



EVERESTRIDGE



ENTRAR



Monitoramento
de segurança (SOC)
e de redes (NOC)

Índice

[A importância do monitoramento de segurança](#)
[- SOC \(Security Operations Center\)](#)

[Entenda mais sobre segurança da informação](#)

[Mas, afinal, para que serve o monitoramento?](#)

[A importância do monitoramento de segurança](#)

[NOC: a sua rede vigiada](#)

[O que é o NOC](#)

[Como funciona](#)

[Como o NOC melhora o desempenho de sua rede](#)

[Aplicações práticas](#)

[SOC, segurança para dados e estrutura](#)

[O que é o SOC](#)

[Atividades](#)

[Aplicações do SOC](#)

[Problemas que um SOC pode evitar](#)

[A terceirização do NOC e do SOC](#)





O mundo vem sofrendo uma revolução tecnológica. Com isso, as empresas tiveram a necessidade de se atualizar diante de mudanças ocorridas em vários setores. Uma das principais delas está relacionada à segurança da informação, que engloba o monitoramento de segurança.



ÍNDICE





Entenda mais sobre a segurança da informação

A segurança da informação baseia-se em três aspectos:

- **Disponibilidade.** É a garantia de que todos os dados estejam disponíveis quando o usuário precisa deles;
- **Integridade.** É a manutenção de todas as informações armazenadas no seu formato original;
- **Confidencialidade.** É a garantia de restrição de acesso às informações e do sigilo destas.

Todo plano de segurança da informação deve conter esses fundamentos e ser monitorado durante 24 horas. Quem deseja adquirir o monitoramento da segurança por meio de serviços terceirizados precisa procurar uma empresa especializadas com certificações internacionais e nacionais.



ÍNDICE



Mas, afinal, para que serve o monitoramento?



A revolução tecnológica e a transformação digital pelas quais as empresas estão passando promoveram uma troca dos sistemas de segurança internos para que elas se mantivessem competitivas. Os novos sistemas têm base na virtualização das informações e dos dados, assim como na automação.

As empresas que contam com banco de dados com diversas informações sobre seus clientes precisam realizar o monitoramento de segurança para evitar falhas no sistema e hackeamento.

O monitoramento de segurança é responsável por detectar, analisar e responder a incidentes de segurança cibernética usando uma combinação de soluções de tecnologia e um forte conjunto de processos.



ÍNDICE



A importância do monitoramento de segurança

O principal objetivo da segurança da informação é proteger e monitorar os dados armazenados e implementar ferramentas e mecanismos que anulem as vulnerabilidades, falhas e ameaças que podem aparecer em decorrência das novas tecnologias.

Por conta disso, as empresas precisam realizar o monitoramento de segurança durante 24 horas. Elas podem implantar um SOC – Security Operations Center e um NOC – Network Operations Center, plataformas que monitoram a rede e sua disponibilidade e se mostram capazes de detectar quaisquer incidentes relacionados à segurança dos dados.

Além de defender de possíveis ataques ou falhas, a segurança da informação contribui para o gerenciamento dos ativos do negócio, o aumento do ROI (retorno dos investimentos) e a redução dos riscos.



ÍNDICE





As principais vantagens do monitoramento de segurança são:

- **Aumento da produtividade.** A redução da quantidade de manutenções e reparos proporciona maior produtividade por parte dos colaboradores.
- **Controle de acesso.** É a habilidade de permitir ou negar o uso do sistema e dos dados aos colaboradores. Por meio desse monitoramento, o tempo de uso indevido na internet será reduzido drasticamente, com o consequente aumento da produtividade dos funcionários e da segurança da empresa contra malwares, vírus e intrusão.
- **Credibilidade da empresa.** Nos negócios, segurança é sinônimo de confiança. Quando os dados são monitorados, tanto companhias parceiras quanto clientes se sentem mais seguros em fazer negócios com a empresa. Se ocorre uma falha no sistema e dados sigilosos são expostos, a reputação da empresa pode ficar manchada para sempre.
- **Proteção de dados.** As informações sobre os clientes devem ser protegidas sob qualquer circunstância. Com a instalação de um sistema adequado, é possível desenvolver as melhores estratégias preventivas e assim evitar prejuízos de grande porte.

