INFOWATCH®

INFOWATCH ATTACK KILLER

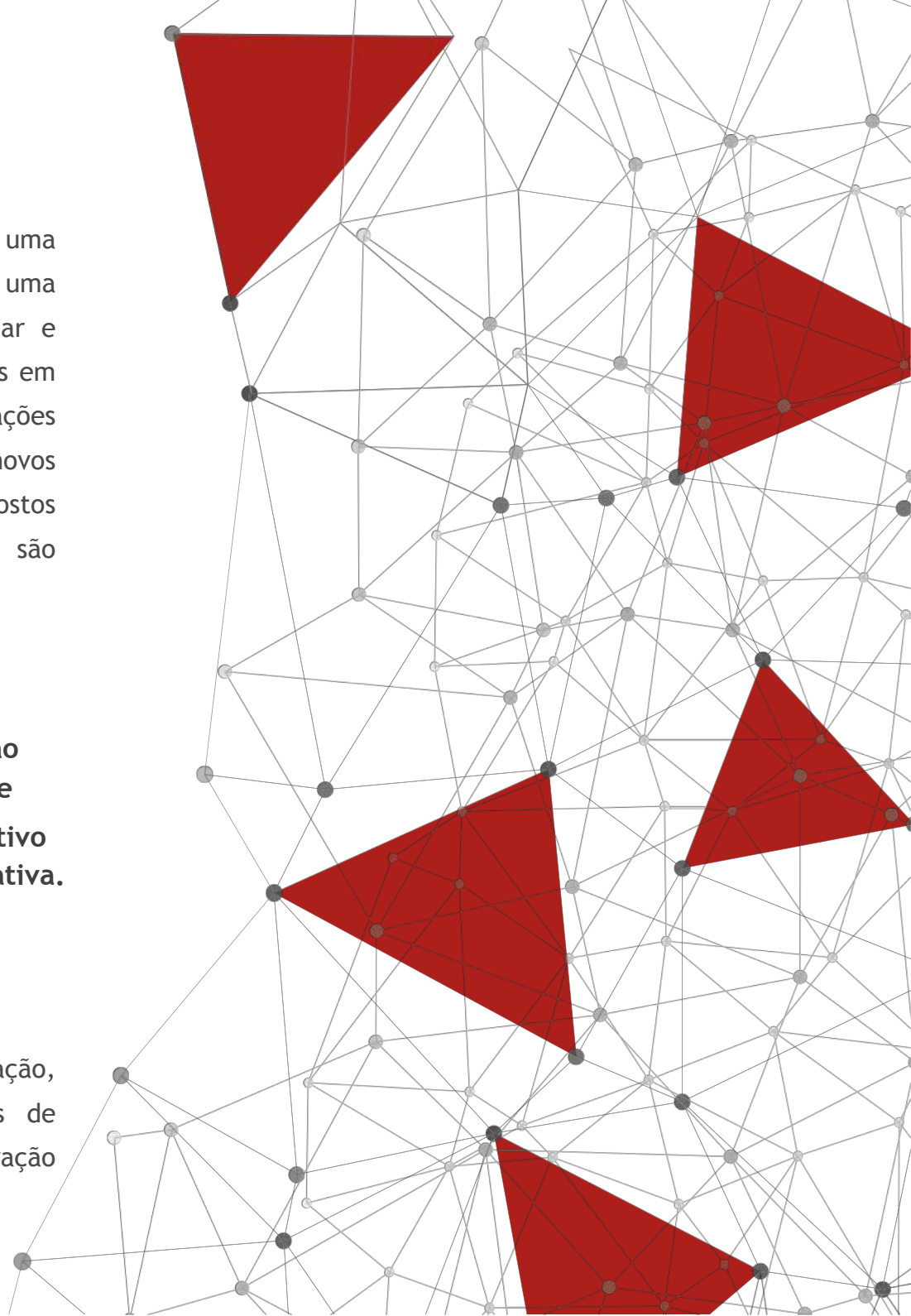
SECURITY AT A HIGHSPEED

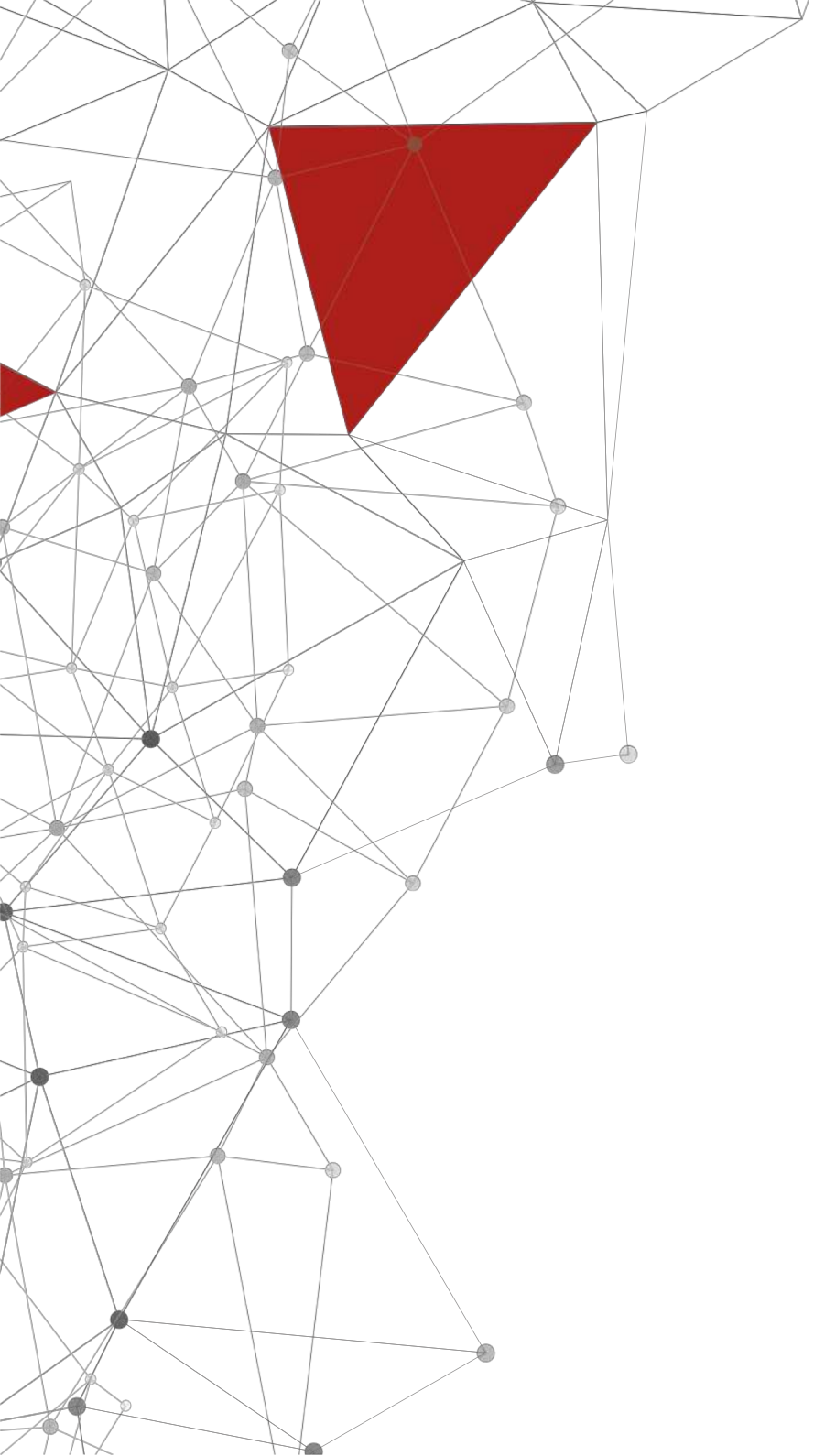
SEGURANÇA A ALTA VELOCIDADE

O ciberespaço sugere alta velocidade na entrega de informações, uma resposta cada vez mais rápida às necessidades do mercado e uma concorrência proativa, portanto, exige a implementação regular e rápida da nova funcionalidade do aplicativo da web. Fazer coisas em alta velocidade leva a erros e ainda não deixa tempo para verificações de segurança padrão. As empresas se preocupam mais com novos recursos do que com relatórios sobre possíveis ameaças, supostos hackers ou enormes perdas, e ainda assim especialistas são responsáveis pela segurança da informação.

