Descrição Técnica da Sucuri

Descrição do Produto e do Serviço

ÍNDICE

DESCRIÇÃO TÉCNICA DA SUCURI

DESCRIÇÃO DO PRODUTO/SERVIÇO

EXPOSIÇÕES

DESCRIÇÃO DA SUCURI

DESCRIÇÃO DA EMPRESA

A Sucuri é uma empresa de segurança reconhecida mundialmente, especializada no fornecimento de segurança abrangente para proprietários de sites. A empresa radicada nos Estados Unidos foi fundada em 2010 e mantém uma presença global. A Sucuri conta com funcionários em mais de 23 países distribuídos pelos principais continentes para assegurar um suporte acessível 24/7/365. A empresa fornece serviços de segurança de sites para mais de 45.000 clientes pagantes em todo o mundo, limpa e conserta mais de 500 sites infectados por dia, monitora mais de 400.000 sites e lida com mais de 16 bilhões de visualizações de páginas únicas por mês.

Toda a tecnologia que a Sucuri possui é construída por nossa equipe de engenheiros de segurança e pesquisadores. Nossa tecnologia foi desenvolvida para atender às crescentes ameaças de segurança online à medida que surgem. Nossa equipe dedica-se a garantir a confidencialidade, integridade e disponibilidade de cada site dentro da rede Sucuri.

A Sucuri importa-se com cada site e trata cada um deles como se fosse o seu próprio site. A solução que oferece é construída sobre três principais pilares - Proteção | Detecção | Resposta. Adota-se uma abordagem de defesa em profundidade para a segurança de sites, na qual emprega várias camadas de segurança para fornecer a solução mais abrangente disponível. Trata-se de uma combinação de pessoas, processos e tecnologia para cuidar dos sites e mitigar ataques da maneira mais rápida e eficiente possível.

Esses pilares permitem à Sucuri implantar uma solução defensiva para impedir que os atacantes abusem os componentes do seu site. Essa solução de prevenção é acoplada a um mecanismo de verificação contínuo destinado a identificar quaisquer elementos nocivos que podem revelar-se indicadores de um compromisso em potencial. Finalmente, a Sucuri oferece uma equipe profissional de Resposta a Incidentes (IRT) para quando os ataques são bem-sucedidos, dando às empresas a tranquilidade que precisam com atenção obsessiva às ameaças atuais e emergentes dentro do domínio de segurança de sites.

PESSOAS, PROCESSOS E TECNOLOGIA

Não há soluções do tipo turnkey para a segurança. Trata-se de uma combinação de pessoas, processos e tecnologia que ajuda a criar uma abordagem flexível e escalável para a segurança de qualquer organização. Os produtos da Sucuri são projetados para reduzir o risco de violação de marcas através da implantação de mecanismos tanto pró-ativos quanto reativos, abordando cada um dos elementos acima descritos. A solução da Sucuri é uma oferta complementar que se acopla aos controles de segurança existentes de uma organização, satisfazendo uma série de requisitos de governança, ao mesmo tempo que permite que as equipes de segurança continuem a se concentrar em suas principais responsabilidades.

DESCRIÇÃO DO PRODUTO/SERVIÇO

A Sucuri fornece uma solução de segurança completa para sites, chamada de Pacote de Segurança de Sites (Website Security Stack - WSS). Esse pacote é composto por quatro plataformas centrais projetadas para fornecer às organizações uma solução holística de segurança para suas propriedades de sites.

PLATAFORMA DE MONITORAMENTO

A plataforma de monitoramento é um sistema de detecção de intrusão (Intrusion Detection System - IDS) de software como um serviço (Software as a Service SaaS) baseado na nuvem. Essa plataforma foi construída sobre o conceito de um sistema de monitoramento de integridade baseado na rede (Network-Based Integrity Monitoring System - NBIMS). Trata-se de um mecanismo de escaneio remoto e local (server-side) contínuo, que proporciona visibilidade sobre o estado de segurança de um site quase em tempo real.

