PRÉMIOS DE SEGURANÇA

SECURITY MAGAZINE | REVISTA DOS PROFISSIONAIS DE SEGURANÇA

Viriatus

Cybersec

O VIRIATUS disponibiliza um conjunto integrado de funcionalidades avançadas de cibersegurança que permitem às organizações obter uma visão contínua, centralizada e acionável do seu estado de segurança. A plataforma realiza recolha e ingestão de dados em tempo real a partir de múltiplas fontes, incluindo firewalls, endpoints, sistemas de deteção, ferramentas de vulnerabilidades e fontes externas de threat intelligence (OSINT). Estes dados são normalizados e correlacionados automaticamente, permitindo identificar padrões de comportamento suspeito e potenciais incidentes de segurança. Ao nível da monitorização e deteção, o VIRIATUS integra capacidades de análise contínua de eventos (SIEM), com geração de alertas inteligentes e priorização baseada em risco, reduzindo significativamente o ruído e permitindo foco nos eventos críticos. Inclui ainda funcionalidades de gestão de vulnerabilidades, permitindo identificar, classificar e acompanhar falhas de segurança em ativos internos e externos, bem como mecanismos de análise da superfície de exposição externa (Attack Surface Management), identificando ativos expostos, subdomínios, serviços e potenciais vetores de ataque. A plataforma incorpora mecanismos de automação e inteligência artificial, que suportam a triagem de alertas, a correlação de eventos e a recomendação de ações, acelerando o processo de resposta a incidentes e reduzindo a dependência de intervenção manual.

No domínio da integração, o VIRIATUS é agnóstico a fornecedores, permitindo ligação a múltiplas tecnologias já existentes nas organizações, potenciando o aproveitamento dos investimentos realizados e eliminando silos operacionais. Adicionalmente, disponibiliza dashboards e relatórios em tempo real, que fornecem uma visão clara da postura de segurança, indicadores de risco e nível de exposição, suportando decisões informadas ao nível técnico e de gestão. A plataforma encontra-se totalmente alojada em território europeu, assegurando conformidade com requisitos de soberania de dados e enquadramentos regulatórios como o RGPD, NIS2 e DORA. No seu conjunto, estas funcionalidades permitem não apenas detetar e responder a incidentes, mas sobretudo antecipar riscos, reduzir a superfície de ataque e operacionalizar uma abordagem contínua e proativa à cibersegurança.

O desenvolvimento do VIRIATUS nasce de uma falha estrutural no modelo atual de cibersegurança: as organizações continuam a operar com abordagens fragmentadas, reativas e incapazes de acompanhar a velocidade e sofisticação das ameaças modernas. Apesar do investimento crescente em tecnologia, a realidade é que a maioria das empresas continua sem uma visão integrada do seu estado de segurança. Ferramentas isoladas geram volumes massivos de dados e alertas, mas sem contexto, correlação ou capacidade de ação em tempo útil.

O resultado é um paradoxo crítico: mais tecnologia, mas menor controlo efetivo. A este cenário soma-se a escassez global de talento especializado em cibersegurança, que limita a capacidade operacional das equipas e torna insustentável um modelo dependente de análise manual e intervenção constante. Simultaneamente, o novo enquadramento regulatório europeu, com destaque para a Diretiva NIS2 e o regulamento DORA, veio exigir às organizações um nível de maturidade, monitorização contínua e

capacidade de resposta que a maioria não consegue atualmente garantir. Perante este contexto, tornou-se evidente que não bastava evoluir as ferramentas existentes — era necessário redefinir o modelo. O VIRIATUS foi desenvolvido para responder a esta disrupção, introduzindo uma abordagem contínua, autónoma e orientada ao risco, que elimina silos tecnológicos, reduz a dependência de intervenção humana e transforma dados dispersos em inteligência acionável em tempo real. Mais do que resolver um problema tecnológico, o VIRIATUS responde a uma necessidade estrutural do mercado: permitir às organizações recuperar controlo, antecipar ameaças e operar com confiança num ambiente digital cada vez mais hostil e exigente.

A implementação do VIRIATUS tem demonstrado resultados consistentes, tanto ao nível quantitativo como qualitativo, evidenciando o seu impacto real na melhoria da postura de cibersegurança das organizações. Do ponto de vista quantitativo, destaca-se: Redução significativa do tempo de deteção e resposta a incidentes (MTTD/MTTR), com melhorias que podem ultrapassar 50%, resultado da correlação automática de eventos e priorização baseada em risco; Diminuição do volume de alertas irrelevantes, através de mecanismos de filtragem e inteligência aplicada, permitindo reduções superiores a 60% no ruído operacional; Aumento da visibilidade sobre ativos e superfície de ataque, com identificação de novos ativos expostos e vulnerabilidades críticas que anteriormente não eram monitorizadas; Crescimento sustentado da adoção, com mais de 40 organizações a utilizar a plataforma desde o início da sua comercialização em 2025 e uma taxa de crescimento superior a 100%. Ao nível qualitativo, os resultados são igualmente relevantes: Melhoria significativa na capacidade de decisão, através de dashboards e indicadores de risco claros e acionáveis; Evolução de um modelo reativo para uma abordagem proativa, com identificação antecipada de riscos e vulnerabilidades; Maior eficiência operacional das equipas de segurança, reduzindo a dependência de análise manual e libertando recursos para tarefas de maior valor; Melhor alinhamento com requisitos regulatórios, nomeadamente NIS2 e DORA, facilitando processos de auditoria e reporting; Aumento da confiança organizacional, permitindo às empresas operar com maior segurança e controlo sobre os seus ativos digitais. Estes resultados refletem não apenas ganhos operacionais, mas uma transformação estrutural na forma como a cibersegurança é gerida, posicionando o VIRIATUS como um facilitador de maturidade e resiliência digital nas organizações onde é implementado.