Mais de 80% dos especialistas em segurança da informação concordam que as ameaças externas são as mais perigosas e difundidas hoje, enquanto 51% acreditam que um aplicativo da web é o ponto mais vulnerável da infraestrutura corporativa.

Atualmente, espera-se que a equipe de segurança da informação, como uma unidade de negócios, não apenas previna erros de programação em um estágio inicial, mas também acelere a liberação da atualização e, ao mesmo tempo, garanta a segurança deles.





A PROTEÇÃO COMEÇA NO ESTÁGIO DO DESENVOLVIMENTO...

Cada aplicativo da Web contém pelo menos cinco vulnerabilidades críticas, que os hackers podem explorar para assumir o controle de um recurso e obter acesso a bancos de dados, transações financeiras e pagamento, cliente e outras informações confidenciais.

Toda mudança em um recurso é uma ameaça em potencial: novas linhas de código contendo um erro acidental ou um backdoor intencional; uma conta de usuário recém-criada, protegida por uma senha fraca ou que oferece privilégios excessivos; ou um novo processo de negócios dando origem a um novo esquema de fraude. Quaisquer alterações em um objeto protegido exigem uma reconfiguração obrigatória do sistema de segurança.

Três anos atrás, não causou muitos problemas: os sistemas de informação foram atualizados uma vez por mês ou até mesmo um trimestre, deixando tempo suficiente para testes de laboratório e auditoria de segurança de terceiros. Hoje, os sistemas mudam uma vez a cada 2-3 dias no setor bancário, notavelmente com menos frequência na fabricação e com muito mais frequência no comércio eletrônico.

Sendo assim, as verificações de segurança devem ser automáticas e fazer parte integrante do desenvolvimento da Web.

...E NUNCA PARA!

Hackers, ataques DDoS e vazamentos de dados chegam às manchetes todos os dias. O problema não está com programadores que escrevem um código "ruim", mas com erros de website padrão embutidos em plataformas web, senhas de usuário fracas, o fato de que derrubar o site de um concorrente custa menos do que a concorrência justa no mercado e muitas outras razões.

Um ser humano pode acompanhar constantemente todas as vulnerabilidades publicadas, controlar sem falhas as configurações de ferramentas da Web, monitorar o conteúdo do usuário, verificar todos os possíveis vetores de ataque e reagir imediatamente ao tráfego anormal?

De acordo com os resultados da pesquisa anual da InfoWatch, o fator humano é o gargalo da segurança corporativa.

A abordagem da InfoWatch para garantir a segurança da infraestrutura crítica da Web baseia-se em três pilares:

- **Continuidade**
- **Adaptação**
- **Exclusão do fator humano ao máximo**

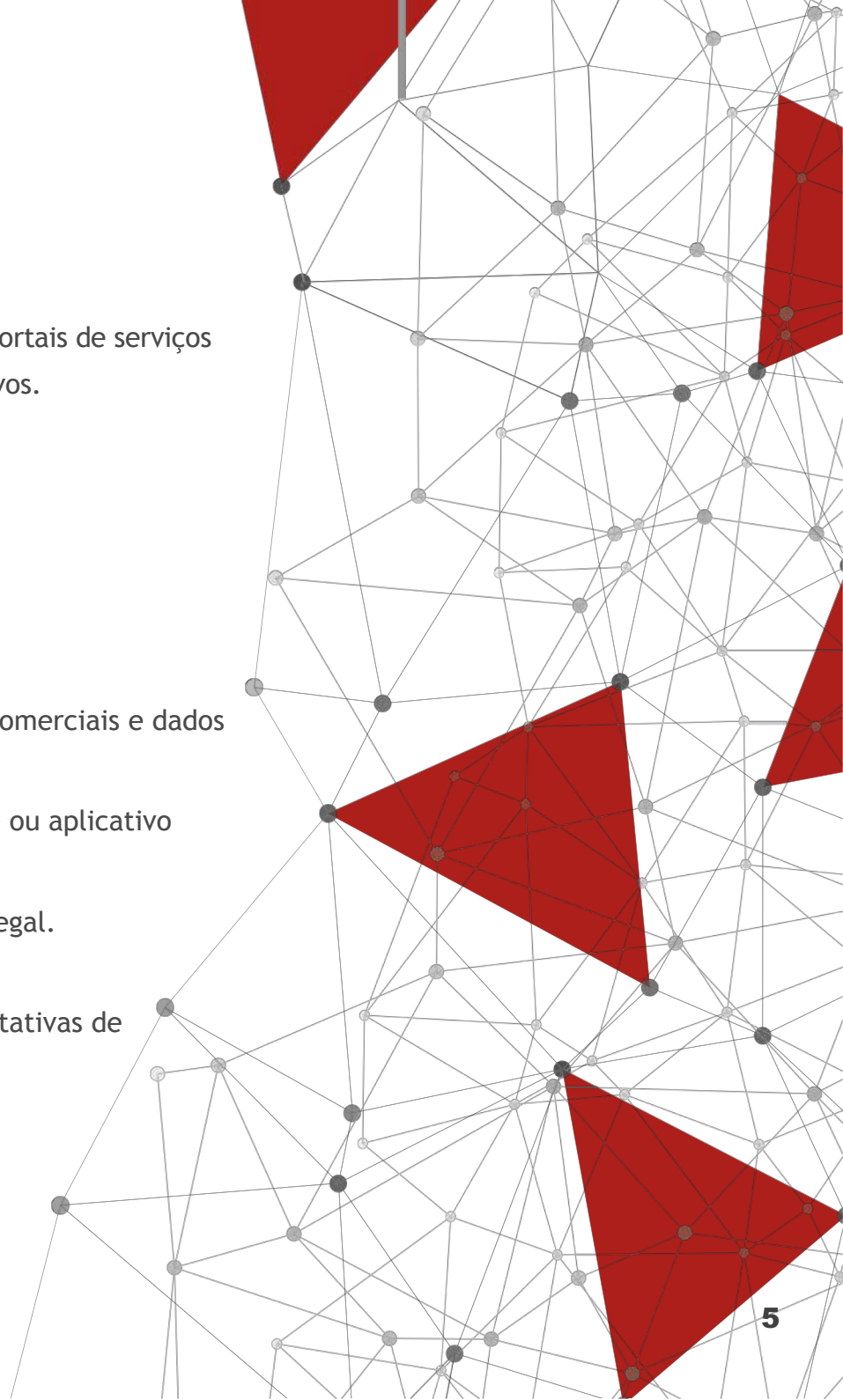
INFOWATCH ATTACK KILLER

Segurança continua ativa de aplicações de negócios essenciais

A solução é útil para sistemas bancários online, sites de comércio eletrônico, portais de serviços públicos, sistemas de trabalho em equipe, lojas online e outros sites e aplicativos.

QUESTÕES CRÍTICAS RESOLVIDAS RAPIDAMENTE

- Garantia de disponibilidade de recursos da web para os clientes.
- Proteção confiável de informações confidenciais, como segredos comerciais e dados pessoais.
- Garantia de transações financeiras concluídas por meio de um site ou aplicativo corporativo.
- Proteção contra falsificação de dados ou postagem de conteúdo ilegal.
- Manter a classificação de pesquisa de sites mesmo em caso de tentativas de manipulação de código por intrusos.
- Proteção dos usuários do site contra ataques, que injetam códigos maliciosos em páginas de sites.

