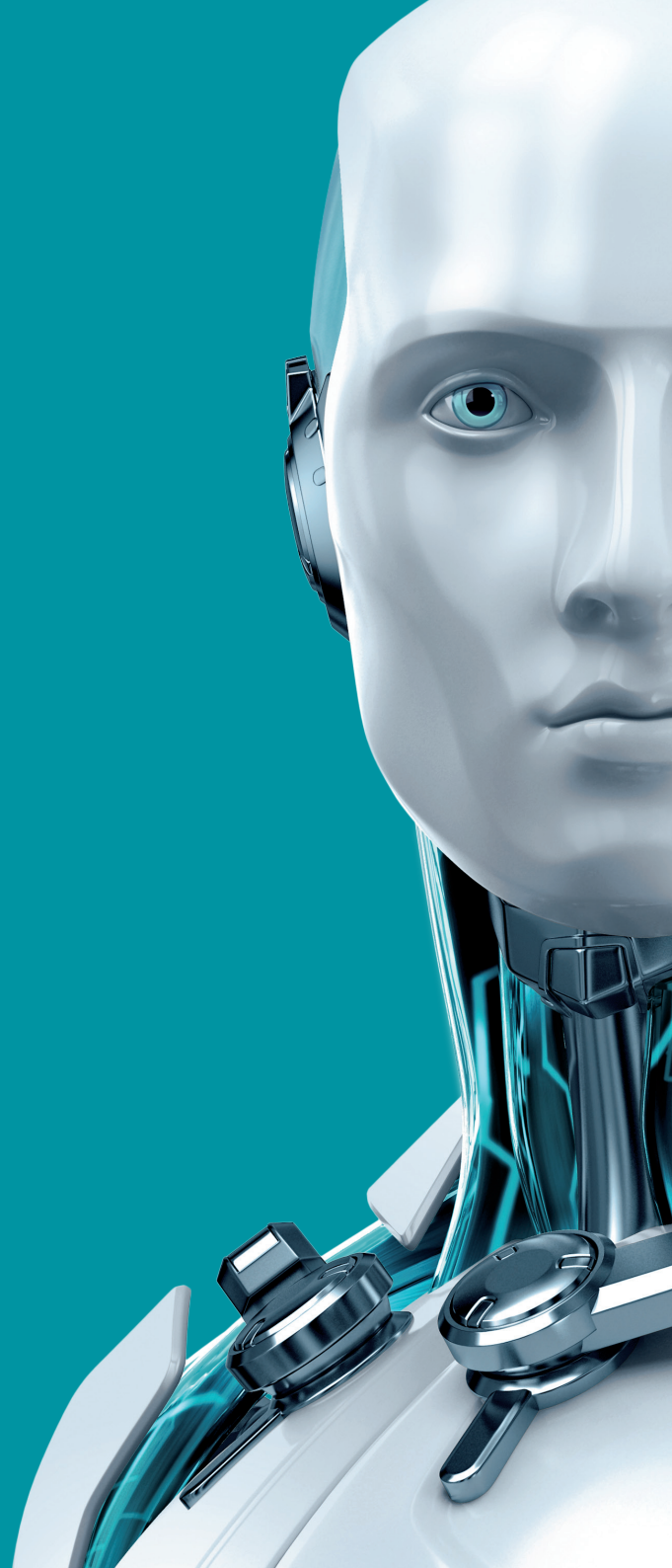
GREYCORTEX MENDEL

Análise de Tráfego de Rede

Visão Geral do Produto

BUSINESS

ESET TECHNOLOGY ALLIANCE



GREYCORTEX MENDEL

Análise de Tráfego de Rede com o GREYCORTEX MENDEL

O GREYCORTEX MENDEL é uma análise de tráfego de rede avançada, com monitoramento de performance, detecção de ameaça e solução de profunda visibilidade de rede para empresas, governo e infraestrutura crítica. O MENDEL usa inteligência artificial moderníssima, aprendizado de máquina e grandes análises de dados para tornar a infraestrutura das organizações de TI seguras e confiáveis.

