UOL DIVEO

SIEM - Smart Correlation

IDENTIFIQUE E GERENCIE DE MANEIRA PROATIVA
SEUS LOGS E INCIDENTES DE SEGURANÇA

IDENTIFIQUE E GERENCIE DE MANEIRA PROATIVA SEUS LOGS E INCIDENTES DE SEGURANÇA

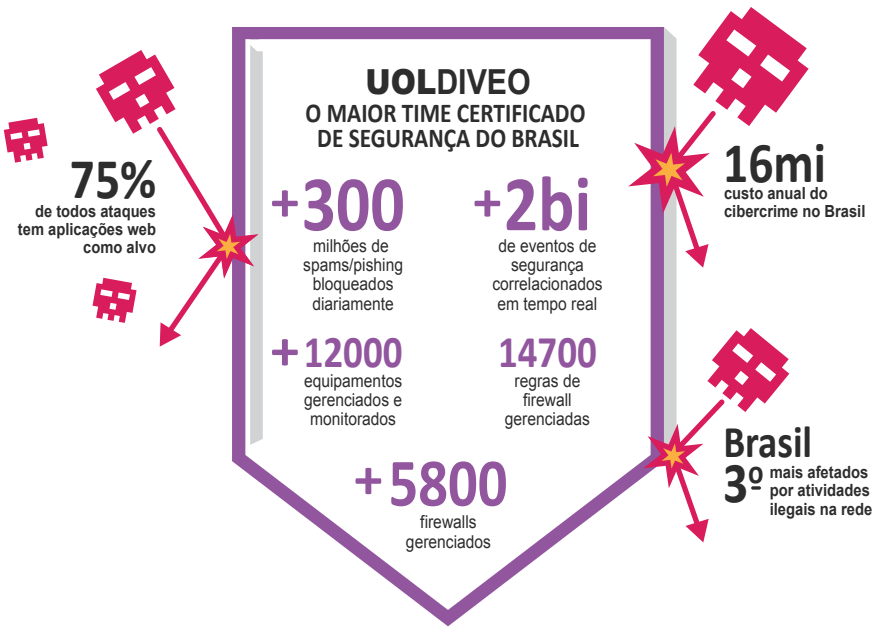
Os incidentes de segurança já são um destaque no mercado mundial. Estes problemas também já são uma realidade no Brasil, na qual o mantém como um dos países com maior foco dos hackers, principalmente para roubo de informações e crimes eletrônicos.

Proteger sua empresa contra as constantes ameaças e tendências globais é uma tarefa árdua e complexa, principalmente quando se faz necessário conhecer por completo seu ambiente tecnológico, extrair e correlacionar informações importantes que indicam uma falha ou exploração de segurança.

O SIEM do MSS UOLDIVEO é o serviço que opera de forma proativa e automática para detectar comportamento anômalos e incidentes de segurança

Este serviço agrega inteligência e proatividade na coleta, análise e tratamento dos eventos gerados pelos diversos dispositivos existentes na infraestrutura de TI e Segurança do cliente, correlacionando suas informações e extraindo resultados efetivos que auxiliam na atuação preventiva para identificação de ataques, resposta a incidentes, suporte para mitigação de riscos, análise causa raiz, atender às exigências legais e normativas, além de fornecer exibilidade para geração customizada de outros indicadores necessários ao negócio do cliente.

Especialistas de segurança do **SOC (Security Operations Center)** do **UOLDIVEO** monitoram os eventos de log 24x7x365, garantindo que quaisquer ocorrências anômalas, tendências, e atividades críticas sejam imediatamente identificadas, escaladas e tratadas.