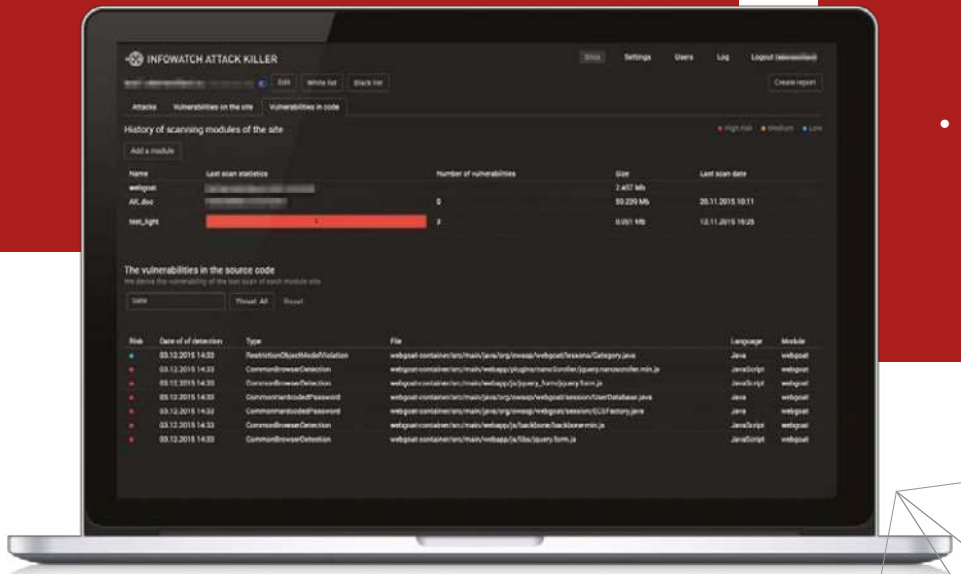


INFOWATCH ATTACK KILLER: ARQUITETURA

INFOWATCH ATTACK KILLER CUSTOM CODE SCANNER (CCS)

Tecnologia de análise estática para detectar vulnerabilidades do código-fonte do aplicativo.

- Identificando erros de código-fonte de acordo com os requisitos de programação segura dos fornecedores de PCI DSS, OWASP e plataforma.
- Suportando todas as linguagens de programação mais populares (Java, PHP, JavaScript, C #, etc.)
- Os relatórios são simples e não exigem conhecimento especial



INFOWATCH ATTACK KILLER WEB APPLICATION FIREWALL (WAF)

Pesquisa contínua de vulnerabilidades de aplicativos e proteção automatizada ativa contra ataques de hackers.

- Detecção de vulnerabilidades de aplicativos e proteção ativa contra hackers.
- Algoritmos de autoaprendizagem adaptando-se automaticamente a mudanças nos recursos da web.
- Não há necessidade de reconfiguração manual após cada atualização.
- Identificação de ataques em várias etapas com base em diversos eventos de segurança.
- Geração de relatórios e gráficos fáceis de ler e intuitivos.

INFOWATCH ATTACK KILLER ANTIDDOS

Proteção contínua contra ataques DDoS com base em uma rede distribuída em nuvem de nodes de filtragem.

- Assim que um site ou aplicativo é conectado, ele está sob proteção ativa e contínua.
- A proteção automática responde imediatamente a anomalias perigosas.
- Protegendo até projetos Web de carga extremamente alta contra ataques DDoS de qualquer intensidade.
- Isolando o tráfego parasitário no nível do node de filtragem, para que o site receba tráfego "limpo".
- Os usuários aprendem sobre tentativas de ataque apenas de relatórios.

COMO FUNCIONA

1

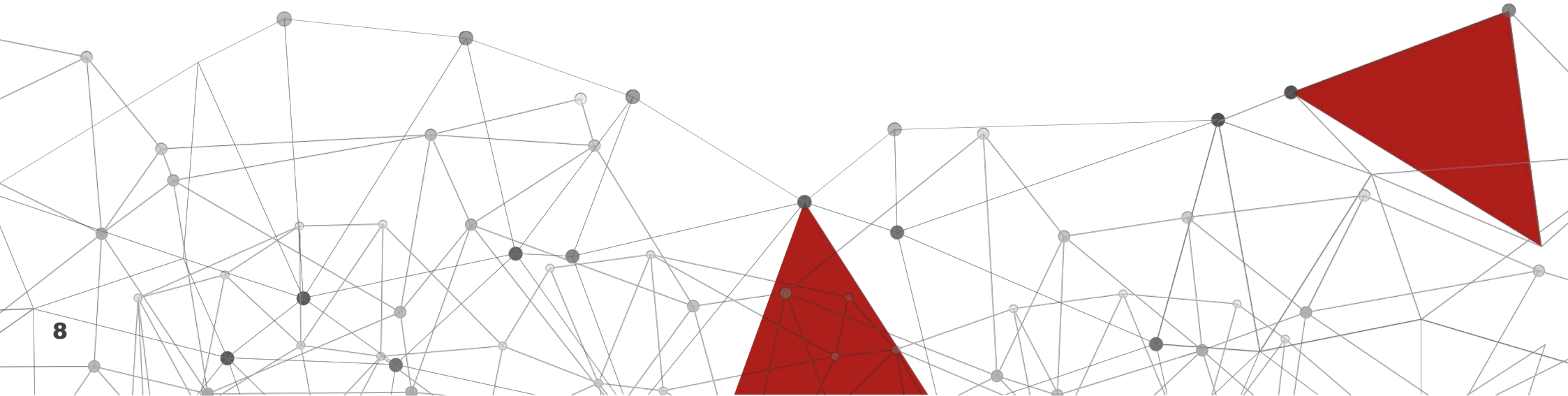
Custom Code Scanner (CCS) detecta vulnerabilidades e, em seguida, emite recomendações de correção. Com o InfoWatch Attack Killer no lugar, qualquer aplicativo está pronto para ser lançado, mesmo que um código contenha erros

