SOC, o exército de ciberdefesa das organizações

digitalinside.pt/soc-o-exercito-de-ciberdefesa-das-organizacoes

Bruno Castro 4 de junho de 2024

Neste cenário, um Security Operations Center (SOC), quer interno, quer *as a service* (isto é, *outsourced*) destaca-se como o verdadeiro exército de ciberdefesa das organizações. Um SOC consiste em uma unidade especializada, dedicada à monitorização, deteção, análise, mitigação, resposta a incidentes de segurança e sua respetiva recuperação. Assim como um exército é responsável pela proteção do território e pela soberania de uma nação, por sua vez, o SOC é responsável pela proteção do espaço digital de uma organização num modelo de 24 horas x 7 dias por semana, defendendo-a contra as ameaças digitais constantes. O objetivo é ter uma guarda armada constantemente vigilante a eventuais intrusões e ações maliciosas dentro da organização antes que passem a ser disruptivas ou destrutivas.

Através de avançadas ferramentas de análise e inteligência em coordenação com equipas de operadores/analistas experientes, é possível estabelecer um serviço continuo de monitorização e alarmística que permita detetar & reagir em tempo útil a eventuais ações erróneas, suspeitas ou maliciosas dentro da organização. Quando uma ação – errónea, suspeita ou maliciosa – é detetada, a equipa do SOC entra em ação de forma coordenada, semelhante a um exército que se mobiliza para um conflito, em que cada frente tem a sua função estratégica, cuja coordenação pretende guiar até à derradeira vitória sobre o potencial inimigo.

Este processo de deteção e resposta a incidentes no contexto de um SOC, integra vários processos que devem ser levados a cabo, nomeadamente: **identificação** de eventuais comportamentos anómalos, suspeitos ou maliciosos, e qual a sua origem (em âmbito de investigação forense)); **contenção** da ameaça (ou incidente), de forma a limitar e prevenir eventuais danos; **erradicação** da ameaça e restauração dos sistemas afetados; **recuperação** do pleno funcionamento, após verificação de que os sistemas estão devidamente higienizados e que a ameaça é definitivamente removida; por fim, **lições aprendidas,** em que a equipa deve reunir as informações relevantes sobre o incidente e extrair lições que permitam a melhoria da resposta a futuros incidentes.

No entanto, e como uma das principais tendências de mercado da segurança – é claramente um “must-to-have” atual – importa ter em consideração o esforço de implementar um SOC de forma eficiente. É efetivamente uma tarefa complexa – requer um elevado investimento em tecnologia, software, know-how e pessoas formadas e especializadas. Neste sentido, cabe às organizações avaliar o esforço necessário, de forma a perceber se reúnem condições para implementar um SOC internamente, com todo o investimento que requer, ou se, a melhor solução será optar por selecionar um SOC “*as a service*” através de um fornecedor externo que disponibilize uma solução configurada à sua medida, para ser escalável e atender às necessidades crescentes e urgentes da sua organização. Para esta opção, e sendo cada vez mais uma tendência

de mercado, é fundamental que o processo de seleção e compra do serviço responda especificamente às necessidades da sua organização (em prol de algo standard num formato de “igual para todos”).

Qualquer que seja a opção, esta é a solução que uma organização não pode perder – seria impensável qualquer pessoa sair de casa e não trancar a porta da frente; não ter um SOC que forneça esta camada de proteção e defesa holística e personalizada em tempo real, será sinónimo de deixar a sua organização, literalmente, de portas abertas para o cibercrime na sua generalidade. Investir num SOC robusto não é apenas uma medida de segurança, é sobretudo, uma necessidade estratégica para assegurar a (boa e ininterrupta) continuidade das operações num ambiente digital cada vez mais hostil e imprevisível.

Além da resposta ativa ou reativa, o SOC desempenha igualmente um papel crucial na implementação de estratégias preventivas. Num mundo onde a reputação e a confiança são fatores de enorme valor acrescentado, a capacidade de uma organização prevenir-se perante ciberameaças, é um diferencial competitivo cada vez mais valorizado na indústria, ou até na maioria dos sectores empresariais e estatais, mas também nos normativos de segurança a nível mundial. Desta feita, o SOC não funciona somente como um defensor de sistemas e dados, mas também como um defensor da confiança, integridade e reputação de uma organização. É cada vez mais vulgar existir a necessidade de comprovar a existência de um SOC na organização para demostrar compliance e confiança perante as autoridades, parceiros ou reguladores.

No campo de batalha cibernético, que está em constante evolução, um SOC “à sua medida” faz toda a diferença. Por isso, aconselho vivamente todos os responsáveis de segurança: *don’t sleep on SOC,* e não deixe a sua organização desprotegida enquanto dorme…