O MENDEL não é uma outra ferramenta de monitoramento de comportamento de rede. Ele usa a combinação de análise de ameaça, aprendizado de máquina, inteligência artificial, pacote de inspeção, correlação de eventos e outras ferramentas para identificar atividade suspeita dentro de uma rede. Isso permite às equipes de segurança achar ameaças com grande assertividade e tomar ações mais rápidas do que as soluções de segurança de rede tradicionais.

Identificando ameaças antes que o dano aconteça

Muitos outros provedores focam em métodos conhecidos de ataque ou pedaços de códigos maliciosos. Usando métodos de inteligência artificial avançadas, o MENDEL vai além das ameaças conhecidas para detectar e identificar sintomas de comportamento malicioso em nível atômico. Ameaças são identificadas em seu estágio inicial, diminuindo o tempo de resposta a incidentes, prevenindo mais danos e reduzindo os riscos como um todo.

O MENDEL também possui detecção baseada em assinatura integrada e inteligência de ameaças conhecidas, aumentando sua capacidade de detecção, ao mesmo tempo em que reduz a taxa de falsos positivos.

8 – 16 horas
Tempo que um adversário precisa para invadir uma rede

8 meses
Tempo médio que uma ameaça persistente avançada fica imperceptível

98 dias
Tempo médio de detecção de uma ameaça persistente

71%
Das organizações não conseguiram detectar falhas

Adaptação Automática

A ferramenta de Análise de Comportamento de Rede única do MENDEL usa análise matemática avançada em aprendizado de máquina para gerar e adaptar regras de detecção de tráfego passado. Ele integra os inputs de outras ferramentas de detecção e inclui algoritmos especializados que, entre outras funções, conseguem distinguir entre o comportamento de máquina e o humano. A ferramenta de Análise de Comportamento de Rede do MENDEL é a única solução no mercado que oferece essa habilidade.

Detecção Mais Sensível

O protocolo de Métricas de Rede de Segurança Avançada do MENDEL permite que ele monitore mais de 70 funcionalidades de cada fluxo de rede individual. Esse nível avançado de análise torna o MENDEL mais efetivo para detectar comportamento malicioso e outras ameaças do que as soluções atuais do mercado.

As técnicas avançadas de exploração de dados do MENDEL asseguram que ele consiga processar muito mais funcionalidades de fluxo de dados do que soluções baseadas em protocolos NetFlow, em tempo real. Além disso, o MENDEL pode ampliar para 10Gbps em uma única configuração de sensor e coletor, e para até 40Gbps por coletor.

O MENDEL detecta ameaças escondidas

– Malware em celulares e aparelhos integrados
– Vazamento de dados com DNS, SSH, HTTP(S), etc
– Tráfego tunelado
– Anomalias de protocolo
– Ataques disfarçados
– Detecção de spam
– Preparação para roubo de dados e exfiltração
– Coleta de dados automatizada
– Roubo de dados
– Ataques de phishing

Melhor Monitoramento de Performance

O MENDEL fornece insights detalhados da performance do aplicativo, tanto do ponto de vista do usuário quanto do ponto de vista da rede. Seu design sem agente oferece a habilidade de monitorar cada uma de todas as transações através de múltiplos tipos de aplicativos. Essas transações são mostradas em uma ampla variedade de visualizações com classificação completa e capacidade de filtragem, dando às equipes dados detalhados para salvaguardar e otimizar processos corporativos críticos, bem como habilitar análise de causa raiz de maneira fácil e rápida, tudo em tempo real. Isso significa que as empresas veem não somente melhoria na segurança de rede, eficiência e visibilidade, mas também um retorno sobre investimento (ROI) apreciável.