2

Um scanner dinâmico, construído no WAF, determina a gravidade das vulnerabilidades detectadas e prioriza medidas de correção

3

Em seguida, as vulnerabilidades detectadas e quaisquer opções para explorá-las são automaticamente passadas da proteção passiva (scanners estáticos e dinâmicos) para a ativa: filtros DDoS, parte do AntiDDoS e firewall de aplicativo da Web (WAF)



4

O AntiDDoS e o WAF adaptam automaticamente suas configurações e adicionam regras de filtragem - patches virtuais - que bloqueiam consultas perigosas para uma funcionalidade vulnerável

5

Assim que um site ou aplicativo é conectado, ele está sob proteção contínua contra ataques DDoS.
Todo o tráfego protegido é permanentemente roteado através da rede distribuída de nodes de filtragem

6

Enquanto os programadores estão trabalhando nas vulnerabilidades detectadas e as atualizações lançadas passam por todo o ciclo de teste, o InfoWatch Attack Killer fecha automaticamente possíveis vetores de ataque

Com segurança contínua, todos ganham: uma empresa terá uma funcionalidade de lançamento rápido, clientes fiéis e receita; um desenvolvedor terá tempo suficiente para correção de erros sem qualquer pressão; enquanto um especialista do ISM terá um sistema funcionando com segurança

SEGURANÇA CONTÍNUA COM A CONTINUIDADE DOS NEGÓCIOS

Segurança como um recurso e sua vantagem competitiva

A base confiável estabelecida no estágio de desenvolvimento de aplicativos garante um desempenho estável, transações financeiras seguras e privacidade de dados armazenados.

