*Por Thales Cyrino e Rodrigo Leal**

Capítulo V

História e evolução dos Centros de Operações de Segurança (SOCs)

Como abordado em capítulos anteriores, as ameaças de segurança cibernética estão se tornando mais complexas e sofisticadas. Por trás destas ameaças estão organizações com alto nível de conhecimento, como Anonymous, Conti, Revil, Lapsus$ e outras. As principais motivações para os ciberataques são ganhos financeiros, reconhecimento, motivação política, espionagem corporativa, dentre outras. Neste contexto, é possível identificar que qualquer pessoa, organização pública ou privada, país ou qualquer outra entidade que, de alguma forma esteja conectada, é um alvo em potencial.

Para se proteger deste tipo de ataque, primeiramente, é necessário monitorar todos os ativos que possam ser uma porta de entrada para ameaças digitais e, hoje, com o aumento exponencial das superfícies expostas, isto se torna cada vez um desafio maior. Além desta etapa, é fundamental termos ações visando construir redes robustas e controles de acessos seguros, como já tratado nos capítulos passados.

Para endereçar a necessidade de monitoramento constante foram criados os SOCs - Security Operation Centers. O SOC é um conjunto de profissionais de segurança cibernética responsáveis pelo monitoramento e investigação em tempo real de eventos de segurança para prevenir, detectar e responder a ameaças cibernéticas através processos e tecnologias.

Os SOCs são o resultado da soma entre as melhores tecnologias de segurança, gerenciadas pelos mais experientes profissionais com processos realmente qualificados e eficazes. Com operações 24x7, os analistas monitoram e gerenciam cada ativo da companhia e respondem prontamente a qualquer sinal de alerta. É difícil algo passar despercebido. Eles têm ali, ao alcance dos olhos, tudo que pode representar uma ameaça para o negócio: uma informação sensível sendo enviada para uma pessoa de fora da empresa, uma máquina desatualizada, configurações malfeitas, tentativas de acesso a dados sigilosos por pessoas não autorizadas, tudo que possa representar um risco cibernético deve ser identificado e tratado da melhor forma possível. Dessa maneira, através de uma metodologia, é possível conter as atividades suspeitas rapidamente.

A história de evolução do SOC está relacionada à evolução dos ataques e das ferramentas de segurança, ao aprimoramento dos processos e, no centro de tudo, à capacitação dos profissionais.

Podemos dividir esta história em 4 principais momentos:

• ***Monitoração de disponibilidade***

Nesta fase, basicamente, era feita uma gestão de ativos de rede e análise de código malicioso, o que podemos entender como um NOC – Network Operation Center, modelo existente até 1995 e realizado principalmente por Governos e Forças Militares.

• ***Monitoração reativa***

Podemos dizer que foi a partir de 1996 que realmente se iniciaram as primeiras iniciativas de SOC. Com a implementação de antivírus, IDS e Firewalls foi possível identificar vírus e intrusos. A partir de 2001, com a implantação de gestão de vulnerabilidades, IPS e AntiSpam, foi possível iniciar um trabalho de conformidade e aumentar a capacidade de resposta a incidentes, já que a visibilidade de fato aumentou.

Entre 1996 e 2006, o papel do SOC ainda era reativo e somente Governos, Forças Militares, grandes empresas e bancos implementavam esta estrutura dentro de suas organizações.

• ***Monitoramento proativo***

A principal evolução que ocorreu no modelo de SOC foi entre 2007 e 2013, quando, de fato, o monitoramento passou a ser

proativo. Com a implementação de soluções de DLP (data leakage prevention), SIEM (Security Information and Event Management), passou a ser possível identificar APTs (Advanced Persistent Threats). O termo APTs é utilizado para descrever um ataque onde o intruso ou intrusos estabelecem uma conexão de longo prazo em uma rede para extrair dados sensíveis e confidenciais. O principal trabalho do SOC neste período foi identificar e conter APTs, iniciando assim uma monitoração proativa. Neste período também surgiram os MSSPs (Managed Security Services Providers), empresas especializadas em prover serviços de SOC, o que permitiu que outras organizações, além de Governos, forças militares, grandes empresas e bancos, pudessem contar com um SOC, já que o alto custo em ferramentas, processos e pessoas era e ainda é inviável para muitas companhias.

