

# Transformando Problema em Conhecimento

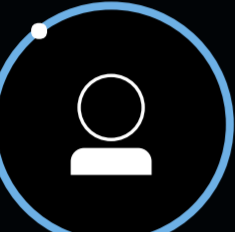
Com equipes de segurança cada vez mais enxutas e enfrentando um fluxo cada vez maior de dados de ameaças, os analistas de hoje estão sobrecarregados.

[Conheça nosso site](#)

[Fale com especialista](#)

Uma organização comum enfrenta **200,000** ocorrências de segurança por dia

## Um fluxo de ameaças e vulnerabilidades



USUÁRIOS



CLOUD

Os analistas de segurança enfrentam milhares de vulnerabilidades, ameaças e ataques todos os dias. O QRadar elimina os problemas da rede, pois foca nas ocorrências de segurança importantes para que as equipes de segurança possam agir rapidamente na defesa contra eles.

### Interpretação dos Dados

Normalize o registro e os dados de fluxo de rede em um formato consistente para uma análise mais eficiente.

### Atividade do Perfil

Crie uma linha de base de assets, usuários, serviços e atividades de rede para aprender padrões comuns e permitir uma detecção precisa de anomalias.

## Analítica Avançada

### Análise de Padrões

Analisa atributos de situações em tempo real contra padrões de atividades mal intencionadas conhecidas para identificar e classificar rapidamente as ameaças ativas.

### Deteção de Anomalias

Detecta padrões comportamentais "comuns" ao longo do tempo e identifica desvios da normalidade conhecida que podem indicar uma ameaça.

### Análise Histórica

Muitos invasores pulam etapas comuns na tentativa de violar sistemas. Quando determinadas ações não são precedidas pelo comportamento esperado, a análise histórica pode sinalizá-las para que seja dada atenção.

### Análise Estatística

Analisa estatisticamente o comportamento da entidade para ajudar a identificar sistemas periféricos potencialmente comprometidos, como terminais que enviam volumes grandes e anormais de dados para serviços em nuvem não autorizados.

### Comportamento da Entidade

Monitora continuamente as entidades da máquina em busca de comportamentos, serviços e conexões anormais para detectar os sistemas comprometidos de maneira mais eficiente.

### Análise de Limite

Analisa os volumes de atividades para identificar desvios da norma, como aumentos ou reduções de itens, por exemplo, a largura de banda ou o uso de serviços.

### Análise Comportamental do Usuário

Analisa continuamente o comportamento do usuário individual para detectar desvios que podem ajudar a identificar credenciais de usuário comprometidas e atividades internas mal intencionadas.

### Grupo de Colegas

Agrupa os usuários em grupos de colegas com base em atividades semelhantes e procura continuamente comportamentos anormais para encontrar usuários de alto risco ou mal intencionados de maneira mais rápida e precisa.

### Inteligência de Ameaças

Compara os atributos da situação com informações atualizadas sobre ameaças, como domínios ou hashes mal intencionados, para identificar as mais recentes ameaças conhecidas de maneira mais precisa.

### Análise de Previsões

Usa um modelo de previsão comportamental para prever comportamentos futuros e detectar quando ações ou comportamentos fogem do esperado.

### Alerta

Reúne sinais relacionados descobertos durante a análise para estabelecer a cadeia de ponta a ponta de uma ocorrência de segurança, determinar a gravidade da situação e gerar um único alerta.

## Investigar

### Causa Raiz

## Raciocínio Cognitivo

Utiliza o processamento de linguagem natural para criar automaticamente gráficos de conhecimento, usados para determinar a causa raiz, fornecer uma visão geral do ataque e identificar IOCs relacionados.

### Agente Contra Ameaças

Melhore drasticamente a velocidade, o rendimento e a precisão para se defender contra ataques cibernéticos de maneira mais eficiente.

Com o QRadar, um analista de segurança pode evitar a confusão e o atraso causados por milhares de ocorrências por dia e, em vez disso, direcionar incidentes suspeitos com eficiência, baseado em informações claras e úteis.

[Conheça nosso site](#)

[Fale com especialista](#)