realprotect

CASO DE SUCESSO

Comitê de Esportes utiliza o Monitoramento de Segurança Real Protect para mitigar ameaças avançadas

Respeitamos a privacidade de nossos clientes, por isso, não divulgaremos as informações da empresa.
Os gestores não possuiam visibilidade sobre a infraestrutura de TI. Essa visibilidade é essencial para que os riscos ao ambiente e ao negócio possam ser mitigados. Para conquistar essa visibilidade, os gestores precisavam de monitoramento contínuo das informações geradas pelos ativos. O monitoramento também deveria identificar a disponibilidade de todos os ativos de TI da infraestrutura do Comitê.

Plataforma de Segurança

Para que os gestores pudessem de fato compreender o ambiente e mitigar as ameaças, era preciso mais do que apenas coletar e observar as informações geradas pelos ativos, foi preciso correlacionar as informações geradas por cada um dos ativos de segurança. Todo o tráfego passou a ser analisado pelo SOC Real Protect, fornecendo a visibilidade necessária pelos gestores e área operacional.

Setor

Esportes

O Desafio

Os gestores não possuiam visibilidade sobre a infraestrutura de TI, essencial para mitigação de riscos do ambiente. Para atingir essa visibilidade, era preciso monitoramento das informações geradas e disponibilidade das soluções de segurança e dos ativos de TI.

A Solução

Foi utilizado uma plataforma de segurança envolvendo soluções como SIEM e Anti-APT, agregados à inteligência de segurança gerada pelo SOC Real Protect. Todo o tráfego passou a ser analisado e correlacionado para a identificação de incidentes de segurança, fornecendo a visibilidade necessária pelos gestores e área operacional.

Os Benefícios

A partir da inteligência de segurança gerada pelo SOC Real Protect, foi possível reduzir os tempos de detecção de anomalias e agilizar a resposta a incidentes de segurança. A inteligência também permitiu uma revisão das políticas vigentes e mitigação dos riscos de segurança para o negócio.

Inteligência de Segurança

Os serviços de Monitoramento de Segurança e Monitoramento de Disponibilidade de Ativos demandaram a utilização de uma plataforma de segurança, que envolveu soluções como SIEM e Anti-APT. Todas as informações geradas eram redirecionadas, correlacionadas e analisadas pelo SOC Real Protect. Utilizando a solução de Anti-APT, oferecemos a tecnologia para detectar e responder aos ataques direcionados e ameaças avançadas. Contando com mecanismos de detecção e Sandboxing personalizados, tornou-se possível identificar e analisar malwares, comunicações de C&C e atividades evasivas de agressores invisíveis para a segurança padrão.

A utilização dessa inteligência de segurança, gerada pelo SOC Real Protect, foi a grande responsável pela redução dos tempos de detecção de anomalias e resposta a incidentes. Com a visibilidade pretendida, os gestores também puderam mitigar os riscos ao ambiente e ao negócio.

Atividades da Operação

Os serviços de Monitoramento de Disponibilidade de Ativos e Monitoramento de Segurança possuem uma série de atividades desenvolvidas no momento da operação, veja o que foi realizado pelo SOC Real Protect:

> Monitoramento contínuo e automatizado dos alertas de segurança: utilizando correlação de eventos de todas as soluções monitoradas do ambiente além dos controles de segurança com seus devidos thresholds e criticidades, escalando os incidentes quando necessário através do processo de resposta a incidentes da Real Protect, adaptado para a realidade do Comitê.

> Identificação dos riscos do ambiente: por meio dos eventos analisados para melhorar o nível de segurança, mitigando e resolvendo os GAPS de segurança.

> Monitoramento de disponibilidade dos ativos: para identificar rapidamente as indisponibilidades, entender a causa raíz dos problemas e resolvê-los.

> Análise SWOT com todas as fraquezas e ameaças: para que sejam analisadas pela equipe de segurança do Comitê.

> Análise da superfice de exposição do Comitê: para mitigação e resolução das vulnerabilidades do ambiente.

Sobre a Real Protect

A Real Protect é referência nacional em Segurança da Informação, auxiliando empresas a conectar em a SI ao negócio, reduzindo riscos e otimizando seus investimentos em segurança. Há mais de 10 anos no mercado prestando serviços com o mais alto nível de excelência, a Real Protect foi a primeira empresa na América Latina a obter a certicação UCS da MSP Alliance.