Higiene da Segurança:
A linha de frente da segurança

Versão 1.3
Publicado em: maio de 2021

Securosis, L.L.C. 515 E. Carefree Highway Suite, 766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Observação do autor

O conteúdo deste relatório foi desenvolvido independentemente de quaisquer patrocinadores. Ele é baseado no material postado originalmente no blog da Securosis, mas foi aprimorado, revisado e editado profissionalmente.

Um agradecimento especial a Chris Pepper pela edição e suporte ao conteúdo.

Higiene da Segurança

Índice

Por que a higiene da segurança é essencial para a proteção

Depois de muitas décadas como profissionais de segurança, é triste continuar vendo os mesmos problemas e erros. Parece que estamos presos em um Feitiço do Tempo de hacking. Levante-se, conserte os erros cometidos por usuários ou administradores, lide com um novo ataque e preencha relatórios de conformidade, apenas para ter que fazer tudo de novo no dia seguinte. Claro, vivemos em um mundo assimétrico quando se trata de segurança.
Os invasores só precisam acertar uma vez para conseguir entrar no seu ambiente. Os defensores só precisam estar errados uma vez - um fato que os invasores exploram para ganhar áreas de entrada, brechas, significativas. Não é justo, mas ninguém disse que a vida era justa.

O conselho mais básico que damos a qualquer pessoa que esteja criando um programa de segurança é certificar-se de que você lida bem com os fundamentos. Você se lembra dos fundamentos de segurança, certo? Visibilidade para todos os ativos. Mantenha uma forte configuração e postura de segurança para esses ativos. Corrija os sistemas de forma eficiente e eficaz quando os fornecedores emitirem patches de atualizações. A maioria dos praticantes concorda com os fundamentos somente para, em seguida, passar o dia todo tentando descobrir como funciona o malware mais recente dos adversários, perdendo alguns dias caçando ameaças em seu ambiente ou simplesmente supondo que isso não acontecerá com eles. Sabe, coisas divertidas. Os fundamentos são simplesmente... chatos.

O conselho mais básico que damos a qualquer pessoa que esteja criando um programa de segurança é certificar-se de que você lida bem com os fundamentos.

Mas o fato é que os fundamentos funcionam. Talvez não para todos os ataques, mas para muitos deles, e é assim que eles se tornaram fundamentais em primeiro lugar. Vamos lembrar você disso neste artigo. Não podemos eliminar todos os riscos, mas seria uma pena se não estivéssemos tornando mais difícil para os adversários encontrarem uma brecha para controlar o seu ambiente. Trata-se de fechar os caminhos de menor resistência, garantindo que

oponentes indignos, como *script kiddies* (jovens que fazem scripts) e hackers comuns, não o derrubem. Se pudermos fazer os adversários se esforçarem para comprometer seu ambiente, eles provavelmente cometerão um erro, acionando a detecção ou deixando para trás evidências para uma investigação futura.

Muitos dias ruins

Conforme revisamos as listas de milhares de violações ao longo dos anos, vimos que algumas resultaram de configurações incorretas, da não correção de vulnerabilidades conhecidas ou falharam em não instalar os patches de fornecedores. Vamos examinar três violações específicas para descobrir o lado negativo da falta de higiene de segurança.

- **Microsoft Exchange:** A violação de destaque mais recente envolveu um ataque a servidores do Exchange instalados localmente, on-premises, e resultou em invasores obtendo acesso total aos servidores. Seguiu-se uma série de ataques de ransomware, destacando a necessidade de manter esses componentes críticos atualizados.

- **Equifax:** A empresa deixou os servidores, voltados para a Internet, vulneráveis ao ataque do Apache Struts, por não ter aplicado os patches de correção, permitindo a execução remota de código. O patch estava disponível no Apache, mas a empresa não o aplicou a todos os sistemas. Pior ainda, sua equipe de operações verificou se havia sistemas sem patch de correção e não encontrou nenhum, embora ainda tivessem sistemas vulneráveis. Foi uma falha de higiene típica, resultando em centenas de milhões de identidades de usuários roubadas. A Equifax acabou pagando centenas de milhões de dólares para lidar com suas responsabilidades. Foi um péssimo dia.