Entre 2013 e 2015, o monitoramento proativo evoluiu ainda mais com a adoção de tecnologias e processos, como CASB, Cloud Security, UEBA, TIP, Sandboxing, CERT e BYOD.

• ***Monitoramento proativo com automação***

A partir de 2015 o SOC continuou evoluindo com a inclusão de "threat intelligence", através de feeds opensource e comerciais. A inteligência contra ameaças enriqueceu o contexto dos incidentes e ajudou os analistas de segurança a tomarem melhores decisões. O threat intelligence também deu visibilidade às táticas, aos comportamentos, às ferramentas e aos processos dos adversários, adicionando mais valor aos SOCs através de TTPs (Táticas, Técnicas e Procedimentos) focados em threat hunting, permitindo uma detecção e remediação de ameaças escondidas mais rapidamente. Para se ter uma ideia, em 2013, o MITRE iniciou o ATT&CK que é uma base de conhecimento de comportamento e taxonomia dos adversários cibernéticos, que passou a ser utilizado em maior escala pelos SOCs neste momento.

Outro grande avanço neste momento foi a adoção de automação, ou seja, através de ferramentas como a SOAR (Security Orchestration, Automation and Response), foi possível escalar as respostas aos incidentes já conhecidos implementando estas automações. A implantação de automação nos SOCs faz parte de processo contínuo de evolução.

Os SOCs continuam em processo de evolução contínuo, primeiro, para atender à demanda de proteger mais superfícies expostas, e, segundo, para tentar se antecipar às novas ameaças que surgem todos os dias. O investimento em conhecimento é de suma importância, atrelado ao grande desafio da falta de profissionais. Hoje se estima que faltam 4 milhões de profissionais de cybersecurity no mundo, 441 mil só no Brasil. Atualmente, no mundo 100% conectado, todas as organizações devem possuir um SOC, próprio ou terceirizado, uma vez que é muito importante

