



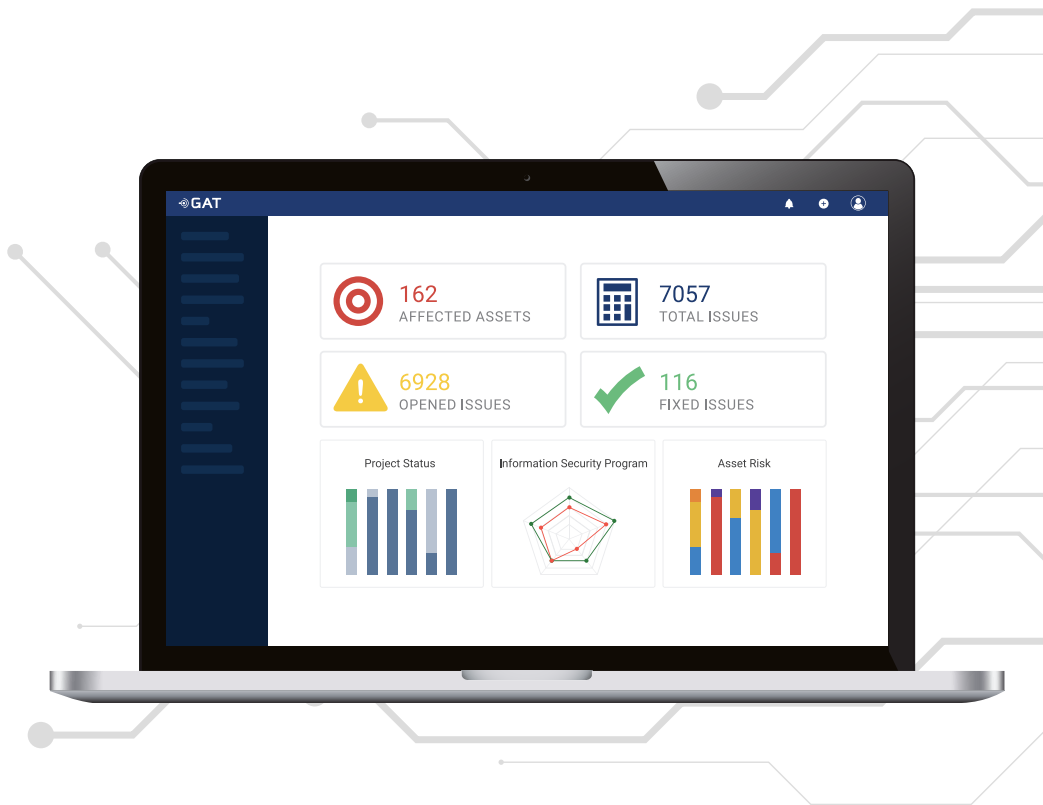
Get Ahead of Threats

DATASHEET

Gestão Integrada de Risco Cibernético e Conformidade



Índice



1. Introdução

2. Agregue valor ao seu negócio com GAT

3. GAT: a quem se destina

4. Casos de uso

5. Benefícios

6. Resultados

7. O que GAT oferece?

8. Integrações e arquitetura

9. Gestão Integrada de Riscos

10. Planos

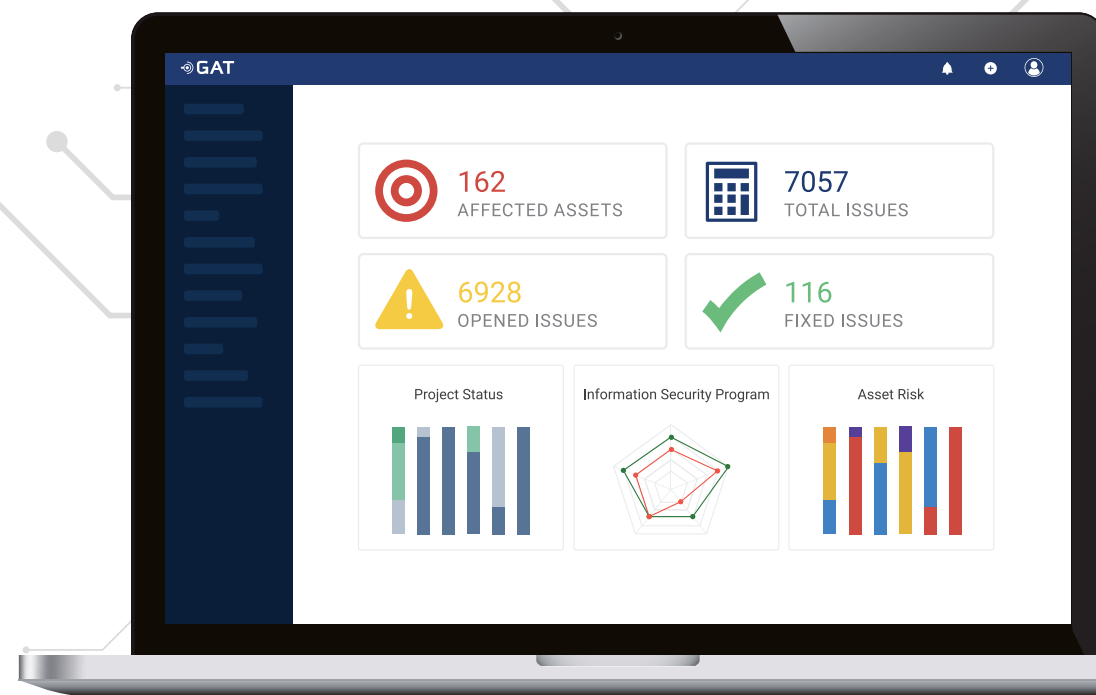
11. Segurança como Serviço

Tenha visibilidade da maturidade da sua segurança em tempo real e esteja à frente das ameaças