- **Citrix:** Quando um componente de tecnologia importante é atualizado, você deve aplicar o patch. Não é como se os invasores não fizessem a engenharia reversa dos patches para encontrar as vulnerabilidades. Essa situação foi particularmente problemática quando a Citrix foi hackeada no início de 2020 porque os invasores puderam realizar pesquisas automatizadas para encontrar dispositivos vulneráveis. Então, foi isso que eles fizeram. As mitigações iniciais sugeridas pela Citrix, em vez de lançar um patch, não eram confiáveis nem amplamente implementadas em sua base de clientes, deixando muitas organizações expostas. Ao mesmo tempo, o código de *exploit* amplamente distribuído facilitou essa exploração. Depois que a Citrix lançou os patches, os clientes os adotaram rapidamente e basicamente encerraram o ataque. O processo de patching funciona, mas apenas se você realmente o aplicar.

Não gostamos de provocar empresas que sofreram violações, mas precisamos aprender com seus erros. E a higiene da infraestrutura está cada vez mais complicada. O ataque à SolarWinds no final de 2020 foi um exemplo em que, mesmo fazendo a coisa certa e corrigindo a ferramenta com um patch, acabou dando acesso aos invasores. Se você olhar para essa situação isoladamente, pode perguntar: "Por que se preocupar com o processo de patching?"

Essa pergunta indica que você aprendeu a lição errada. Volte alguns parágrafos, onde diz: “Você não pode eliminar todos os riscos”. Ataques à cadeia de suprimentos acontecem e, francamente, você não pode fazer muito a respeito além de focar na detecção e no monitoramento. Mas não corrigir um componente com patches abre seus sistemas para qualquer pessoa com o *exploit*.

Não é uma opção

Depois de todas as desvantagens acima, digamos que você ainda resista a praticar uma boa higiene de infraestrutura. Não se baseie em nós. Escute o seu auditor, que irá encontrar (e relatar) todos os tipos de deficiências se você não puder manter as coisas fortemente configuradas e corrigidas com patches. Vamos destacar alguns mandatos regulatórios que exigem correção via patches.

- **PCI:** Os requisitos 2, 6 e 11 mencionam patches.
- **ISO 27001:** O controle A.12.6.1 lida com a correção de vulnerabilidades (patching).
- **Artigo 25 da GDPR:** Proteção de dados por design e por padrão e Artigo 32: Segurança de processamento alude à necessidade de ter sistemas que protejam os dados do cliente e, se os sistemas não tiverem uma boa higiene, eles não podem proteger os dados do cliente.

> Não gostamos de provocar empresas que sofreram violações, mas precisamos aprender com seus erros.

- **NIST SP 800-53 R3:** Gerenciamento de Configuração (CM-Configuration Management), Avaliação de Risco (RA-Risk Assessment) e Integridade de Sistemas e Informação (SI-System and Information Integrity) destacam a necessidade de aplicar patches na infraestrutura.