Desenvolveu-se com o objetivo de detectar múltiplos indicadores de compromisso (Indicators of Compromise - IoC), que incluem, mas não se limitam a:

- Distribuição de Malware
- Incidentes de Notificações (Blacklisting)
- Spam de SEO
- Certificados SSL
- Páginas de Phishing Lure
- Páginas de Phishing Lure
- Mudanças no DNS

A plataforma de monitoramento inclui um mecanismo de alerta no caso em que um IoC é detectado. Então o Grupo de Operações de Segurança (Security Operations Group - SOG) é notificado e toma medidas imediatamente pelo IRT de segurança. A plataforma não requer instalação ou mudanças na aplicação. Todos os sites são adicionados e configurados via o painel Sucuri. Para ativar o escaneio do lado do servidor, é necessário ter um agente PHP no root do domínio principal.

Observação: Os eventos de monitoramento podem ser emitidos para o sistema de gerenciamento de informação e eventos (System Information and Event Management - SIEM) da empresa contratante mediante solicitação.

PLATAFORMA DE PROTEÇÃO

A plataforma de proteção ("Sucuri Firewall") é um sistema de prevenção de intrusão (IPS) Website Application Firewall (WAF) SaaS na nuvem para sites. Funciona como um proxy reverso, interceptando e fiscalizando todos os pedidos de Hypertext Transfer Protocol/Secure (HTTP/HTTPS) para um site, filtrando todas as solicitações maliciosas na rede Sucuri antes que cheguem ao seu servidor. O Firewall Sucuri inclui motores tanto de Patching Virtual quanto de Hardening Virtual, que permitem a mitigação de ameaças em tempo real sem impactar o site.

O Firewall Sucuri é construído sobre uma rede de distribuição de conteúdo (Content Distribution Network - CDN), que fornece recursos de otimização de desempenho para um site. O CDN utiliza uma abordagem de propriedade (proprietary approach) para armazenamento em cache dinâmico e conteúdo estático em todos os nós da rede para garantir o melhor desempenho em todo o mundo.

Além disso, o Firewall Sucuri oferece serviços completos para Domain Name Server (DNS).

O Firewall Sucuri é executado em uma rede Anycast distribuída globalmente (Globally Distributed Anycast Network - GDAN), construída e administrada pela equipe da Sucuri. A configuração GDAN permite alta disponibilidade e redundância em caso de falhas na rede. A Sucuri atualmente administra seis pontos de presença (Points of Presence - PoP).

Pontos de Presença

San Jose, CA
Dallas, Texas
District of Columbia (DC)
Londres, Reino Unido
Frankfurt, Alemanha
Tóquio, Japão

A plataforma é suportada pelo centro de operações de segurança da Sucuri (Sucuri Security Operations Center - SOC), que fornece monitoramento 24/7/365 e resposta a todos os ataques. Algumas das características que a plataforma de proteção oferece a proprietários de sites incluem:

- Mitigação de Ataques Distribuídos de Negação de Serviço (Distributed Denial of Service - DDoS)
- Prevenção de Tentativa de Exploração de Vulnerabilidades (SQLi, XSS, RFI / LFI, etc...)
- Proteção Contra os Top 10 do OWASP (Open Web Application Security Project) e muito mais
- Ataques de Controle ao Acesso (tentativas de Força Bruta)
- Otimização de Performance

A plataforma não requer instalação ou mudanças na aplicação. Tudo é feito via DNS, através da adição de um A record ou através da mudança para servidores de nomes (name servers) da Sucuri.

PLATAFORMA DE RESPOSTA

A plataforma de resposta oferece uma equipe profissional de respostas a incidentes de segurança (Security Incident Response Team - RT). Essa equipe está disponível para responder a todos os incidentes de segurança relacionados com o site, incluindo questões identificadas pela Sucuri. A equipe é altamente treinada e capaz de mitigar todas as infecções de sites e todas as questões relacionadas com malware.

Esta plataforma existe devido à natureza complexa da segurança de sites. Intrusões ocorrem por muitas razões. Embora nossas várias tecnologias são empregadas para ajudar na prevenção de tais compromissos, existem coisas além do controle da Sucuri. Os exemplos incluem, gerenciamento ou criação de senhas de usuário fracas, configurações de segurança pobres e outras questões semelhantes relativas ao ambiente.