As ameaças para o negócio estão em toda parte: ataques cibernéticos, ransomwares, parceiros e fornecedores, vazamento de dados, erros humanos, não conformidades, ocasionando risco financeiro e de reputação.

Com tantas variáveis, é desafiador responder: como está nossa segurança agora?

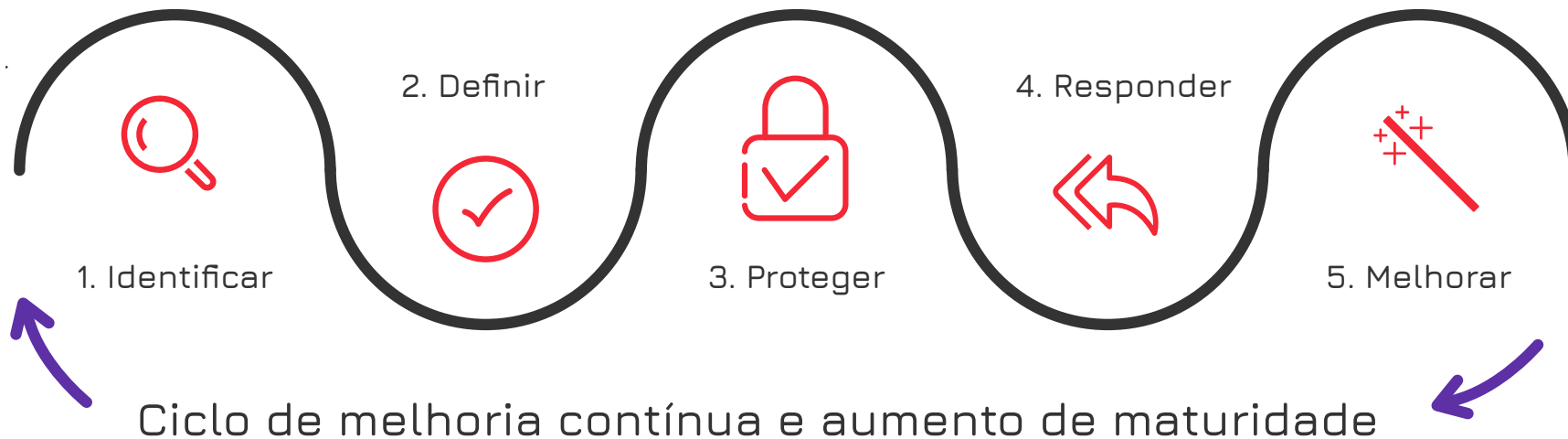
Estas preocupações são comuns a todas as empresas, independente do seu tamanho e segmento de mercado em que atuam.