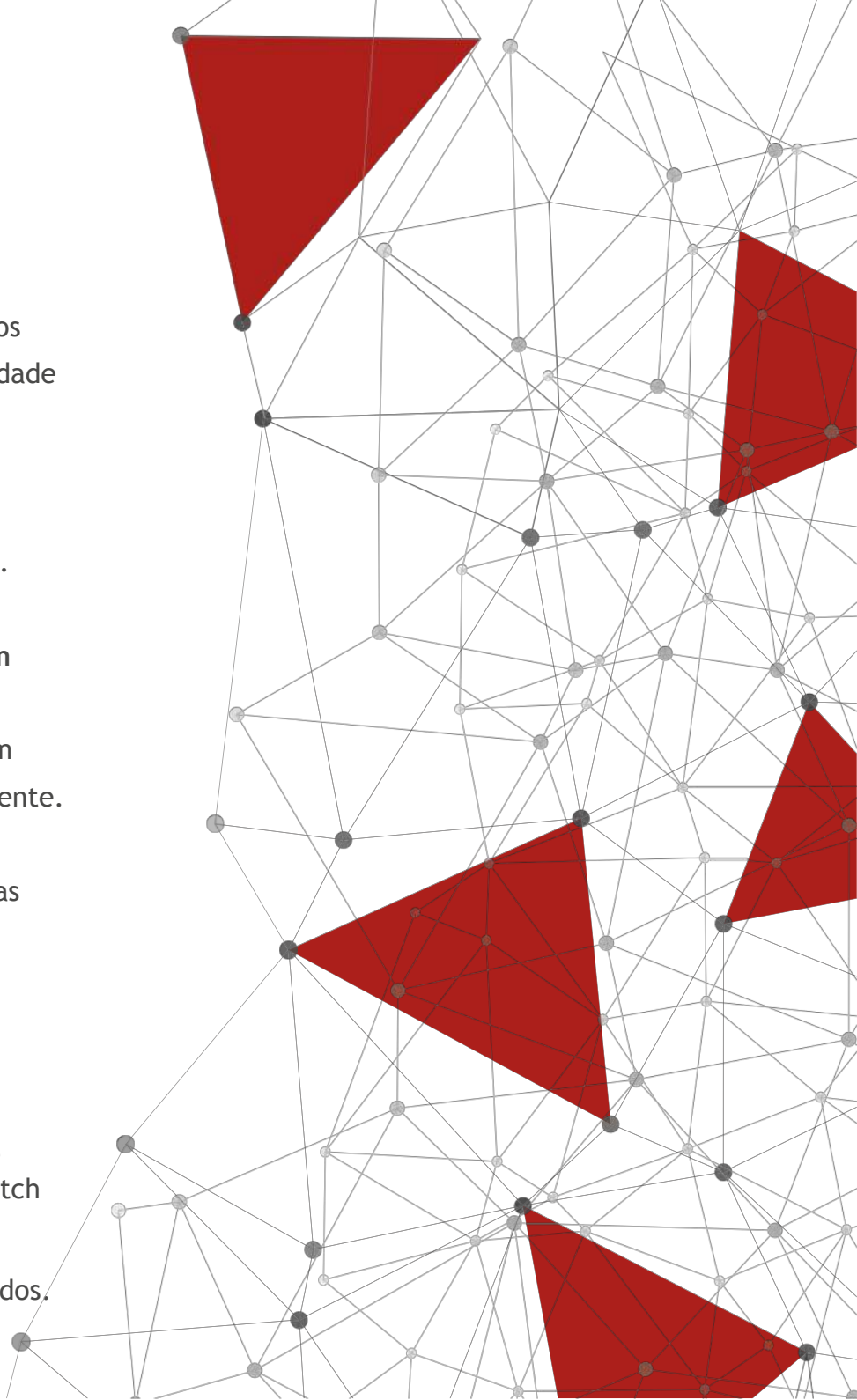
Com o InfoWatch Attack Killer, sua proteção começa logo no estágio de desenvolvimento. A confiança do usuário no site ou na confiabilidade dos aplicativos da Web aumenta a fidelidade do cliente e atrai novos públicos.

Mesmo atualizações vulneráveis estão seguras e prontas para serem lançadas

Não importa o quão simples sejam as atualizações, elas podem colocar em risco a segurança e, portanto, um aplicativo deve ser verificado regularmente. Verificações manuais de atualizações frequentes retardam a liberação do código. O InfoWatch Attack Killer permite a implantação imediata de novas funcionalidades graças à pesquisa contínua e à correção automática de vulnerabilidades até que os programadores as consertem.

Fator humano agora não pode afetar a operação sustentável

A indisponibilidade de recursos da Web causa perdas de reputação e financeiras. Embora a velocidade da resposta a incidentes geralmente dependa da reação dos operadores do sistema de segurança, o InfoWatch Attack Killer reage imediatamente a anomalias, evita falsos positivos devido a seus algoritmos de autoaprendizagem e, portanto, garante a disponibilidade contínua de um recurso da Web para usuários autorizados.



POR QUE INFOWATCH ATTACK KILLER?

Uma única solução para proteger contra todas as ameaças da Web

Trazendo equilíbrio à segurança, desenvolvimento e negócios

Conectividade modular

A proteção começa em qualquer módulo

Interface web única e relatório unificado

Gráficos e relatórios intuitivos sobre tentativas de ataques registrados em todas as camadas de proteção

União tecnológica de melhor qualidade

O InfoWatch Group uniu as principais tecnologias, cada uma delas é comprovada na batalha no mercado de segurança da informação

Compliance assistido

INFOWATCH®

soue

soue.com.br
contato@soue.com.br
+55 (11) 4382.2551