Independentemente do tamanho e do setor da empresa, é de extrema importância que haja um monitoramento de segurança eficiente. Isso garante uma reputação positiva e o sucesso da empresa em relação à concorrência.

NOC: a sua rede vigiada

Hoje, a maioria dos processos das empresas se apoia na tecnologia, desde o chão de fábrica até a área comercial e a logística. Portanto, é fundamental o monitoramento da infraestrutura de Tecnologia da Informação – TI.

Os ambientes de TI requerem cuidados constantes para que os sistemas se mantenham eficientes e rápidos. Num mundo tão ágil, flexível e dinâmico, o departamento de TI precisa crescer e se tornar cada vez mais complexo para que as empresas se mantenham competitivas.

O monitoramento de redes NOC (Network Operations Center ou Centro de Operações de Rede) tem como objetivo principal manter a infraestrutura de TI monitorada para encontrar possíveis problemas e evitar perdas financeiras.

O que é o NOC

O NOC é uma estrutura que monitora e gerencia eventos de TI com profissionais altamente especializados em administração de redes. O monitoramento é feito por meio de alertas gerados pelos ativos de TI.

Além de monitorar os eventos da rede, o NOC também recebe requisições e responde a falhas. Em outras palavras, ele não coleta apenas dados do ambiente de TI e sim de todo o negócio, o que torna a empresa mais competitiva.



ÍNDICE





O NOC também atualiza licença e softwares, realiza backups e executa scripts que estabilizam incidentes de forma imediata, assim como gera relatórios para que a empresa possa implementar melhorias necessárias. O relatório do NOC contém sumário de alertas, performance/capacidade, previsão futura, gerenciamento de nível de serviço e disponibilidade.

O NOC é uma das boas práticas de TI no que diz respeito a tomada de decisão por parte dos empreendedores.

Como funciona

O funcionamento do NOC se dá por meio de um conjunto de ferramentas que monitoram e coletam dados e serviços, informações de infraestrutura de TI, aplicações vindas dos usuários finais de maneira direta.

Essas ferramentas vão realizar os registros de atendimento, emitir relatórios de performance, gerenciar filas de atendimento, encaminhar processos para outros setores etc.

Por meio do monitoramento de segurança, o NOC coleta dados do ambiente durante 24 horas por dia e sete dias por semana, registrando o desempenho de redes, eventos e incidentes que podem ou não causar algum impacto à empresa.

Em resumo, o NOC monitora os incidentes que possam afetar a performance e a disponibilidade dos negócios, e responde a eles. Esses eventos detectados pelas ferramentas de monitoramento identificam os problemas e notificam em tempo real os operadores. Por meio de fluxos de trabalho e processos pré definidos pelo departamento de TI, os operadores têm condições de encontrar soluções rápidas.

O NOC pode ser operado por empresas terceirizadas que vão acompanhar a disponibilidade de todo o ambiente de TI e o desempenho de rede, oferecendo respostas eficazes.

Como o NOC melhora o desempenho de sua rede

O NOC realiza muito mais que o monitoramento. Ele também ajuda a melhorar o desempenho da rede, pois trata oscilações, eventos recorrentes e incidentes de impacto. Saiba como isso é feito:



ÍNDICE





Coleta de dados automática

O monitoramento e o gerenciamento da infraestrutura de TI fornecem dados fundamentais sobre a rede e sobre todos os setores que precisam de melhorias. Como a rede é monitorada o tempo todo (24/7), os dados são enviados de forma automática.

Aumento de eficiência e economia de tempo

Com o monitoramento de redes automático, todos os equipamentos da rede são monitorados em tempo real.

O NOC ajuda a reduzir gastos, economizar tempo e em consequência há aumento de eficiência. Com isso, a empresa pode aplicar recursos em outros setores, sem se preocupar em compilar os ativos de TI de forma manual.

Detecção precoce e manutenção ativa

Com o monitoramento de redes sendo realizado ininterruptamente, sempre que acontecer alguma irregularidade, um alerta será enviado e o problema será resolvido de forma imediata. Essa detecção precoce evita que haja redução da produtividade.

