento tem como objetivo a **verificação diária de possíveis ataques internos** à empresa, por meio da análise dos incidentes registrados na plataforma **Bitdefender GravityZone**. O procedimento deve ser executado **diariamente**, garantindo o monitoramento contínuo da segurança do ambiente.

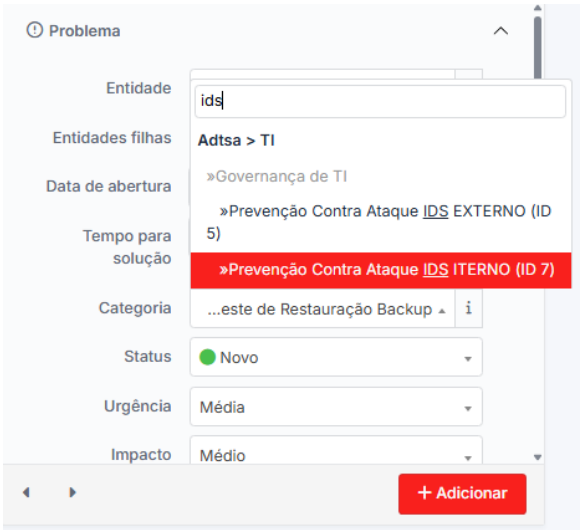
**Passo a passo:**

1. **Acesso à plataforma Bitdefender**
   - Acesse o endereço: https://cloud.gravityzone.bitdefender.com
   - Realize o login com suas credenciais.
2. **Consulta de incidentes**
   - No menu principal, acesse a aba **Incidentes**.
   - Aplique o filtro de período para **Últimas 24 horas**.
   - 

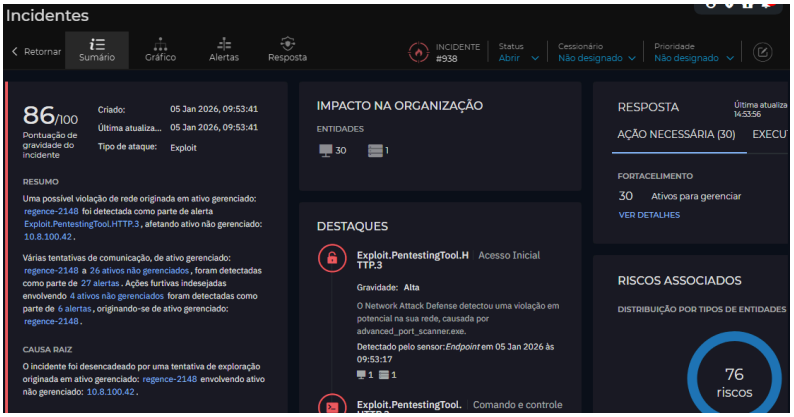
# AUDITORIA DIÁRIA DE ATAQUE INTERNO

### 3. 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
  - 

  - 

## 4. 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.
  - Exemplo de problema:
  - 

  - 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 gráfico, selecione o computador infectado e clique em **Isolar.**
  - **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.**
  - 


## 5. Encerramento

- Após o tratamento da não conformidade na estrutura:
  - Encerre o **problema** criado no GLPI.

# AUDITORIA DIÁRIA DE ATAQUE INTERNO

- Encerre o **chamado** correspondente, seguindo o seguinte padrão:

Na verificação diária dos eventos de segurança gerados pelo **Bitdefender GravityZone** 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}**

**2. Onde aconteceu ?**
Local, sala, equipamento, fornecedor
Sala de TI, **{Unidade/Local}**, console **Bitdefender GravityZone**, 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 **Bitdefender GravityZone** 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 **Bitdefender GravityZone** 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**.

# AUDITORIA DIÁRIA DE ATAQUE INTERNO

- **Acesse o grafana**
  - **Acesse o Grafana e vá em Menu>Dashboards>Complience>Complience Redes e Sistemas**
  -