O VIRIATUS diferencia-se das soluções existentes no mercado por não ser apenas mais uma ferramenta de cibersegurança, mas sim uma plataforma integrada que redefine a forma como a segurança é operacionalizada nas organizações. Enquanto a maioria das soluções atua de forma isolada — focando-se em áreas específicas como SIEM, gestão de vulnerabilidades ou monitorização — o VIRIATUS agrega estas capacidades numa abordagem unificada, eliminando silos tecnológicos e permitindo uma visão contínua e correlacionada de toda a superfície de risco, interna e externa.

Adicionalmente, ao contrário das soluções tradicionais que dependem fortemente de intervenção manual e equipas altamente especializadas, o VIRIATUS incorpora mecanismos de automação e inteligência artificial que permitem priorizar riscos, reduzir ruído e acelerar a resposta a incidentes de forma significativa. Esta abordagem torna a cibersegurança mais eficiente e acessível, mitigando o impacto da escassez de talento no setor. Outro fator diferenciador é a sua orientação nativa para os desafios regulatórios europeus, nomeadamente NIS2 e DORA, permitindo às organizações não só melhorar a sua segurança, mas também estruturar processos e evidências de conformidade de forma contínua. Por fim, destaca-se o facto de ser uma solução desenvolvida com engenharia portuguesa e totalmente alojada em território europeu, assegurando soberania de dados e alinhamento com os requisitos legais e estratégicos da União Europeia

— um aspeto cada vez mais crítico face à dependência de tecnologias externas. Em conjunto, estes elementos posicionam o VIRIATUS não como uma evolução incremental, mas como uma abordagem distinta e mais eficaz à cibersegurança, centrada na integração, automação e controlo contínuo do risco.

O VIRIATUS apresenta um elevado grau de sofisticação tecnológica, resultante da convergência de cibersegurança, data engineering, sistemas distribuídos e machine learning aplicado. A plataforma suporta ingestão contínua de dados em larga escala (high-throughput pipelines) provenientes de múltiplas fontes heterogéneas, incluindo logs de rede, endpoints, APIs de segurança e feeds de threat intelligence. Estes dados são sujeitos a processos de normalização, enriquecimento e indexação em tempo real, sendo posteriormente analisados através de mecanismos de correlação multi-dimensional e análise comportamental, permitindo identificar padrões anómalos e cadeias de ataque complexas. Integra modelos de machine learning e heurísticas avançadas para classificação de eventos, redução de falsos positivos e priorização dinâmica baseada em risco contextual, recorrendo a técnicas de feature extraction sobre dados estruturados e não estruturados.

A arquitetura é baseada em microserviços e processamento distribuído, garantindo escalabilidade horizontal, resiliência e baixa latência. Inclui ainda capacidades de automação tipo SOAR, com orquestração de respostas, playbooks automatizados e triagem inteligente de alertas. Complementarmente, incorpora funcionalidades de Attack Surface Management, com discovery contínuo e análise de exposição externa. A plataforma é desenvolvida segundo princípios de secure-by-design e compliance-by-design, operando integralmente em infraestrutura europeia.

A fase de testes piloto do VIRIATUS foi conduzida em Portugal, em colaboração com várias organizações clientes da CYBERS3C, em diferentes setores de atividade, permitindo validar a solução em contextos reais e heterogéneos. Durante este período, com uma duração aproximada de 6 a 9 meses, foram atingidas metas críticas para a maturação da plataforma, nomeadamente: Validação da integração com múltiplos sistemas e tecnologias (multi-vendor); Teste da capacidade de ingestão e correlação de grandes volumes de dados em tempo real; Afinação dos modelos de priorização de risco e redução de falsos positivos; Avaliação da eficácia dos mecanismos de deteção e resposta a incidentes; Validação da usabilidade e relevância operacional junto de equipas de segurança; Teste da capacidade de identificação de ativos expostos e vulnerabilidades na superfície externa. Este processo permitiu não só validar a robustez técnica da solução, mas também ajustar a plataforma às necessidades reais das organizações, garantindo alinhamento com desafios operacionais e requisitos regulatórios como a NIS2. Como resultado, o VIRIATUS evoluiu de um conceito tecnológico para uma solução validada em produção, com impacto direto na melhoria da visibilidade, redução do risco e aumento da eficiência operacional das equipas de cibersegurança.