OPINIÃO

Automação do SOC: como diminuir o tempo de resposta a incidentes de 60 minutos para um minuto

Eduardo Lopes (*)

De 60 minutos para um minuto.

Essa é a diferença entre o tempo de resposta a um incidente cibernético da maneira tradicional para a automatizada. É uma disparidade que pode ser vital para o seu negócio, em um momento em que os prejuízos financeiros ocasionados por ciberataques são cada vez maiores, apesar dos altos investimentos em cibersegurança feitos pelas empresas. Diante desse contexto, é mandatório que as organizações substituam o aporte em tecnologias "hypadas" por uma estratégia de automação de respostas a incidentes. E o SOC tem um papel fundamental nesse processo.

Estima-se que os investimentos em SOC como serviço terá um crescimento esperado de US$ 10,5 bilhões até 2032, enquanto o valor do custo de danos do cibercrime deve atingir aproximadamente US$ 7,5 trilhões até 2025. A diferença é gritante e mostra a importância de desenvolver uma estratégia de segurança mais assertiva. Embora seja um pilar crítico de cibersegurança para qualquer empresa moderna, o SOC precisa passar por inovações que o deixem mais preparado para lidar com o atual cenário de ameaças.

- São muitos os desafios pelos quais os Centros de Operações de Segurança estão passando ultimamente, entre eles:
- Integração insuficiente: falta de adequação entre sistemas e ferramentas de automação
- Dependência excessiva de automação: confiar inteiramente em automação sem monitoramento humano
- Configuração errada de playbooks: erros na criação de playbooks automáticos, que podem resultar em respostas incorretas ou excessivamente genéricas
- Ausência de visibilidade em tempo real: acarretando atrasos na identificação de erros na própria automação
- Falta de personalização: usar soluções de automação sem adaptar as respostas para o ambiente específico de cada empresa
- Atualizações negligenciadas: deixar as ferramentas de automação desatualizadas, ignorando as novas ameaças ou as melhorias nos procedimentos
- Respostas automáticas mal calibradas: automação que executa ações excessivamente agressivas ou bloqueia serviços críticos sem uma verificação adequada
- Falta de treinamento da equipe: confiar na automação sem treinar adequadamente a equipe para supervisionar, ajustar e intervir quando necessário

Como se pode ver, para que o SOC cumpra o seu papel, de fato, e ajude a reduzir o tempo de resposta a incidentes por meio de automação, ele precisa do suporte de algumas tecnologias, como o Managed Detection and Response (MDR), o Security Information and Event Management (SIEM) e o Security Orchestration, Automation, and Response (SOAR). Enquanto o SIEM coleta, faz correlação e análise de dados, identifica padrões de comportamento e detecta anomalias, o MDR utiliza essas informações para tomar decisões estratégicas. Já o SOAR pode automatizar os processos de resposta a incidentes garantindo uma resposta mais rápida e eficiente.

É a combinação da inteligência humana com a automação que permitirá às organizações terem um melhor tempo de resposta a incidentes, e não a adoção desenfreada de novas tecnologias. Como vimos no início deste artigo, os danos causados pelos ciberataques só tendem a aumentar nos próximos anos e já passou da hora do board aproveitar melhor as soluções que já "têm em casa", como o SOC. Com as ferramentas certas e automatizado, ele tem tudo para reduzir ao mínimo o tempo de resposta a incidentes e garantir a continuidade do negócio.

(*) CEO da Redbelt Security.

Exército americano incorpora novo drone ao seu arsenal

No ambiente militar, os drones tornaram-se uma plataforma muito importante para reconhecimento e combate, não só pelo seu baixo custo e versatilidade, mas também por permitirem diminuir o número de baixas.

Vivaldo José Breternitz (*)

JESHOOTS_com_de_Pexels_CANVA

Em função disso, o exército dos Estados Unidos está adicionando novos drones ao seu arsenal – dentre estes, está o Switchblade 600, construído pela AeroVironment, que será produzido em massa no âmbito do programa Replicator, do Pentágono – antes mesmo do Pentágono incluir essa arma no Replicator, o exército já planejava comprar alguns Switchblade 600, após ver o que ele foi capaz de fazer na Ucrânia, Síria e Iraque – agora, está adquirindo mil unidades do drone.

O Switchblade 600 é dotado de recursos que lhe permitem rastrear e atacar alvos mesmo fora de sua linha de visão. São necessários apenas dez minutos para colocá-lo em ação, e pode permanecer no ar por cerca de 40 minutos, tendo um alcance de quase 40 quilômetros. Pode ser guiado manualmente ou operar autonomamente, com recursos de inteligência artificial.

Sua velocidade em missões de reconhecimento está ao redor de 110 km/h, mas se a missão assim o exigir, o Switchblade 600 pode voar a até 185 km/k. É armado com um projétil antitanque que pode causar danos consideráveis a blindados e outros alvos.

Alguns profissionais da área têm chamado o Switchblade 600 de drone kamikaze pois choca-se com o alvo que pretende destruir, destruindo-se também. No entanto, fontes do Departamento de Defesa americano dizem estar mais interessadas pelo uso do Switchblade 600 em outros domínios, como o de comando e controle.