Devido ao vetor de ataque expandido fora do controle da Sucuri, a plataforma de resposta foi projetada para fornecer às organizações uma equipe complementar para auxiliar na identificação e na erradicação de invasões bem sucedidas. A plataforma inclui a análise das suas causas, auxiliando na aplicação de patches e na restauração do ambiente à ordem operacional.

A Plataforma de Resposta inclui, mas não se limita a:

- Infecções de malware no nível do servidor
- Infecções de Malware de Sites
- Injeções de Spam de SEO
- Redirecionamentos de Usuários Maliciosos
- Defacements de Sites
- Remoção de Todos os Backdoors
- Remoção de Notificações de Listas Negras de Sites

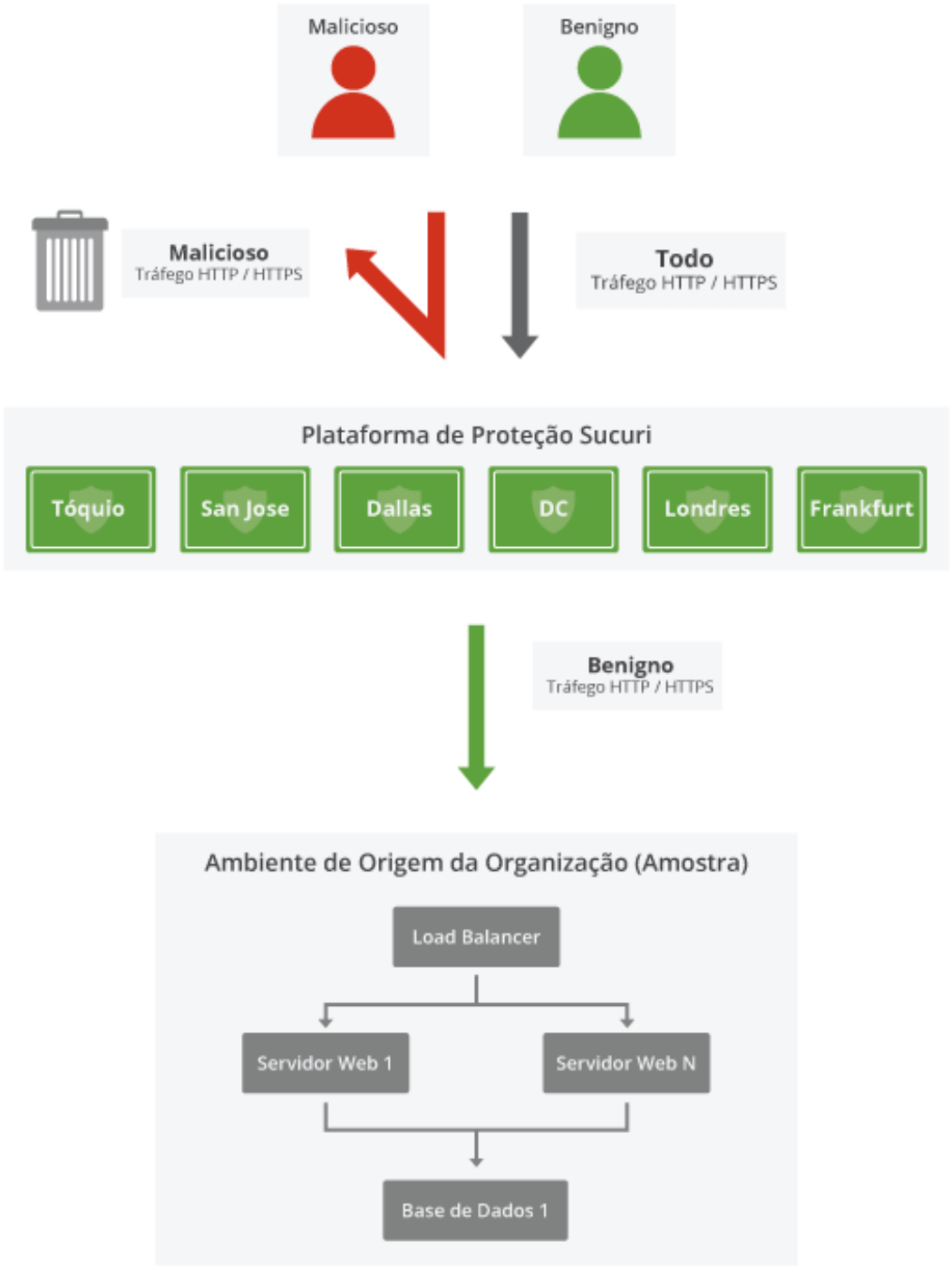
A plataforma não requer nenhuma instalação ou mudança na aplicação, mas requer acesso direto ao web server / application via FTP/SFTP ou SSH.

