



Os recursos de EDR e HIPS que a sua organização precisa para combater ameaças.

Trabalhando em conjunto, o DarkLayer Guard™ e o VectorN Detection™ são as ferramentas proativas e autônomas ajustadas para sobrepor sobre outras tecnologias de proteção baseadas em detecção de código.

Aprimorada com o TTPC (Ameaça para Correlação de Processos), sua organização ganha as ferramentas de busca de ameaças essenciais para mapear os pontos críticos de segurança no seu ambiente.



DARKLAYER
GUARD™

O Sistema de Prevenção de intrusão essencial baseada em host (HIPS)

O DarkLayer Guard™ é um mecanismo exclusivo de filtragem de tráfego bidirecional que oferece suporte à listagem branca / preta totalmente personalizável.

Com ele, sua organização pode bloquear a comunicação na rede para reduzir as explorações de Zero Hour, Ransomware C & C, ataques de última geração e fugas de dados.

Usando nossa tecnologia inovadora Threat To Process Correlation, podemos identificar processos de ataque e fornecer recursos HIPS para endpoints.

As técnicas de ofuscação de malware estão ficando mais avançadas e capazes de evitar a detecção tradicional.

Com o DarkLayer Guard™ e o VectorN Detection™, o malware é bloqueado ao nível do tráfego, impedindo a comunicação com a infraestrutura criminosa.

Aproveitando a inteligência exclusiva obtida por meio do bloqueio de ameaças no nível do DNS, HTTP e HTTPS, o DarkLayer Guard™ e o VectorN Detection™ não apenas oferecem a capacidade de impedir ataques ativos, mas também aceleram o processo de investigação. Dessa forma, endpoints vulneráveis podem ser identificados e reforçados contra ameaças futuras, garantindo uma abordagem proativa à segurança.

O custo de implementar uma nova solução, incluindo uma solução de segurança, tem sido uma proposta intimidante para empresas, especialmente aquelas menores e com recursos mais limitados.

Esse não é o caso aqui.

100% compatível com suas soluções existentes e outros módulos Heimdal Security, DarkLayer Guard™ e VectorN Detection™ são as soluções autônomas para combater malwares, ransomwares e outras ameaças.

"Em termos de prevenção de ataques, já vimos um valor claro nos primeiros dois meses em que usamos o Heimdal, mesmo tendo alguns ataques de ransomware bloqueados. A maneira como detecta malware que o antivírus não vê é especial. Heimdal é uma maneira simples e rápida de melhorar nossa segurança central e nos ajuda a prevenir ataques antes que eles aconteçam."

- Kifaf General Trading, principal distribuidor da Sony Entertainment na Região dos Emirados Árabes Unidos

"Mesmo que nossa rede esteja muito bem protegida, sabíamos que tínhamos que adicionar uma camada extra de segurança aos nossos clientes. Simplesmente porque a maior parte são laptops. Quando esses clientes deixaram o prédio, ficou claro que o antivírus não era suficiente de acordo com o cenário moderno de ameaças."

- Schultz Information



VECTOR
DETECTION™

Detecção autônoma de código para encontrar ameaças não vistas por NGAV e scanners de código

Ao rastrear a comunicação de dispositivo para infraestrutura, o VectorN Detection™ detecta cepas de malware de segunda geração que nenhum outro produto pode ver, entregando efetivamente um HIDS na camada de tráfego da máquina.

Usando "Learning Machine" para estabelecer padrões de ataque e oferecer indicadores de comprometimento / ataque (IOA / IOC), esse é um complemento exclusivo que impulsionará qualquer outro tipo de segurança de terminal.

Os criminosos podem facilmente contornar os scanners de código e de comportamento, como o antivírus, bem como os firewalls, desencadear ataques de ransomware devastadores ou criar fugas de dados que prejudiquem a sua organização.

10,975 DOMÍNIOS MALICIOSOS

O número de domínios maliciosos removidos mensalmente no Reino Unido, por uma única agência.

- NCSC.gov.uk

1,783 RECLAMAÇÕES RANSOMWARE

O número de reclamações registradas O Internet Crime Complaint Center (IC3), com uma média de 5 vítimas diárias

- FBI

3,785 FUGAS DE DADOS CORPORATIVAS

Em 2017, conforme registrado no Internet Crime Complaint Center (IC3). Em média, 10 fugas acontecem diariamente.

- FBI

85%

dos MSPs relataram que as vítimas do ransomware tinham software antivírus.

- Datto, Inc: Global State of the Channel Ransomware Report, 2018

65%

dos MSPs relataram que as vítimas de ransomware tinham filtros de email/spam.

- Datto, Inc: Global State of the Channel Ransomware Report, 2018

29%

dos MSPs vítimas tinham pop-up blockers.

- Datto, Inc: Global State of the Channel Ransomware Report, 2018



Anti-Malware Solution of the Year
Impedir, não apenas atenuar ataques
Entre em contato hoje mesmo para descobrir como eles melhoram o seu ambiente.



Contate-nos em

+45 7199 9177

or

corpsupport@heimdalsecurity.com