redbelt.com.br / contato@redbelt.com.br / +55 11 3512-7453

Datasheet
Threat Intel

Threat Intelligence é a diferença entre prevenir a ocorrência de um ataque e ser vítima de um incidente cibernético.

Por meio de pesquisas personalizadas para categorizar, vincular e analisar ativos em todas as camadas da Internet, a solução de Threat Intelligence da Redbelt Security fornece insights fáceis de consumir.

Assim, alimenta e fortalece a estratégia de defesa do negócio.

Fornecemos uma visão compreensiva do cenário único de ameaças da organização. Trazemos uma combinação de recursos avançados de pesquisa e análise, automação e inteligência finalizada por especialistas.

Com tecnologias como SOCRadar (Cyber Threat Intel & Dark Web Radar) e a ferramenta CHRONOS, desenvolvida pelo time técnico da Redbelt, a solução possibilita buscas automatizadas em múltiplas camadas da internet — surface, dark e deep web — para identificar e mitigar potenciais ameaças.

Também oferecemos ação direta através do takedown de sites maliciosos e perfis falsos. E o monitoramento de usuários VIPs em redes sociais, para antecipar engenharias sociais, bem como a análise de grandes vazamentos de dados para proteger credenciais e informações sensíveis.

Nossos dashboards em tempo real e nosso acervo de inteligência contextualizada, o negócio ganha insights críticos que permitem uma resposta rápida e eficiente a incidentes de segurança, garantindo resiliência e integridade digital.

Benefícios da solução de Threat Intelligence

Acesso ao CHRONOS. Plataforma desenvolvida pelo nosso time de especialistas, que oferece recursos de dashboards em tempo real, alarmes com notificações, permitindo uma visão abrangente e atualizada das ameaças cibernéticas, e é uma ferramenta crucial para a identificação proativa e resposta rápida a incidentes de segurança.

Integração com SOC e SIEM. Gerenciamento de IoCs de forma avançada, colaborando com equipes de segurança para respostas coordenadas e eficientes.

Descoberta de riscos desconhecidos. Acesso à inteligência finalizada por especialistas, customizável e fácil de escalar. Identificação de ameaças globais, fora do perímetro da organização.

Defesa cibernética informada. Melhora da estratégia de segurança com uma consciência situacional holística de vulnerabilidades, atores de ameaças, como atuam e impacto potencial no negócio.

Compreensão de prioridades. Menor fadiga de alertas com acesso instantâneo às ameaças específicas que são importantes para a organização, à medida que ocorrem. O que ajuda a priorizar as atividades de segurança e prevenir ataques de forma eficaz.

Reuniões gerenciais: produzimos relatórios e realizamos reuniões de acompanhamento do projeto de forma periódica.

Aumente a eficiência do SOC

A solução de Threat Intelligence da Redbelt Security oferece aos analistas de segurança rastreamento atualizado de invasores, malware e vulnerabilidades para ajudá-los a priorizar alertas e compreender as capacidades e motivações do adversário. É uma abordagem proativa para identificar e mitigar ameaças avançadas que podem não ser detectadas por ferramentas de segurança. Ao invés de esperar que alertas ou incidentes sejam gerados, os analistas de segurança realizam buscas ativas por sinais de comprometimento e atividades maliciosas no ambiente.

Ao correlacionar os alertas gerados pelo SOC com os indicadores de Threat Intel, as equipes de segurança obtêm orientação direta durante a triagem, investigação e resposta. Isso melhora a velocidade e a eficácia da segurança, ao mesmo tempo que reduz a fadiga geral dos alertas.

O que está incluído

Monitoramento de vazamento de dados e segredo de códigos

- Visão dos cibercriminosos sobre o negócio
- Alertas contextualizados
- Relatórios sobre o incidente desde a detecção até a conclusão
- Time especializado para apoio em respostas a incidentes
- Melhoria da resposta a incidentes

Monitoramento de domínios e aplicativos falsos

- Identifique os nomes de domínio que usam a sua marca
- Detecte nomes de domínio de diferentes TLDs
- Detecte registro de domínios semelhantes criados para golpes
- Identifique apropriação indevida da marca
- Melhore a resposta a fraudes

Monitoramento e proteção de VIPs e executivos

- Monitoramento 24x7 de pessoas físicas em todas as camadas da Web
- Monitoramento e remoção de perfis falsos nas redes sociais
- Detecção de possíveis contas fraudulentas
- Monitoramento e detecção de e-mails corporativos expostos
- Identificação de credenciais vazadas

Remoção de conteúdo infrator (takedown)

- Detecção precoce de conteúdo infrator
- Notificação rápida
- Menos tempo de exposição ao risco
- Verificações automáticas e acompanhamento por especialistas
- Mais proteção da jornada de compra de consumidores e clientes
- Proteção do lucro e da reputação da marca

Visualize o risco cibernético, adapte proativamente as barreiras de proteção e antecipe investidas de cibercriminosos. Decifre e interprete o que ameaça o negócio e eleve a capacidade de prevenção e resposta. Tome providências antes de ataques.

› Converse com um de nossos consultores