PRÉMIOS DE SEGURANÇA

SECURITY MAGAZINE | REVISTA DOS PROFISSIONAIS DE SEGURANÇA

Endurance Command Center – ECC VisionWare | Um exército de defesa digital contra ciberameaças

VisionWare

A plataforma Endurance Command Center (ECC) representa uma nova geração de soluções de ciberdefesa, desenvolvida no âmbito do serviço SOCaaS (Security Operations Center as a service) da VisionWare, concebida para responder aos desafios crescentes da cibersegurança moderna através de uma abordagem integrada, inteligente e orientada ao cliente. O ecossistema Endurance Command Center (ECC) contempla diferentes componentes tecnológicos, e num contexto em que as ciberameaças evoluem de forma cada vez mais rápida e automatizada, o ECC destaca-se como uma plataforma unificada de defesa contra ameaças avançadas. Um dos principais fatores diferenciadores da plataforma é a integração, num único ecossistema, de capacidades que habitualmente se encontram distribuídas por múltiplas ferramentas.

O ECC combina ingestão e correlação de eventos, analítica comportamental, monitorização de rede, monitorização de sistemas e mecanismos de automação e orquestração de resposta a incidentes, oferecendo uma visão holística da postura de segurança das organizações e reduzindo lacunas de visibilidade. Esta abordagem elimina uma das principais barreiras das soluções tradicionais do mercado e democratiza o acesso a tecnologias avançadas de ciberdefesa, proporcionando uma relação custo-benefício altamente competitiva. A plataforma integra ainda mecanismos avançados de deteção baseados em Machine Learning (ML) e Artificial Intelligence (AI), capazes de identificar padrões de comportamento e detetar desvios que possam indicar atividades maliciosas, incluindo ameaças emergentes. Complementarmente, a automação da resposta a incidentes permite acelerar a mitigação de ataques e reduzir significativamente o tempo entre a deteção e a contenção de uma ameaça. A experiência do cliente constitui também um dos pilares do ECC.

A plataforma disponibiliza um portal dedicado que oferece visibilidade total sobre alertas e incidentes, permitindo acompanhar o seu estado, consultar informação detalhada, interagir diretamente com os analistas do SOC e aprovar ações de remediação. Os dashboards são interativos e totalmente personalizáveis, adaptando-se aos diferentes níveis de maturidade e decisão dentro das organizações, facilitando a interpretação da informação e o apoio à tomada de decisão.

A plataforma centraliza num único ambiente tecnológico e em tempo real, as capacidades de comunicação, monitorização, deteção e resposta a incidentes de segurança, permitindo às organizações proteger os seus ativos digitais com maior visibilidade, eficiência e rapidez de reação. A plataforma integra mecanismos avançados de deteção baseados em Machine Learning (ML) e Artificial Intelligence (AI), capazes de identificar padrões de comportamento e detetar desvios que possam indicar atividades maliciosas, incluindo ameaças emergentes. É totalmente monitorizada pela VisionWare e suas equipas, sem necessidade de recorrer a outros fornecedores/parceiros externos, facto que acelera ainda mais o tempo de resposta e reacção.

Esta plataforma centraliza a comunicação num único painel e assegura um serviço de monitorização e resposta a incidentes em regime 24x7, suportado por equipas especializadas responsáveis por acompanhar

as organizações ao longo de todo o ciclo do serviço e garantir elevados padrões de qualidade e melhoria contínua. Combinando inovação tecnológica, automação inteligente e uma experiência centrada no cliente, o ECC representa uma nova geração de plataformas de ciberdefesa, permitindo às organizações reforçar a sua resiliência digital e enfrentar com confiança os desafios do panorama atual de ciberameaças.

A inovação da solução ECC diferencia-se de forma sustentada face às soluções disponíveis no mercado sobretudo pela sua abordagem integrada, flexibilidade operacional e custo sustentável. Enquanto a maioria das soluções comerciais posiciona as capacidades de SOAR como complementares e dependentes de SIEM e UEBA, implicando múltiplos licenciamentos e elevados custos de implementação e operação, o Endurance integra nativamente estas funcionalidades numa única plataforma. Esta abordagem reduz o custo total de entrada e utilização, removendo barreiras que excluem organizações de menor dimensão, mas com relevância estratégica e elevado impacto potencial em caso de incidente de segurança disruptivo a nível nacional ou internacional. Num mercado onde se observa uma crescente desagregação entre soluções de Network Detection & Response (NDR) e plataformas SIEM/SOAR, o Endurance destaca-se por fornecer uma visão unificada da superfície de ataque, incluindo ambientes híbridos IT/OT. Esta capacidade é muito relevante em contextos críticos onde a instalação de agentes não é possível, assegurando monitorização contínua e eficaz sem comprometer a operação.

Destaca-se ainda a sua escalabilidade diferenciadora, permitindo a ingestão e análise de grandes volumes de eventos de segurança, sem limites ao número de ativos monitorizados, integrando-se nativamente com múltiplas plataformas e sistemas terceiros.Transforma ainda dados massivos em inteligência acionável através de feeds globais de Cyber Threat Intelligence. Esta é uma solução que ultrapassa o modelo tradicional ao agregar numa única solução componentes adicionais como SIEM, SOAR, Gestão de Vulnerabilidades e EDRaaS, consolidando todas as capacidades essenciais de defesa cibernética numa plataforma única, inovadora e adaptada às necessidades reais das organizações modernas.

Em termos de tecnologia esteve envolvido: » Security Information and Event Management (SIEM): responsável pela ingestão de toda a informação de segurança da organização e utilizando analítica avançado possibilitar a deteção de comportamento malicioso na organização; » User and Entity Behaviour Analytics (UEBA): tecnologia de analítica avançada capaz de detetar o comportamento normal de entidades da organização utilizando técnicas de Machine Learning (ML) e Artificial Intelligence (AI) de forma a detetar desvios comportamentais que possam indicar a ocorrência de incidentes de segurança; » Security Orchestration, Automation and Response (SOAR): Tecnologia capaz de coordenar uma resposta totalmente automática em caso de incidente de segurança, de forma a mitigar eficazmente possíveis danos causados e bloquear ações maliciosas. Esta componente diminui substancialmente o tempo entre a deteção e a mitigação; » Network Detection & Response (NDR): Tecnologia de análise de comunicações de rede com capacidade de detetar comunicações maliciosas e efetuar um bloqueio preventivo das comunicações. » IT Monitoring (ITM): Tecnologia responsável pela monitorização da disponibilidade dos sistemas internos da organização no que respeita a sua disponibilidade e normal operação dos serviços disponibilizados; » Customer Engagement (CE): Tecnologia de comunicação com o cliente onde se inclui portal de cliente, integrações das plataformas de ITSM e múltiplos canais de comunicação: exs. - Email, Microsoft Teams, Slack, Telegram, etc.

Nota: A informação contida neste documento destina-se exclusivamente à divulgação dos Prémios de Segurança da Security Magazine. Qualquer utilização para outros fins requer autorização prévia da Security Magazine e dos respetivos intervenientes.