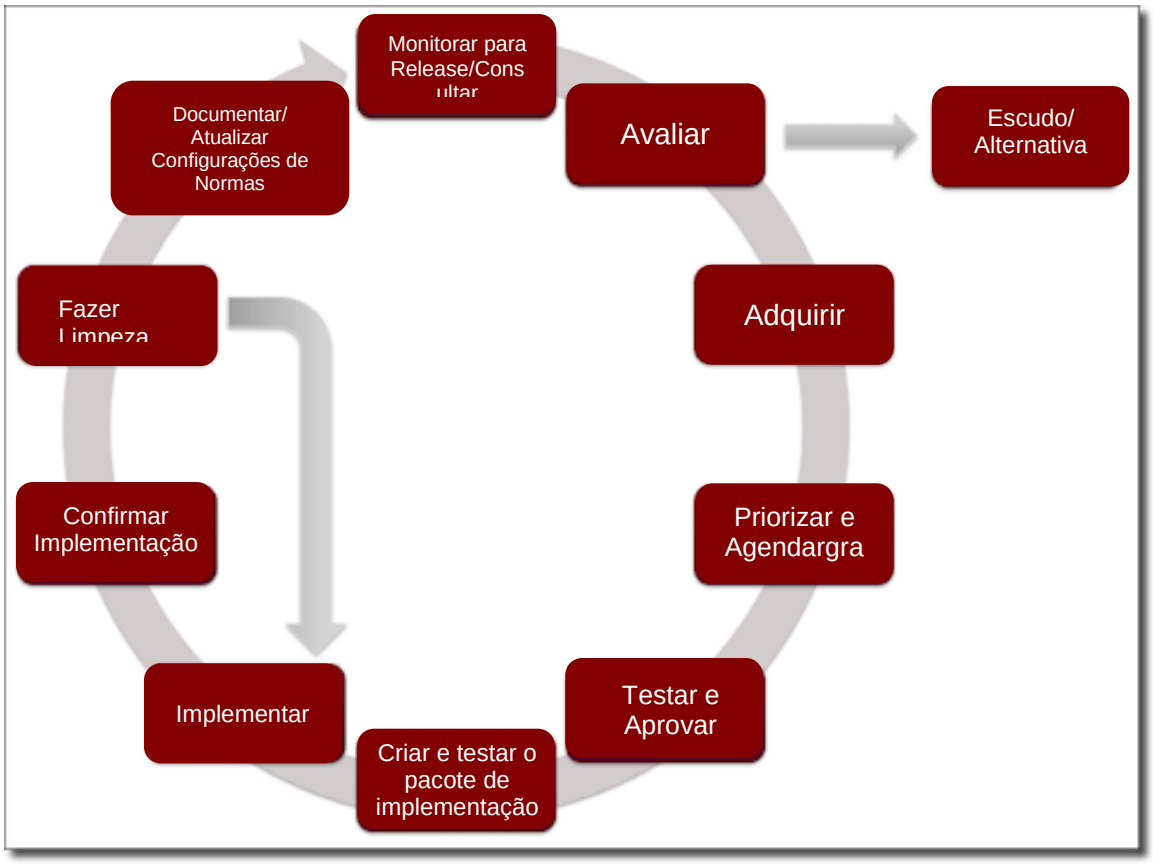
Você não tem opção, não é?

Corrigindo vulnerabilidades

Conforme mencionado acima, o conselho mais básico que podemos dar sobre segurança é aplicar bem os fundamentos. Isso não o isola de adversários determinados e bem financiados, mas eliminará os caminhos de menor resistência que a maioria dos invasores toma.

Como se isso não bastasse, agora você tem uma margem de erro essencialmente zero porque os invasores automatizaram o reconhecimento de muitos ataques. Assim, se você deixar algo exposto, eles o encontrarão. Eles têm bots e scripts procurando constantemente por links fracos.

Dito isso, você não está lendo este artigo para ficar ouvindo sobre os desafios da segurança, está? Vamos mudar nosso foco para como corrigir problemas.



Corrija rápido e completamente

Os próprios fornecedores lançam atualizações e patches para vulnerabilidades descobertas em seus produtos. Os clientes então aplicam os patches em seus sistemas para que eles se mantenham atualizados e seguros. Temos feito correções, como indústria, há muito tempo. E nós, da Securosis, pesquisamos sobre patches há quase tanto tempo quanto. Sinta-se à vontade para entrar na máquina do tempo e verificar nosso trabalho inicial sobre correção no Projeto Quant original.

A imagem acima mostra o processo de patching detalhado que definimos em 2009. Você precisa de um processo confiável e consistente para aplicar patches de forma eficaz. Iremos apontar especificamente para a importância da etapa de Teste e Aprovação devido ao grande risco de implementar um patch que desative um componente.

No entanto, trabalhar com um processo de patching robusto pode levar de alguns dias a um mês. Muitas empresas maiores esperam ter patches implantados dentro de um mês após o release. Mas, na realidade, algumas semanas podem ser muito tempo para aplicar um patch importante para um problema que está sendo explorado ativamente. Você precisa de um processo de alta prioridade para aplicação de patches que tratam de vulnerabilidades de risco muito alto. Um requisito essencial é estabelecer e concordar com os critérios para acionar o esforço de patches de correção de alta prioridade (fora do ciclo) e quais partes do processo normal de patching você irá ignorar.

