|  |  |
| --- | --- |
| Seguradorax, the oldest and most mature of the UEBA vendors (founded in 2008), offers UEBA solutions, structured as two platforms and multiple modules. | A Seguradorax, a mais antiga e experiente das empresas fornecedoras de UEBA (fundada em 2008), oferece soluções UEBA estruturadas em duas plataformas e múltiplos módulos. |
| Providing Additional Context and Information for Investigations | Fornecimento de Contexto e Informações Adicionais para Investigações |
| NICHE PLAYERS | AGENTES DE NICHOS |
| Performing deep custom application monitoring and analytics | Execução de monitoramento e análise profundos de aplicativos personalizados |
| Identifying account compromise | Identificação de comprometimento da conta |
| Securadoraxreports having more than 150 production customers as of early 2017. | A Seguradorax informa ter mais de 150 clientes de produção a partir do início de 2017. |
| On the other hand, customers report that professionalservices and customizations are highly advisable (if not truly mandatory) for a successful deployment. | Por outro lado, os clientes relatam que os serviços profissionais e as personalizações são altamente recomendáveis (se não realmente obrigatórios) para uma implantação bem-sucedida. |
| Seguradorax also retains some focus on IdM and access management use cases, but these are not discussed in this document. | A Seguradorax também observa casos de uso de gerenciamento de acesso e IdM, mas eles não são discutidos neste documento. |
| Seguradorax has recently made forays into broader security monitoring use cases (Securonix SNYPR can operate without and sometimes instead of a SIEM) and into deeper vertical and industry- speciﬁc applications (such as for healthcare application monitoring and ﬁnancial fraud detection). | Recentemente, a Seguradorax fez incursões em casos de uso de monitoramento de segurança mais amplos (o Securadorax SNYPR pode operar sem um SIEM e, às vezes, em seu lugar) e em aplicativos verticais e industriais mais específicos (como monitoramento de aplicativos de assistência médica e detecção de fraude financeira). |
| Identifying account compromise | Identificação de comprometimento da conta |
| The vendor is experimenting with the use of deep learning for security use cases. | O fornecedorestá experimentando a utilização de aprendizagem profunda para casos de uso de segurança. |
| Security Management Framework For The New IT Landscape | Estrutura de Gerenciamento de Segurança para o Novo Cenário de TI |
| But legacy SIEMs and are ill-equipped to handle the volume and complexity described above. | Mas SIEMs legados estão mal equipados para lidar com o volume e a complexidade descritos acima. |
| A new gen SIEM platform must provide content that is pre-packaged with the solution and dynamic to adjust to the realities of today’s cyber threats. | Uma plataforma SIEM de nova geração deve fornecer conteúdo pré-empacotado com a solução e também dinâmico para adaptar-se às realidades das ameaças cibernéticas de hoje. |
| Enabling Rapid Incident Response | Possibilidade de Resposta Rápida a Incidentes |
| Identifying threats only part of the work, responding to threats rapidly is critical. | Identificação de ameaças é apenas parte do trabalho, responder rapidamente às ameaças é fundamental. |
| Graphical user interface with ability to pivot on any entity and drill-down to perform rapid root cause analysis | Interface gráfica do usuário com capacidade de pivotear sobre qualquer entidade e busca detalhada para realizar análise rápida de causa na raiz |
| Seguradorax UEBA is delivered as purpose-built appliances, enterprise software, virtual machine images, or as a no-hardware, partially or fully managed cloud solution. | A Seguradorax UEBA é entregue como dispositivos criados para uso específico, software empresarial, imagens de máquinas virtuais ou como uma solução de nuvem sem hardware, parcialmente ou totalmente gerenciada. |
| Built in playbooks for incident response. | Playbooks integrados para resposta a incidentes. |