PLATAFORMA DE BACKUP

A plataforma de backup fornece a uma organização operações contínuas no caso de uma emergência. A plataforma inclui armazenamento de todos os arquivos de sites e bancos de dados em um local remoto na rede da Sucuri. No caso de um problema, os backups estarão disponíveis para a organização.

A plataforma não requer instalação ou mudança na aplicação. Todos os sites são adicionados e configurados através do painel Sucuri.

EXIBIÇÃO A: DIAGRAMA DE REDE HOLÍSTICO (PLATAFORMA DE PROTEÇÃO)



EXIBIÇÃO B: MITIGAÇÃO DE DDOS

A mitigação de Ataques Distribuídos de Negação de Serviço (DDoS) é uma característica fundamental que o Firewall Sucuri oferece a seus clientes.

ATAQUES DDOS BASEADOS NA REDE (ATAQUES VOLUMÉTRICOS)

A abordagem da Sucuri para mitigar ataques baseados na rede inclui investimento em recursos em todos os locais PoP. A mitigação de DDoS é desenvolvida sobre uma rede anycast, que permite a distribuição de todo o tráfego de entrada (inbound traffic) do outro lado da rede; e explicitamente bloqueia todo o tráfego não-HTTP/HTTPS. A capacidade da rede atual é superior a 250 gigabytes por segundo (GPS). Cada PoP tem vários ports de 10G e 40G de diferentes provedores, todos projetados para absorver e escalar no caso de grandes pedidos de tráfego de entrada e ataques.

ATAQUES DDOS BASEADOS NA APLICAÇÃO (APPLICATION-BASED DDOS)

Esses ataques são projetados para interromper a disponibilidade de um site, atacando os recursos do servidor diretamente. Ao inundar um servidor com pedidos, um atacante é capaz de consumir recursos do servidor local até que o servidor torne-se incapaz de responder a solicitações legítimas. Nesses casos, o site não responderá. A ordem de grandeza é muito diferente. Esses ataques são medidos em solicitações por segundo (Requests Per Second - RPS) e podem começar com 100/200 solicitações por segundo para muitos servidores web.

A abordagem da Sucuri para mitigar esses ataques é sua tecnologia: parte humana e parte inteligência artificial. A plataforma emprega tecnologia que permite que a equipe e o motor analisem os pedidos em toda a rede, o que nos permite separar com precisão os pedidos maliciosos dos benignos. Além disso, na rede Sucuri, os sites podem suportar 300k + RPS por site.

EXIBIÇÃO C: PREVENÇÃO DE EXPLOIT

A prevenção de tentativas de exploits remotas que tentam abusar vulnerabilidades de software, tais como as identificadas pelo projeto de segurança de aplicativos Open Web Application Security Project (OWASP), é uma característica crítica da plataforma de proteção.

Esses ataques podem incluir tentativas de exploits contra o site diretamente e alvos como injeções (SLQi, XSS, etc.), execução remota de código (remote code execution- RCE), erro de configuração de segurança, inclusão remota de arquivos (remote file inclusion - RFI) e muitas outras vulnerabilidades.

A plataforma de proteção usa uma abordagem multinível de propriedade para identificar e remover solicitações de aplicativos maliciosos.

Nível 1	Descrevendo o Aplicativo	O primeiro nível utiliza uma abordagem de recusar todos e um modelo de permissões (whitelist), no qual todos os pedidos que não se encaixam no perfil de um aplicativo são bloqueados explicitamente desde o começo. Esse perfil é construído dinamicamente na tecnologia / plataforma que um site usa. Serviços de terceiros não são usados.
Nível 2	Motor de Lista Negra	O segundo nível usa uma lista negra de modelo de bloqueio de assinatura construído pela equipe Sucuri para contabilizar quaisquer outliers ou ameaças em evolução. Serviços de terceiros não são usados.
Nível 3	Motor de Correlação	O terceiro nível analisa todos os pedidos em toda a rede Sucuri para definir o perfil de comportamento do invasor e aplicá-lo globalmente para todos os sites protegidos pela Sucuri. Este é um mecanismo de aprendizagem que aplica pró-ativamente atualizações para a rede assim que o cenário de ameaças evolui.