Como alternativa, você pode usar um patch virtual temporário, que tenta proteger contra a exploração de uma vulnerabilidade não corrigida com base na assinatura do ataque. Isso só é possível se o ataque tiver um padrão identificável estabelecido para construir a assinatura e, mesmo assim, as assinaturas fornecerem uma proteção inadequada da superfície de ataque. Pelo lado positivo, a implementação de patches virtuais pode ser rápida. No entanto, dado que as informações sobre novas vulnerabilidades de alto risco são muitas vezes vagas, é difícil, senão impossível, garantir que qualquer solução alternativa foi digitada corretamente no padrão identificável ideal ou que o ataque não se transformará para alterar sua assinatura . Tudo se resume a quão perfeitamente o fornecedor do patch virtual temporário pode identificar o padrão. Se isso falhar, uma grande porcentagem de exploits ainda pode passar. E se o fornecedor ultrapassar o padrão, você irá prejudicar seu aplicativo bloqueando transações legítimas. Além disso, você ainda precisa executar vários testes para garantir que nada seja interrompido e, de qualquer forma, você pode não economizar muito tempo com o patch. Há muito a ser considerado, o que significa riscos reais.

Uma das outras desvantagens dos patches virtuais temporários é que todo o tráfego destinado ao componente vulnerável precisa passar pelo ponto de inspeção ou lógica de mitigação. Se o tráfego puder atingir o componente diretamente, o patch virtual temporário será inútil. Por exemplo, se um patch virtual é implementado em um dispositivo de segurança de perímetro para proteger um banco de dados, um usuário interno com acesso direto ao banco pode contornar o patch para explorar o banco de dados sem ele. Neste contexto, alguém de dentro pode simplesmente ser um adversário com uma brecha dentro do perímetro ou com um conjunto de

credenciais de administrador.

Você também precisa entender claramente o que fazer depois que um padrão de ataque for reconhecido. Se você derrubar a conexão inteira, isso poderá impactar muitos outros usuários que usam o mesmo pool de conexão ou afetar o comportamento da aplicação de diferentes maneiras imprevistas.

Para vulnerabilidades de alta prioridade que você não pode corrigir com patch imediatamente, seja porque o patch ainda não está disponível ou devido ao tempo de inatividade ou outros desafios de manutenção, um patch virtual temporário pode fornecer uma alternativa importante de curto prazo. Mas lembre-se de que você não está consertando o componente - você o está escondendo atrás do patch virtual. Com 30 anos de experiência em nosso currículo, podemos dizer com certeza que esperar que um invasor não encontre seus sistemas vulneráveis não é um caminho para o sucesso.

Dada a facilidade com que os adversários podem alterar sua assinatura de ataque para evitar a detecção e patches virtuais temporários, o fato de que é impossível chegar a uma assinatura de detecção perfeita e a dificuldade em garantir que todo o tráfego passe por um ponto de inspeção, implementar um patch do fornecedor é a única solução de longo prazo. Falando em soluções de longo prazo...

Aproveite ao máximo as responsabilidades compartilhadas

Uma das coisas mais interessantes sobre a revolução da nuvem é a ideia de substituir alguns componentes da infraestrutura por serviços de plataforma (PaaS). Já mencionamos isso acima, então vamos nos aprofundar um pouco mais em como a responsabilidade compartilhada pode melhorar a higiene da infraestrutura. Primeiro, a responsabilidade compartilhada é fundamental para a computação em nuvem; cada provedor de nuvem assume responsabilidades específicas. O consumidor da nuvem (você) tem responsabilidades de segurança inerentes. A combinação disso é a responsabilidade compartilhada.

A divisão específica de responsabilidade depende do serviço e do modelo de entrega (SaaS ou PaaS), mas basta dizer que adotar um serviço PaaS para um componente de infraestrutura tira você das operações desse componente. Você não precisa se preocupar com dimensionamento ou manutenção, incluindo patches de segurança. Tenho certeza de que você não sentirá falta de trabalhar até tarde e nos fins de semana, longe da sua família, executando hot fixes em servidores e bancos de dados.