O programa Replicator foi lançado em meados de 2023, sendo que um de seus objetivos declarados é o de ajudar os americanos a enfrentar os maiores recursos chineses em termos de navios, armas e tropas; para isso, deram à AeroVironment um contrato da ordem de US$ 990 milhões.

Vale lembrar que o orçamento militar americano em 2023 foi de US$ 916 bilhões. Já o brasileiro, foi de aproximadamente US$ 22 bilhões.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

Sustentabilidade e SSDs: escolhas tecnológicas que fazem a diferença no futuro

Vivemos em uma era onde as questões ambientais estão no centro das atenções e todos os dias somos confrontados com uma decisão: seguir os mesmos caminhos de consumo ou adotar escolhas mais conscientes e sustentáveis?

Chesky_W_CANVA

Quando se pensa em sustentabilidade, é fácil associar o conceito apenas a práticas de reciclagem ou ao uso de energias renováveis, mas a verdade é que nossas escolhas tecnológicas também desempenham um papel fundamental. Um exemplo disso é a adoção dos SSDs (unidades de estado sólido) em substituição aos tradicionais HDDs (discos rígidos).

Pode parecer um detalhe técnico, mas as implicações para o meio ambiente são profundas. Computadores, smartphones e servidores consomem grandes quantidades de energia, e sua fabricação e descarte geram um volume significativo de resíduos.

Os HDDs, por exemplo, funcionam por meio de partes móveis que giram para acessar os dados. Isso significa que, para manter um disco rígido funcionando, é necessário um fornecimento contínuo de energia para alimentar motores, ímãs e braços mecânicos que realizam a leitura e gravação de dados.

Por outro lado, os SSDs não possuem partes móveis. Utilizam memória flash, o que significa que o acesso aos dados é feito eletronicamente, sem a necessidade de componentes mecânicos. Isso faz com que o consumo de energia seja significativamente menor em comparação aos HDDs, podendo consumir entre 50% a 80% menos energia em uso ativo e ainda menos em modo ocioso.

Outro ponto fundamental para discutir quando falamos sobre sustentabilidade e SSDs é a durabilidade. Embora os discos rígidos possam falhar devido ao desgaste das peças móveis, os SSDs, por não possuírem esses componentes, são menos propensos a falhas mecânicas. Além disso, muitos SSDs têm uma alta resistência ao desgaste em termos de ciclos de leitura e gravação, o que significa que podem durar por muito mais tempo sem perda significativa de desempenho.

Essa longevidade se traduz em menos descarte de dispositivos e, portanto, menos resíduos eletrônicos para serem geridos. Considerando que o descarte inadequado de eletrônicos contribui para a poluição do solo e da água devido à presença de metais pesados e outros materiais tóxicos, prolongar a vida útil dos dispositivos tecnológicos é uma forma importante de reduzir esse impacto ambiental.

Se olharmos para o panorama maior, nossas escolhas tecnológicas desempenham um papel central na promoção de práticas sustentáveis. Cada vez mais, vemos uma mudança na forma como as pessoas compram e utilizam tecnologia. Não se trata apenas de buscar o dispositivo mais rápido ou mais barato, mas de considerar o impacto a longo prazo dessas escolhas.

Mas não são apenas os consumidores que devem carregar essa responsabilidade. As empresas têm um papel fundamental em promover e facilitar o uso de tecnologias mais sustentáveis. Muitos fabricantes de SSDs estão investindo em tecnologias mais verdes e desenvolvendo soluções para melhorar ainda mais a eficiência energética e a durabilidade desses dispositivos.

No fim das contas, cada escolha que fazemos conta. Se você está em dúvida entre um SSD e um HDD para o seu próximo computador, considere os impactos a longo prazo. Optar por tecnologias mais sustentáveis, como os SSDs, é uma maneira tangível de contribuir para a proteção do meio ambiente.

Nosso planeta enfrenta desafios significativos, mas o futuro ainda está em nossas mãos. Ao fazer escolhas tecnológicas inteligentes, podemos reduzir nossa pegada de carbono, diminuir o volume de resíduos eletrônicos e garantir que a inovação continue a ser um motor de progresso, sem sacrificar a saúde do nosso planeta!

(*) Diretor de Vendas da Netcore - empresa que fabrica memórias RAM e SSDs para o mercado brasileiro.

News @TI

TD Synnex oferece no Brasil soluções multi-nuvem da Vawlt

@ A TD SYNNEX anuncia o acordo com a Vawlt Technologies para distribuir no Brasil suas soluções de armazenamento e segurança de dados. Com essa parceria, os clientes passarão a ter acesso à solução da Vawlt, que combina ambientes on-premise com nuvens privadas e múltiplas nuvens públicas, assegurando total independência de provedores de nuvem. Os clientes também se beneficiarão de melhor desempenho em movimento, privacidade e proteção de dados contra ameaças como ransomware, entre outras vantagens que incluem uma relevante economia de custos. A solução da Vawlt constrói uma camada de software que distribui dados simultaneamente em vários nós, em diferentes nuvens e on-premises, criando uma "super nuvem", permitindo ao usuário usufruir o melhor dos diversos ambientes de cloud por meio de um único painel de controle (https://lac.tdsynnex.com/br/pt-br/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.