Além disso, a plataforma de proteção emprega um Patching Virtual e uma abordagem de Hardening Virtual a sua estratégia de mitigação:

PARCHE VIRTUAL	Com patching virtual, a equipe Sucuri é capaz de responder rapidamente às ameaças emergentes sem impactar os sites. Todas as correções são aplicadas no âmbito da Sucuri. O patching virtual é especialmente eficaz para organizações maiores que possuem governança estrita de segurança sobre quando e como patches podem ser aplicados em um ambiente de produção. Regras personalizadas também podem ser aplicadas.
HARDENING VIRTUAL	Com o hardening virtual, a equipe da Sucuri é capaz de aplicar patches agnósticos a vulnerabilidades em um site. O hardening pode ser específico para a plataforma (WordPress, Joomla !, Drupal, etc) ou mais genérico para um servidor web (ou seja Apache /IIS).

A eficácia da plataforma de proteção é limitada a sua capacidade de ver todo o tráfego de entrada. A técnica de evasão mais comum é o ataque direto ao servidor de origem. Todo o tráfego direto para o servidor de origem deve estar limitado à rede da Sucuri.

EXIBIÇÃO D: PREVENÇÃO DE EXPLOIT

A plataforma de proteção é capaz de mitigar ataques interceptando todo o tráfego de entrada e realizando análise em tempo real de todos os pedidos dos protocolos HTTP / HTTPS (os pedidos da camada 7). O tráfego que é criptografado (utiliza HTTPS) também deve ser analisado.

Para alcançar esse objetivo, o end-point deve encerrar-se na rede Sucuri. A plataforma de proteção deve interceptar e analisar todo o tráfego para ser eficaz. Toda a análise é feita na memória, em tempo real - **não há armazenamento dos pacotes de solicitação**. Os únicos dados armazenados são os meta-dados de pedidos, na forma de logs de acesso web.

As organizações têm várias opções relativas a SSL:

OPÇÃO 1	Uso de certificados Comodo DV gerados pela Sucuri.
OPÇÃO 2	Uso de um certificado LetsEncrypt Gratuito gerado pela Sucuri.
OPÇÃO 3	Uso de um certificado customizado gerado pela organização.
OPÇÃO 4	A Sucuri fornece um CSR para que as organizações gerem um certificado via seu próprio CA.

EXIBIÇÃO E: INSTALAÇÃO E CONFIGURAÇÃO

Cada plataforma tem seu próprio requisito de configuração e implantação, mas cada uma delas foi projetada para ser simples e requer baixa sobrecarga e engajamento. Os requisitos são:

PLATAFORMA DE PROTEÇÃO	Não requer instalação. Uma mudança no A-record via DNS. Também suporta gerenciamento de DNS total via mudança de nameservers. A hora de ir ao vivo depende do valor Time to Live (TTL).
PLATAFORMA DE MONITORAMENTO	Não requer instalação. Escaneio Remoto: Os domínios são carregados para o painel da Sucuri via API ou interface do painel. Escaneio do servidor: agentes de domínio PHP são carregados no root de cada diretório do site no servidor web. ** Requer acesso SFTP/FTP/SSH para carregar arquivos. A organização pode optar por carregar arquivos por conta própria.
PLATAFORMA DE RESPOSTA	Não requer instalação. No caso de um incidente, todos os eventos são manipulados e geridos através do sistema de tickets da Sucuri. O suporte e acordo de nível de serviço (Service Level Agreement - SLA) está no seu contrato. Requer acesso ao servidor via SFTP/FTP/SSH. As alterações podem ser negociadas no seu contrato.
PLATAFORMA DE BACKUP	Não requer instalação. O suporte e acordo de nível de serviço (Service Level Agreement - SLA) está no seu contrato.