Em última análise, transferir alguma responsabilidade para um provedor de serviços reduz tanto o ataque quanto a área de superfície operacional, e isso é uma coisa boa.
A longo prazo, usar os serviços PaaS estrategicamente é uma das melhores maneiras de reduzir o risco do stack de tecnologia.

Em última análise, transferir alguma responsabilidade para um provedor de serviços reduz tanto o ataque quanto a área de superfície operacional, e isso é uma coisa boa. A longo prazo, usar os serviços PaaS estrategicamente é uma das melhores maneiras de reduzir o risco do stack de tecnologia. De fato, um provedor de serviços ainda pode cometer um erro, mas o risco é consideravelmente menor. Os provedores de serviços precisam se preocupar com sua reputação e valor de marca e dedicam recursos consideráveis para lidar com vulnerabilidades e manter os clientes seguros.

A cadeia de suprimentos

Se há algo que aprendemos com a recente violação da SolarWinds e o ataque à Target (de 2013), que começou com uma violação de um contratado terceirizado, é que as responsabilidades de higiene não terminam nos limites do seu ambiente. Conforme mencionado acima, você pode não ser responsável por manter os componentes de infraestrutura de seus fornecedores e parceiros, mas é responsável por como seus pontos fracos podem afetar seu ambiente.

Espera, o quê? Vamos esclarecer um pouco. Se um parceiro de negócios externo ficar comprometido e o invasor entrar em seu ambiente e começar a causar estragos, adivinha só... Você é responsável por isso. Claro, você pode argumentar que o parceiro era responsável por proteger o ambiente e falhou. Mas isso não vai ajudar quando você estiver na frente do comitê de auditoria da sua organização explicando por que seu programa de risco de terceiros não era bom o suficiente.

Assim como queremos aproveitar o modelo de responsabilidade compartilhada para obter ajuda operacional e reduzir a superfície de ataque, você precisa empregar recursos adicionais no gerenciamento de risco para entender a importância do que está em risco para escolher uma abordagem de remediação apropriada.

Sucesso e Consistência

Devemos reiterar que nenhuma das abordagens à higiene da segurança da infraestrutura é mutuamente exclusiva. Um patch elimina a vulnerabilidade em um componente, mas há casos em que um patch virtual temporário pode reduzir temporariamente um risco imediato. A melhor solução de longo prazo sempre envolverá patches fornecidos diretamente pelo fornecedor e pode incluir a mudança para um serviço PaaS. Você precisará descobrir a melhor abordagem caso a caso, equilibrando risco, disponibilidade e sua capacidade de revisar a aplicação.

Obtenha um ganho rápido

Vulnerabilidades de alta prioridade acontecem o tempo todo, e como você lida com elas normalmente determina como as pessoas percebem a capacidade e a competência da equipe de segurança. Nesse cenário, vamos considerar uma pequena organização de serviços financeiros, talvez um banco regional. Eles usam uma aplicação cliente/servidor desenvolvida internamente para lidar com dados de empréstimos de clientes e usam procedimentos armazenados para processamento de back-end. A equipe da aplicação atualiza periodicamente a interface da web do front-end, mas o back-end permaneceu praticamente inalterado. É uma situação comum: se não estiver quebrado, não conserte; o aplicativo parece moderno para os clientes (que usam a interface da web) e o back-end funciona bem o suficiente. Porém, de vez em quando, eles recebem um alerta do fornecedor sobre uma vulnerabilidade considerável que afeta o banco de dados de back-end, sinalizando o release iminente de um patch. Dessa forma, a equipe de segurança deve descobrir o melhor e mais seguro caminho a seguir.

Vulnerabilidades de alta prioridade acontecem o tempo todo, e como você lida com elas normalmente determina como as pessoas percebem a capacidade e a competência da equipe de segurança.