Além disso, o NOC garante uma manutenção ativa para gerar maior estabilidade no ambiente de TI, uma vez que ocorre a manutenção dos principais sistemas, backups de dados críticos e atualizações de softwares, antivírus etc.

Redução de interrupções

Qualquer problema na rede precisa ser tratado de forma correta

e rápida. Com o monitoramento de redes contínuo e remoto, o tempo de inatividade dos sistemas e as interrupções são reduzidos, o que garante a melhora no atendimento ao cliente.

Acompanhamento constante

De acordo com pesquisa do Network Barometer Report, quando as redes são monitoradas, a resposta é 69% mais rápida e há uma redução de 32% no tempo de reparo.

Segundo esse estudo, um terço dos eventos é causado por erro ou configuração humana. Dessa maneira, os problemas de rede podem aparecer a qualquer hora, atrapalhando a produtividade da empresa. Por isso, o acompanhamento constante é fundamental para se solucionar os eventos de forma mais rápida.

Aplicações práticas

Entre os itens que garantem a alta performance do NOC estão integração, comunicação, conscientização, treinamento, suporte ou help desk, alerta de ocorrências e gestão de riscos.

O monitoramento de rede em tempo real e constante pode ser utilizado em diversas situações. As principais aplicações práticas são:

- Monitoramento web em relação à experiência dos usuários;
- Inspeção de middleware e banco de dados;
- Controle de disponibilidade e performance de links de comunicação;
- Acompanhamento de redes WAN, WLAN, LAN, sistemas e segurança de perímetro;
- Monitoramento do tráfego de links junto às operadoras de comunicação;
- Supervisão dos sistemas de estrutura e armazenamento em nuvem.
- Monitoramento de sistemas operacionais e servidores.

SOC, segurança para dados e estrutura

Enquanto o NOC é voltado para o desempenho e a gestão de rede, o que garante a disponibilidade para os processos, o SOC (Security Operations Center – Centro de Operações de Segurança) é focado na segurança dos dados e da estrutura da empresa.

As operações do NOC e do SOC apresentam algumas diferenças entre si e se complementam mutuamente. O NOC identifica eventos ou problemas que afetam a disponibilidade e o desempenho das redes. Já o SOC atua no monitoramento de segurança e na identificação de ataques que a base de dados pode sofrer em sua estrutura.

O que é o SOC

A internet e a tecnologia promoveram uma reestruturação nos ambientes de trabalho, tornando-os cada vez mais remotos e virtuais. Com esse avanço e essa nova dinâmica, a preocupação com a segurança de dados e com as informações cresceu consideravelmente.

De acordo com um estudo da Hewlett Packard Enterprise – HPE, milhares de empresas em todo o mundo são vulneráveis aos riscos dos ataques cibernéticos. Uma das opções que garantem a detecção, preservação e proteção dos dados, assim como a resposta rápida às ameaças, é a adoção do SOC.

O SOC é uma ferramenta que centraliza todos os serviços referentes à segurança da informação, combinando processos, projetos, tecnologias adotadas, recursos humanos etc. para formar uma estrutura que gerencia a segurança da informação.

Atividades

O principal objetivo do SOC é aumentar a segurança dos dados e garantir sua integridade. As atividades que envolvem o SOC são:

- **Prevenção.** É realizada com o uso de práticas capazes de prevenir incidentes, por meio de atualizações de hardwares, softwares, rastreadores, antivírus e outras tecnologias relacionadas à segurança;
- **Detecção.** Identifica falhas, problemas e ameaças de segurança nos processos;
- **Resposta.** Soluciona os incidentes de segurança encontrados, agindo de maneira eficaz e rápida. O SOC pode bloquear ataques, corrigir falhas e reduzir quaisquer efeitos negativos causados por esses incidentes;
- **Avaliação.** Analisa e monitora todos os processos de vulnerabilidade, de acordo com os riscos que a empresa pode enfrentar.



ÍNDICE



Aplicações do SOC

A estrutura do SOC atua no monitoramento de todos os recursos de segurança, como UTM, antivírus, anti-DDoS, IPs e firewalls. Ele cruza dados sobre os eventos, detecta tentativas de ameaças ou invasões e proporciona uma solução chamada Security Information and Event Management – Siem.