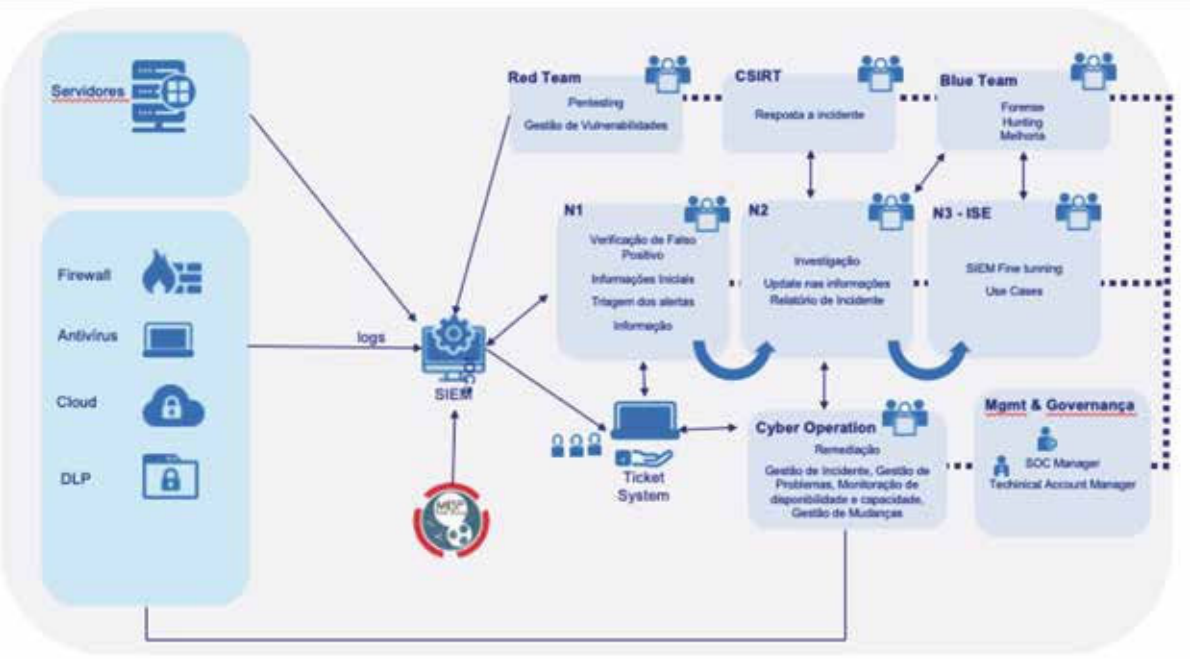

Figura 1 – Modelo de estruturação de um SOC.

para avaliar todos os desafios e riscos, entender os custos diretos e indiretos de se manter uma estrutura atualizada em processos, pessoas e tecnologias para que o negócio não seja afetado.

O SOC deve estar sob gestão de um CISO (Chief Information Security Officer), mas esta é apenas uma de suas responsabilidades. Portanto, o SOC deve ser gerenciado ou dirigido por um profissional sênior que reporte diretamente ao CISO, já que este é responsável também pelo planejamento de arquitetura de segurança e pelo alinhamento constante com o board e as áreas de negócio para entender e apoiar o desenvolvimento do negócio com segurança, através de uma metodologia de security by design, governança, fraude, programas de conscientização, entre outros. É importante também que o CISO tenha autonomia e reporte diretamente ao board, e não mais ao CIO. Este é um movimento global que já vem ocorrendo e o principal motivo é garantir autonomia a este profissional, considerando que cybersecurity hoje é um risco de negócio e deve ser tratado como tal.

Existem diversas formas de se estruturar um SOC, dependendo do nível de maturidade da organização. A Figura 1 traz um modelo com algumas funções, como Red Team, CSIRT, Blue Team, Cybersecurity Operations, Gestão e Governança, e N1, N2 e N3 para gestão e triagem dos eventos.

Como se pode notar, é possível internalizar ou terceirizar cada uma destas funções de acordo com o momento e recursos de cada organização. Independentemente de qual parte do SOC seja interna ou externa, é importante entender os desafios, as vantagens e as desvantagens de cada modelo.

As principais vantagens de se terceirizar um SOC são: menor valor de investimento e facilidade para gerenciar os custos, acesso imediato a especialistas em cybersecurity, escalabilidade, flexibilidade, acesso a múltiplos feeds de threat intelligence, isenção de conflito com outras áreas da organização.

Já as principais desvantagens podem ser: envio de dados para fora do perímetro, acesso a um time compartilhado, conhecimento limitado do negócio, pouca possibilidade de customização de serviços e valores.

Por isso, a decisão de se terceirizar e a escolha de uma empresa para fornecer este tipo de serviço devem ser feitas de forma criteriosa para que as vantagens possam superar as desvantagens, já que os Centros de Operações de Segurança oferecem às empresas a oportunidade de se manterem focadas em seu core business. Diante de um cenário em que organizações passam por uma grande transformação digital e enfrentam ameaças em constante evolução, ao mesmo tempo em que lidam com os crescentes custos e a complexidade de sua infraestrutura, o SOC como serviço se mostra uma alternativa eficaz para desafogar os times de TI e apoiar as decisões de negócios.

**Thales Cyrino é técnico em processamento de dados, administrador de empresa pela Universidade Anhembi Morumbi e pós-graduado em Marketing pela FGV SP, com mais de 20 anos de experiência no mercado de TI. Atualmente, é diretor de vendas de cybersecurity na NTT.*

Rodrigo Leal é graduado e mestre em Engenharia Elétrica com MBA em Gestão de Projetos e cursando MBA Executivo de Negócios do Setor Elétrico pela Fundação Getúlio Vargas. Desde 2006 é funcionário da Chesf, onde já exerceu cargos de Assessor e Gerente, na área de Telecomunicações, Proteção e Automação. Atualmente está como assessor do Diretor de Operação. Também ocupa a posição de Vice-Presidente do Conselho Diretor da UTC América Latina e Coordenador do Comitê de Tecnologia da Informação e Telecomunicações no CIGRE-Brasil.