Fácil de Usar Sem Causar Lentidão em Sua Rede

O MENDEL não é somente ferramentas, métodos e capacidades avançadas. Ele é instalado rapidamente, economiza tempo de administração e coleta dados sem causar lentidão na velocidade da rede. Os gerentes de TI amam o MENDEL porque:

- instalar e configurar configurações básicas no MENDEL leva 30 minutos. O MENDEL estuda a rede e a ferramenta IDS começa a reportar os resultados imediatamente. Dados acionáveis estão disponíveis após 7 dias e o ciclo de aprendizado completo para a ferramenta de Análise de Comportamento de Rede termina em 28 dias.
- O MENDEL torna o relatório e a compreensão das ameaças identificadas fácil, com filtragem e classificação, relatórios customizados e uma interface de web intuitiva para economizar tempo.
- O MENDEL monitora e visualiza, mas sem interromper, o tráfego de rede enquanto registra as informações em cada fluxo de dados. Isso significa que os usuários podem facilmente identificar cada fluxo em tempo real e descobrir quem usa certos serviços, nós de rede e banda larga. Acessa aplicativos e performance de rede e conduz análises com causa raiz, sem criar lentidão no tempo de resposta da rede.

A Análise de Comportamento de Rede se Encontra com o Aprendizado de Máquina

A ferramenta de Análise de Comportamento de Rede do MENDEL emprega análise matemática avançada no aprendizado de máquina, métodos de classificação supervisionada e não supervisionada, cluster e análises isoladas:

– Modelos de comportamento normal na rede, todas as subredes, hosts, serviços e fluxos de dados individuais
– Análise Bayesiana de funcionalidades transformadas
– Modelos de mistura probabilística (algoritmo de maximização de expectativas Gaussiano)
– Várias técnicas de racional ad hoc

Sobre o GREYCORTEX

O GREYCORTEX usa inteligência artificial avançada, aprendizado de máquina e métodos de exploração de dados pra ajudar as empresas a tornar as operações de TI seguras e confiáveis. O MENDEL, a solução de Análise de Tráfego de Rede GREYCORTEX, ajuda empresas, governos e o setor de infraestrutura crítica a proteger seu futuro detectando ciberameaças a dados sensíveis, redes, segredos de negócios e reputações que outros produtos de segurança de rede não tem.

A GREYCORTEX nomeou seu software como "MENDEL" em honra a Gregor Johan MENDEL, o pai da genética moderna, que fez suas descobertas na cidade de Brno, Morávia do Sul, República Tcheca, onde a GREYCORTEX tem sua sede.

ESET TECHNOLOGY ALLIANCE

A ESET Technology Alliance visa proteger de maneira mais efetiva os negócios com uma variedade de soluções de segurança de TI complementares. Fornecemos aos consumidores a melhor opção para ficar protegido em um ambiente de segurança dinâmico, combinando nossa tecnologia aprovada e confiável com outros produtos da melhor qualidade.

Informações Técnicas

Arquitetura	A arquitetura empresarial do MENDEL consiste em sensores e coletores. O sensores são usados para detectar ameaças conhecidas e entregar dados de tráfego de rede para a ferramenta de Análise de Comportamento de Rede no coletor. Os coletores são usados para transformar essas métricas em informação. Os sensores do MENDEL podem suportar até 10Gbps e os coletores podem manipular até 40Gbps. Grandes instalações através de muitas localidades são projetadas com um coletor que pode suportar 10 ou mais sensores (ambos físicos e virtuais).
Inputs	Fluxos de dados de rede a partir de tráfego espelhado (SPAN ou TAP) e reputações de IP como botnets conhecidos, fontes de spam, nós TOR, proxies e mais.
Outputs	Interface Gráfica do Usuário na Web e arquivos .pcap que podem ser baixados, relatórios customizados em .pdf e .doc (entregues via e-mail), exporta para o Gestor de Eventos e Informação de Segurança (SIEM) em CEF e IDEA.
Implementação	O GREYCORTEX MENDEL pode ser implementando como um aparelho de hardware ou, com algumas limitações, como um dispositivo virtual. Outras possibilidades incluem o MENDEL em um ambiente SECaaS, modelos de centros operacionais de segurança ou como um auditor de segurança único da rede do cliente.
Instalação	Instalação única: o MENDEL pode ser instalado como um sensor e coletor único de rede em um único aparelho. Instalação distribuída: o MENDEL pode ser instalado com diversos sensores e coletores compartilhando conhecimento sobre tráfego de rede e ameaças (para monitorar geograficamente localidades distantes e/ou processar altos volumes de tráfego).