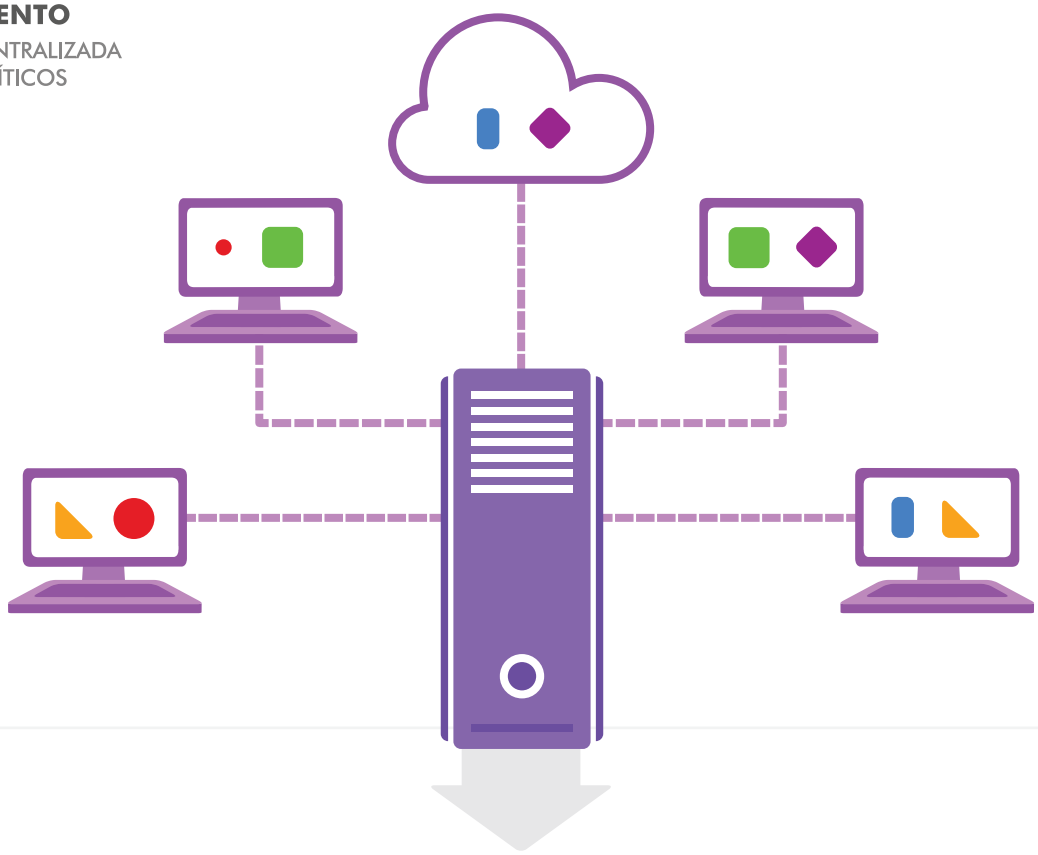


O serviço integra com os principais tipos de dispositivos, garantindo ampla cobertura em toda a infraestrutura de rede e segurança. Todos os dados são mantidos pelo período necessário ao seu negócio, a fim de satisfazer questões de conformidade, legais e as exigências de gestão.

Copyright © 2013 UOLDIVEO SA. Todos os direitos Reservados.

MONITORAMENTO

OBSERVAÇÃO CENTRALIZADA
DOS EVENTOS CRÍTICOS
EM TEMPO REAL



COLETA

COMPRESSÃO, NORMALIZAÇÃO
E AGRUPAMENTO DOS EVENTOS

CORRELAÇÃO

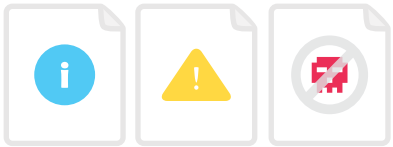
CRUZAMENTOS CUSTOMIZADOS
DOS EVENTOS DE ACORDO COM
A NECESSIDADE DO NEGÓCIO

ANÁLISE

IDENTIFICAÇÃO BASEADA EM
COMPORTAMENTO ANORMAL
E POLÍTICAS DE SEGURANÇA

RESULTADOS

RELATÓRIOS PERIÓDICOS SOBRE A
DETECÇÃO DE INCIDENTES DE
SEGURANÇA EM TEMPO DE REAÇÃO



Copyright © 2013 UOLDIVEO SA. Todos os direitos Reservados.

MODELO DE OFERTA

- ***Básico*** - Monitoração 24x7x365 em tempo real com alertas pré-definidos, tratamento do incidente, análise da causa raiz, relatórios periódicos e dashboards otimizados.
- ***Avançado*** - Monitoração 24x7x365 em tempo real com alertas pré-definidos e customizados de acordo com a necessidade do cliente, coletores externos, tratamento do incidente, análise da causa raiz, relatórios periódicos e dashboards otimizados.

Benefícios do *SIEM* do MSS UOLDIVEO

- Gerenciamento centralizado dos eventos de ativos críticos em tempo real;
- Detecção baseada em comportamento anômalo;
- Automatiza a análise de eventos para discernir ataques reais e invasores;
- Correlacionamento customizado de acordo com a necessidade do negócio;
- Aumento da efetividade na detecção de incidentes e reduz o tempo de reação;
- Compliance com os principais padrões e metodologias do mercado;
- Suporte à rastreabilidade para processos investigativos e incidentes;
- Redução dos riscos relacionados à imagem institucional, perda de receita, descumprimento de normas e regulamentos;
- Monitoração e gerenciamento 24x7x365 através de equipes especializadas.

Copyright © 2013 UOLDIVEO SA. Todos os direitos Reservados.

UOL DIVEO

SERVIÇOS GERENCIADOS

Produtividade para seus negócios

Tel. 11 3092 6161 **www.uoldiveo.com.br**