A primeira etapa do nosso processo é a análise de risco. Com base em uma rápida revisão dos dados da ameaça, há um exploit livre, o que significa que não fazer nada não é uma opção, e o tempo é crucial. Em seguida, precisamos ter uma noção da importância da aplicação. Mencionamos acima a retenção de dados de empréstimos de clientes, então esta aplicação é fundamental para o negócio e está dentro do escopo de supervisão regulatória do banco. Como o uso da aplicação normalmente ocorre durante o horário comercial, um patch pode ser aplicado após o expediente.

Uma solução rápida é necessária porque o exploit está ocorrendo, já que os pesquisadores de segurança indicaram que consultas específicas podem fornecer acesso ao banco de dados. A equipe de segurança implementa um patch virtual temporário usando um dispositivo IPS de

perímetro, inspecionando e bloqueando as consultas perigosas específicas. Os parâmetros de ataque geralmente são muito amplos para o bloqueio de IPS, mas, neste caso, o patch temporário era viável.

Como outra precaução, a equipe aumenta o monitoramento em torno do banco de dados para alertá-los sobre qualquer atividade interna, o que evitaria o patch virtual temporário. O monitoramento adicional detectará um adversário desviando da aplicação usando um dispositivo já comprometido para fazer consultas perigosas diretamente no banco de dados.

A equipe de operações precisa então aplicar o patch do fornecedor durante a próxima janela de manutenção. O patch virtual temporário deu à equipe algum tempo para testar o patch do fornecedor para garantir que não afetaria a aplicação. O teste de patch do fornecedor não mostrou nenhum impacto adverso e a equipe de operações o aplicou com sucesso na janela seguinte.

A última etapa envolve uma revisão estratégica do processo para identificar melhorias para o futuro. Em algum ponto, a aplicação será revista e movida para a presença de nuvem do banco, mas não antes de 24 meses. Faz sentido aumentar a prioridade? Provavelmente não. Mesmo que a próxima vulnerabilidade não seja adequada para mitigação usando um patch virtual temporário, a correção pode ocorrer por meio de uma atualização de emergência fora do horário comercial, sem impacto significativo na disponibilidade da aplicação. Conforme a revisão da aplicação começa, as equipes irão considerar inicialmente mover alguns procedimentos armazenados para uma camada de servidor de aplicação e, posteriormente, migrar os dados para PaaS para reduzir a superfície operacional e o ataque à aplicação. Também devem considerar se uma oferta comercial de SaaS pode substituir a aplicação por completo.

Alinhamento organizacional

O cenário acima mostra como todas as opções de higiene da infraestrutura podem funcionar juntas para mitigar de forma eficaz o risco de uma vulnerabilidade no banco de dados de alta prioridade. Diversas equipes estiveram envolvidas no processo; começando quando a equipe de segurança identificou o problema, trabalhou nas alternativas de correção e decidiu por um patch virtual temporário e monitoramento adicional. A equipe de operações de TI desempenhou um papel essencial no gerenciamento de testes de patches e aplicações do fornecedor. A equipe de arquitetura considerará revisar a aplicação ou migrar para uma oferta SaaS.

Para trabalhar em conjunto com eficácia, todas essas equipes precisam se alinhar e colaborar para garantir o resultado desejado: disponibilidade da aplicação sem perda de dados. No entanto, devemos citar outra equipe com papel fundamental na facilitação do processo: Finanças. Eles pagam por itens como um dispositivo de perímetro que pode fornecer uma solução alternativa e um contrato de suporte/manutenção para garantir o acesso aos patches, especialmente para aplicações legacy facilmente esquecidas. Por mais críticas que sejam as habilidades técnicas para manter a infraestrutura em bom estado, é igualmente importante garantir que o pessoal técnico tenha os recursos para fazer seu trabalho.

Se você tiver alguma dúvida sobre este assunto, ou quiser discutir sua situação especificamente, sinta-se à vontade para nos enviar um recado pelo e-mail info@securosis.com.

Sobre o analista

Mike Rothman, Analista e Presidente

As perspectivas ousadas e o estilo irreverente de Mike são inestimáveis à medida que as empresas determinam estratégias eficazes para lidar com o dinâmico cenário de ameaças à segurança. Mike é especialista nos aspectos mais "atraentes" da segurança, como proteção de redes e endpoints, gerenciamento de segurança e conformidade.
Há 20 anos na área de segurança, ele é uma das pessoas que sabe o que está "por baixo dos panos".