Alguns contratos incluem suporte ao cliente e serviços de integração. Leia o seu contrato ou procure o gerente da sua conta para fins específicos relativos à implantação de cada plataforma e responsabilidades associadas.

EXIBIÇÃO F: OTIMIZAÇÃO DE PERFORMANCE E CACHE

Todo o conteúdo estático é armazenado em cache quando possível. Isso permite respostas mais rápidas às solicitações (500 ms vs 10 ms) e escalas (50 usuários simultâneos vs 200k usuários simultâneos). As plataformas padrão conhecidas, como Wordpress, Joomla!, Drupal e outras aplicações CMS semelhantes usam cookies. Sabemos disso e explicamos como funciona nossa lógica de cache.

O recurso de cache funciona através da construção de uma chave de cache. Cada pedido que corresponde a chave recebe a mesma página. A chave de cache é composta pelo HTTP ou HTTPS, domínio, solicitação URI, e agente de usuário normalizado (ou seja, aparelho móvel, desktop, tablet ou RSS bot). Isso significa que os usuários de diferentes plataformas (desktop vs aparelho móvel) não verão o mesmo conteúdo.

OPÇÕES DE CACHE

A plataforma oferece quatro opções de cache:

OPÇÃO	DESCRIÇÃO DA OPÇÃO	TEMPO
Ativado (Recomendado)	Armazena cache do site todo e somente elimina o cache em poucas horas.	All - 3 hrs +
Cache Mínimo	Armazena cache do site todo e elimina o cache em poucos minutos.	200 - 8 m 404 - 2 m 302 - 15 m 301 - 15 m
Cache do Site (Cabeçalhos do Site)	Armazena cache do conteúdo estático e respeita os cabeçalhos do site.	200 - 180 m 404 - 10 m 302 - 180 m 301 - 180 m
Desabilitado (Usar com cuidado)	Somente armazena cache do conteúdo estático, como imagens, .css, .js, .pdf, .txt, .mp3 e algumas outras extensões.	200 - 1 m 404 - 1 m 302 - 10m 301 - 10m

ELIMINANDO CACHE

A eliminação do cache é uma característica crítica da plataforma. Permitimos que o cache seja eliminado através do Painel Sucuri ou API WAF. Uma vez iniciado, o cache propaga-se através da rede e limpa todos nós dentro de segundos.

EXIBIÇÃO G: SEGURANÇA DE INFRAESTRUTURA E COMPLIANCE

Cada centro de dados que opera a partir das necessidades atende ou excede todas as normas e regulamentos de compliance:

REGULAÇÕES DE COMPLIANCE

SSAE16 COMPLIANCE
OHSAS 18001:2007
PCIDSS PAYMENT CARD INDUSTRY STANDARD
ISO CERTIFICATION
ISO 9001:2008
ISO 14001:2004
ISO / IEC 27001:2005 AND 27001:2013
ISO 50001:2011

INFRAESTRUTURA DA REDE

A rede da Sucuri consiste em múltiplos provedores de trânsito em cada local que é utilizado para o roteamento primário de tráfego, roteamento de tráfego interno e redundância.

A utilização de uma rede compartilhada com uma terminação primária e secundária para cada conexão previne que um ponto falhe.

OPERAÇÕES

- Dispositivo diário de escaneio de vulnerabilidade realizado internamente
- Escaneio de vulnerabilidade diária e escaneio de compliance realizada por terceiros
- Testes de penetração internos e testes de terceiros
- Documentação, práticas e educação contínua de funcionários
- Procedimentos de gestão e modificação de Firewall
- Classificação de dados e de propriedade
- Gerenciamento de incidentes
- BCP (Business Continuity Plan) & DRP (Disaster Recovery Plan)
- Monitoramento de log e revisão de rede contínua

GERENCIAMENTO E RECURSOS HUMANOS

- Treinamento de conscientização de segurança obrigatório e avaliação para cada funcionário
- Práticas de acesso de menor privilégio em todas equipes
- Acordos de não divulgação e confidencialidade
- Verificação de background e avaliação de habilidades
- Gestão ativa em todos os aspectos da comunidade de segurança
- Mantenha-se atualizado no mundo cibernético em constante mudança

sucuri.net | 1.888.873.0817 | sales@sucuri.net