O SOC recebe alertas emitidos de forma automática. Caso as configurações e os processos não consigam deter a invasão, equipes de suporte são acionadas para conter as ameaças.

Além de melhorar o monitoramento de segurança, o SOC apresenta vários benefícios para a empresa. A seguir, os principais:

- **Recuperação de informações e dados;**
- **Melhora nos processos de auditoria;**
- **Maior precisão e velocidade na resposta contra as invasões;**
- **Monitoramento mais preciso e contínuo;**
- **Melhora na análise de processos e dados;**
- **Otimização de tempo;**
- **Agilidade e eficiência na tomada das decisões;**
- **Centralização dos processos e recursos.**



ÍNDICE





As empresas sujeitas às regras de proteção às informações precisam do SOC. De acordo com a Resolução nº 4658/2018 do Banco Central, todas as instituições financeiras e bancos devem implantar o SOC para responder aos incidentes cibernéticos. A lista de instituições que devem aplicá-lo ao SOC inclui:

- **Bancos privados;**
- **Banco Central do Brasil;**
- **Corretoras de valores;**
- **Instituições financeiras;**
- **Operadoras de cartões de crédito;**
- **PCI-DSS – Payment Card Industry Data Security Standards;**
- **CVM – Comissão de Valores Mobiliários**

O SOC não só garante uma maior proteção às informações como fornece dados e relatórios que comprovem isso. Dessa forma, a empresa permanece em conformidade com os órgãos reguladores e melhora sua confiabilidade diante dos clientes e da sociedade



ÍNDICE





ÍNDICE



Problemas que um SOC pode evitar

Atualmente, as informações e dados são fundamentais para que qualquer negócio sobreviva e são alvo da ação de cibercriminosos.

Muitas vezes, as empresas nem percebem as ameaças e os ataques, e só sentem o impacto quando há discrepâncias no setor financeiro ou quando são divulgadas as informações. O SOC pode ajudar a resolver esse tipo de problema, assim como outros.

Uma de suas principais funções é a centralização das operações de segurança (softwares, protocolos, ferramentas) em um único lugar, tornando mais eficiente o monitoramento de segurança.

Os principais problemas que um SOC pode prevenir na sua empresa são:

- **Bloqueio das informações em relação a ataques do tipo ransomware, que costuma exigir alguma forma de pagamento de resgate destas.**
- **Prevenção, detecção e reação frente às ameaças cibernéticas proporcionadas pelo monitoramento contínuo.**
- **Proteção à autenticação de dados e dispositivos em nível executivo que evitam penalidades por negligência, omissão etc.**
- **Revisão periódica eficiente dos riscos e gaps identificados, de modo a evitar que novas ameaças surjam ou até mesmo que ocorram falhas no processo de coleta dos dados.**

É obrigação de todas as empresas manter a segurança de dados que os clientes disponibilizam para elas. É o principal pilar de confiança na relação entre cliente e empresa. Pensando nisso, um sistema centralizado como o SOC é imprescindível para o monitoramento e a detecção de ameaças ou falhas que podem causar prejuízos à sua empresa.

A terceirização do NOC e do SOC

A terceirização do NOC e do SOC é viável e rentável para as empresas, sem prejudicar a produtividade.

A empresa que deseja implementar essas estruturas precisa investir bastante em softwares, equipamentos e profissionais específicos.

Graças a essa terceirização, elas ficam protegidas com menos alocação dos recursos, otimizando a produtividade.

A Everest Ridge é especializada no monitoramento de redes e segurança digital e oferece as melhores soluções personalizadas de NOC e de SOC. Fundada em 2010, ela conta com os melhores serviços para planejar, desenvolver, gerenciar e dar suporte em infraestrutura de TI e Telecom.

Ao terceirizar os serviços de NOC e de SOC com a Everest Ridge, sua empresa vai contar com tecnologia avançada e profissionais altamente qualificados, que irão fornecer soluções e serviços nos setores de monitoramento de segurança e desempenho de redes.

Conheça mais sobre a terceirização de NOC e de SOC e outras soluções com a nossa equipe especializada.



ÍNDICE





EVEREST RIDGE

Tel.: (11) 3181.4008
comercial@everestr ridge.com.br

www.everestr ridge.com.br



VOLTAR