Ele começou sua carreira como programador e consultor de rede, foi analista do META Group antes de fundar a SHYM Technology e, em seguida, ocupou cargos executivos na CipherTrust e TruSecure. Mike então fundou a Security Incite em 2006 para ser uma voz em um setor de segurança muito celebrado, mas ainda aquém do esperado. Depois de fazer um breve período como vice-presidente sênior de estratégia na eIQnetworks, Mike se juntou à Securosis com um cinismo rejuvenescido sobre o estado da segurança.

Mike publicou The Pragmatic CSO em 2007 para apresentar aos profissionais de segurança com orientação técnica as nuances do que é necessário para ser um profissional de segurança sênior. Ele também possui um diploma em Pesquisa Operacional e Engenharia Industrial pela prestigiada Cornell University. Seus pais não estão muito felizes por ele usar literalmente zero por cento de sua educação no dia-a-dia.

Sobre a Securosis

A Securosis, LLC é uma empresa independente de pesquisa e análise dedicada à liderança inovadora, objetividade e transparência. Todos os nossos analistas ocuparam cargos de nível executivo e se dedicam a fornecer serviços de consultoria pragmáticos de alto valor. Nossos serviços incluem:

- **Publicação de pesquisas primárias**: publicamos a maioria de nossas pesquisas gratuitamente em nosso blog e resumimos a pesquisa em artigos que podem ser licenciados para distribuição anualmente. Todos os materiais e apresentações publicados atendem aos nossos rígidos requisitos de objetividade e seguem nossa política de pesquisa totalmente transparente.
- **Cloud Security Project Accelerators**: Os Securosis Project Accelerators (SPA) são conjuntos de ofertas de consultoria para trazer nossa pesquisa aplicada e experiências de campo comprovadas para suas implementações em nuvem. Esses programas detalhados combinam avaliação, workshops personalizados e suporte contínuo para garantir que você possa proteger seus projetos de nuvem melhor e mais rápido. Eles são projetados para cortar meses ou anos de seus projetos enquanto integram práticas de segurança de nuvem de ponta em suas operações existentes.
- **Cloud Security Training:** Somos a equipe que construiu a classe de treinamento CCSK da Cloud Security Alliance e nosso próprio programa de Advanced Cloud Security e Applied SecDevOps. Participe de uma de nossas aulas públicas ou nos chame para uma experiência particular e personalizada.
- **Serviços de consultoria para fornecedores**: oferecemos uma série de serviços de consultoria para ajudar nossos clientes fornecedores a trazer o produto/serviço certo para o mercado da maneira certa para atender aos requisitos críticos do mercado. A Securosis é conhecida por dizer aos nossos clientes o que eles PRECISAM ouvir, não o que querem ouvir. Clientes normalmente começam com uma reunião de estratégia pontual e, em seguida, podem se engajar conosco em regime de contratação para suporte contínuo. Os serviços disponíveis como parte de nossos serviços de consultoria incluem análise e estratégia de mercado e produto, orientação de roadmap de tecnologia, estratégias competitivas, etc. Mas tenha em mente que mantemos nossos rígidos requisitos de objetividade e confidencialidade em todos os compromissos.
- **Pesquisa, apresentação e consultoria personalizadas**: Você precisa de um relatório de pesquisa personalizado sobre uma nova tecnologia ou problema de segurança? Um palestrante altamente conceituado para um evento de segurança interno ou público? Um especialista externo para uma due diligence de fusão ou aquisição? Um especialista para avaliar sua estratégia de segurança, identificar lacunas e construir um roteiro para o futuro? Esses projetos definidos preenchem a lacuna quando você precisa de mais do que um dia de estratégia, mas menos do que um compromisso de consultoria de longo prazo.

Nossos clientes variam de startups a alguns dos fornecedores de tecnologia mais conhecidos, além de usuários finais. Entre os clientes estão grandes instituições financeiras, investidores institucionais, empresas de médio porte e grandes fornecedores de segurança. Para saber mais sobre a Securosis,

visite nosso site http://securosis.com/ .