Agregue valor ao seu negócio com GAT

O GAT é uma plataforma de gestão integrada de riscos (IRM) que permite estabelecer governança, gerenciar processos e projetos, estabelecer planos de ação, fornecendo visibilidade contínua de riscos e aumento de maturidade em cyber segurança.

Proporciona aos líderes de negócio a visão estratégica através do real grau de exposição do seu ambiente, além de facilitar o processo de conformidade com políticas internas e regulamentações.





A quem se destina?

À todas as empresas preocupadas em estabelecer governança da segurança digital e conformidade de seu ambiente organizacional.

Casos de uso

A plataforma GAT simplifica o processo de gestão da segurança da informação e conformidade por meio da automação de tarefas e integração com soluções tecnológicas, otimizando o tempo das equipes com atividades manuais e aumentando a eficácia na tomada de decisão e correção dos apontamentos.

Por meio da combinação de funções como inventário de ativos por criticidade ao negócio, mapeamento regulatório e importação de checklists e dados, a plataforma GAT possibilita atender aos seguintes casos de uso:

- Gestão de Vulnerabilidades
- Gestão de Riscos Digitais
- Gestão de Risco de Fornecedores
- Gestão de Auditorias
- Gestão de Conformidade (Bacen 4.658, ISO 27K, GDPR/LGPD, PCI-DSS)
- Gestão de Segurança de Aplicações

Conheça alguns benefícios do GAT

55%

Aumento de produtividade

94%

Otimização do ciclo de vida das ameaças



Alertas customizados



Monitoração em tempo real



Centralização de dados multiplataforma



Eliminação de controles em planilhas e sistemas descentralizados



Dashboards e indicadores com visões operacionais, gestão e executivas



Checklist de normativos e melhores práticas

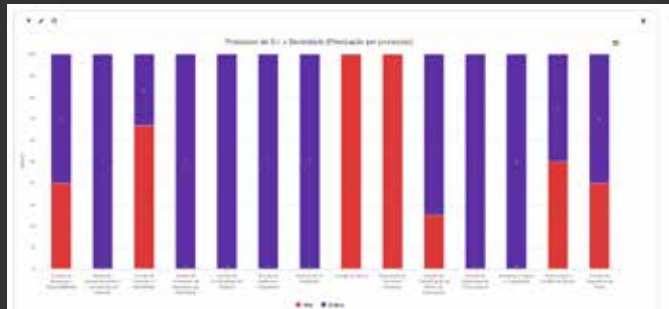


Resultados

A utilização da plataforma GAT traz ganhos exponenciais para toda a empresa no que tange a Gestão de Segurança.

- **Visão executiva** dos riscos cibernéticos e conformidades viabiliza a tomada de decisão e otimização de investimentos
- **Visão técnica** dos apontamentos, com classificação de criticidade, evidências, recomendação e plano de mitigação.
- Compartilhamento do risco e aumento da **sinergia** entre as áreas
- Criação de **plano de ação** de correção com base no impacto ao negócio e acompanhamento das tratativas.
- Visibilidade de **maturidade da segurança** em tecnologias, pessoas e processos.

O que GAT oferece?



Inventário organizacional: cadastre todos ativos do seu ambiente organizacional, como pessoas, IPs, aplicações, Cloud, fornecedores, unidades de negócios, classifique a criticidade e agrupe-os por função ou processo de negócio.

Gestão de projeto: organize suas iniciativas de segurança por projetos, defina um responsável e compartilhe com os envolvidos, estabelecendo assim um de fluxo de trabalho e aprovação.

Base de conhecimento: checklists de boas práticas e normativas de Segurança como: OWASP, ISO27K, LGPD/LPDP, GDPR, PCI-DSS, além de base de vulnerabilidade, recomendação e mitigação que podem ser personalizados conforme a necessidade.

Relatórios: exportáveis em pdf, excel ou csv

Dashboards: customizáveis e ilimitados contendo gráficos com visão operacional, gerencial e executiva. As informações podem ser privadas ou compartilhadas com outros usuários do GAT.

Automação: é possível criar regras para automatizar parte do processo de gestão, como envio de e-mails e repriorização de criticidades, regras de específicas ou excessões à política de segurança.

Workflow: Permite a definição de responsáveis pela correção e data limite, discussão e envolvimento de outras pessoas, e o aceite de risco.

Integrações & Arquitetura

A plataforma GAT oferece integrações nativas, importação de arquivos e uma API pública para criação de conectores customizados para automatizar o processo de gestão. A lista de integrações está em constante crescimento e atualização:

- Nessus e Tenable.io
- Acunetix
- Arachni
- Qualys (Web e Infra)
- Importação de planilhas em CSV

Arquitetura com suporte aos ambientes
Cloud e On-Premise



Gestão Integrada de Riscos

Processos de Segurança



Vulnerabilidades
Ameaças
Testes

Checklists
Auditoria
Conformidade

Inventário de Ativos



Pessoas
Infraestrutura
Aplicações

Cloud
IoT
Processos

Plano de Ação



Recomendação
de correção

Priorização,
atribuição e
acompanhamento

Integrações (API)



Tenable
Arachni
Qualys
Openvas

Acunetix
Nexpose
CSV



Métricas em tempo real



Indicadores
segmentados

Controle de
SLA's

Security as a Service



Programas de
Segurança
Customizados

Projetos
pontuais ou
recorrentes

Security KB



Base de conhecimento de
vulnerabilidades, recomendação,
mitigação, checklists e normativos

Escolha a licença GAT ideal para seu negócio:

Standard

Advanced

Enterprise

HOSPEDAGEM & INTEGRAÇÕES			
Integrações com ferramentas de terceiros	Sim	Sim	Sim
Integração com Active Directory		Sim	Sim
Notificação para Service Desk		Sim	Sim
Instalação local com suporte dedicado (on-premises)			Sim
GESTÃO & OPERAÇÃO			
Gerenciamento de Projetos	Sim	Sim	Sim
Importação de dados (planilhas, scanners, csv)	Sim	Sim	Sim
Orquestrador para ações, alertas e notificações	Sim	Sim	Sim
Relatórios customizados	Sim	Sim	Sim
BASE DE CONHECIMENTO			
Roteiros de conformidade e avaliação: PCI-DSS, ISO 27K, baseline, GDPR/LPDP, avaliação de fornecedores	Sim	Sim	Sim
Itens de verificação (Checklist), correção e testes	Sim	Sim	Sim
Referências cruzadas de vulnerabilidades e controles (CVE, CWE, scanners)	Sim	Sim	Sim
Upload de roteiros e itens customizados	Sim	Sim	Sim
SERVIÇOS E SUPORTE			
Treinamento (opcional)	1 dia	2 dias	2 dias
Onboarding: inclui aconselhamento especializado em cibersegurança e risco, importação de dados e orientações iniciais	Sim	Sim	Sim
Suporte ao Cliente	Sim	Sim	Sim
Programas de Segurança como Serviço	Opcional	Opcional	Opcional

Treinamentos e Workshops sobre Segurança da Informação e Conformidade

Para uma gestão adequada da segurança da informação e conformidade é essencial que os pilares pessoas, processos e tecnologia sejam considerados em conjunto visando a maturidade do ambiente organizacional, com adoção de controles e gerenciamento contínuo para redução de riscos e priorização de investimentos.

Conheça mais sobre cada um dos aspectos a serem considerados e fale conosco para workshops e treinamentos específicos sobre esses temas que possibilitam a otimização de resultados para sua empresa de acordo com a criticidade do seu negócio.

Risk & Compliance

Assessment do atendimento aos requisitos da resolução

Análise do nível de maturidade da organização em segurança da informação

Elaboração dos planos de ação para correção e mitigação dos riscos

Definição da política de segurança cibernética, do plano de resposta à incidentes, do processo de gestão de vulnerabilidade, entre outros.

Cyber-Protection

Gestão de Vulnerabilidades: identificação recorrente de vulnerabilidades, triagem, classificação e priorização das correções

Gestão de baseline: homologação de procedimento de configuração segura para ativos e sistemas, e identificação recorrente

Monitoramento contínuo de ameaças e threat intelligence

Hacker as a Service

Testes de invasão para identificar vulnerabilidades no ambiente organizacional

Auditoria de fornecedores

Exercícios Red Team para validar o processo de monitoração e plano de resposta à incidentes

Education

Definição do programa de conscientização

Criação de campanhas: cartilha, gincana, pílulas de segurança

Avaliação periódica de colaboradores por disparos de phishing e quiz

Auditoria de senhas

Testes de engenharia social para validar a efetividade do programa

Palestras e Workshops de conscientização por níveis de conhecimento

Application Security

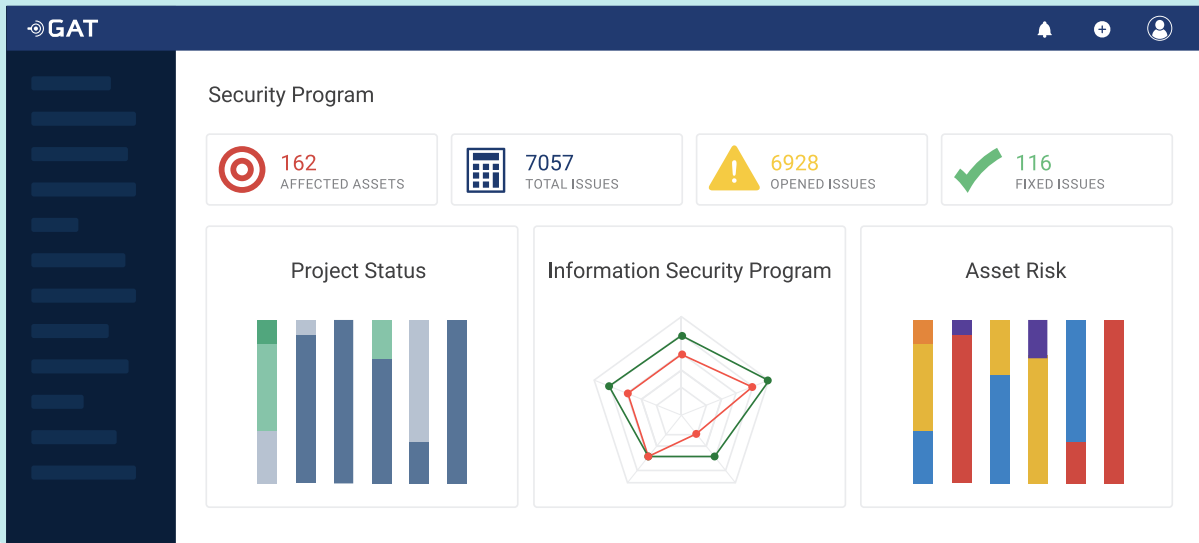
Revisão de maturidade do processo de desenvolvimento em segurança

Revisão dos controles da aplicação

Automatização de testes de segurança

Definição de requisitos de segurança para desenvolvimento e contratação de software

Adoção do ciclo de desenvolvimento seguro de software



Agende uma demonstração

Como está a Segurança Digital da sua empresa?

GAT está comprometido em ajudar empresas a responderem a essa pergunta com confiança e agilidade.

Saiba mais em gat.digital

