INTRODUÇÃO DO CODE42 INCYDR

Deteção de risco de dados e Resposta a Ameaças Internas

O produto Incydr SaaS protege todos os seus IPs e ficheiros, tal como o código fonte, as listas de clientes e roadmaps sem sobrecarregar as equipas de segurança ou inibir a produtividade dos empregados. Com uma simplicidade, sinal e velocidade incomparáveis, o Incydr reúne três dimensões de risco para detetar e responder com rapidez e precisão a ameaças internas.

FICHEIRO

- Monitoriza todos os ficheiros - não apenas aqueles que foram marcados como sensíveis;
- Oferece dados metadata tais como o nome do ficheiro, a quem pertence, tamanho, localização, categoria e hash
- Fornece aos analistas de segurança a capacidade de rever o conteúdo de um ficheiro

VETOR

- Deteta a exposição e exfiltração, incluindo os uploads por web browser, sincronização de ficheiros para a Cloud, partilha de ficheiros, Airdrop e armazenamento amovível.
- Filtra eventos de ficheiros que refletem o que é considerado atividade confiável e não confiável
- Fornece detalhes do vetor tais como o nome de utilizador, nome do domínio, titulo e URL do tabulador do browser, marca, modelo nome do volume, ID da partição e número de série do armazenamento amovível.

UTILIZADOR

- Permite às equipas de segurança para programaticamente monitorizar utilizadores com fatores de risco mais elevados, tais como colaboradores que irão sair ou a contrato a termo.
- Identifica comportamentos de risco como atividades remotas, eventos em ficheiros fora das horas de trabalho normal e tentativas para ocultar exfiltrações
- Fornece 90 dias de histórico dos utilizadores para permitir encontrar patrões e anomalias de comportamento.

Maior colaboração, maior risco interno.

As organizações estão a mover-se mais depressa do que nunca. É criado um novo IP a cada segundo, na cloud, utilizando ferramentas de colaboração. Os colaboradores estão a ser integrados e habilitados cada vez mais a mundo remoto. A sua equipa de segurança precisa de acompanhar estes riscos, ao mesmo tempo que se mantém em conformidade. Ferramentas de segurança como DLP, UEBA e CASB normalmente abordam uma única dimensão de risco, demoram meses a implementar, e sobrecarregam as equipas de segurança com a constante sintonia fine-tuning. Está na altura de adpatar o seu negócio a uma nova abordagem para gerir e mitigar o risco de dados provenientes de ameaças internas.

89% dos CISOs acreditam que uma cultura de colaboração a um ritmo acelerado cria um grande risco.

66% das violações de dados envolvem um informador interno.

69% das organizações violadas por ameaças internas tinham uma solução DLP em vigor.

– Code42 Data Exposure Report

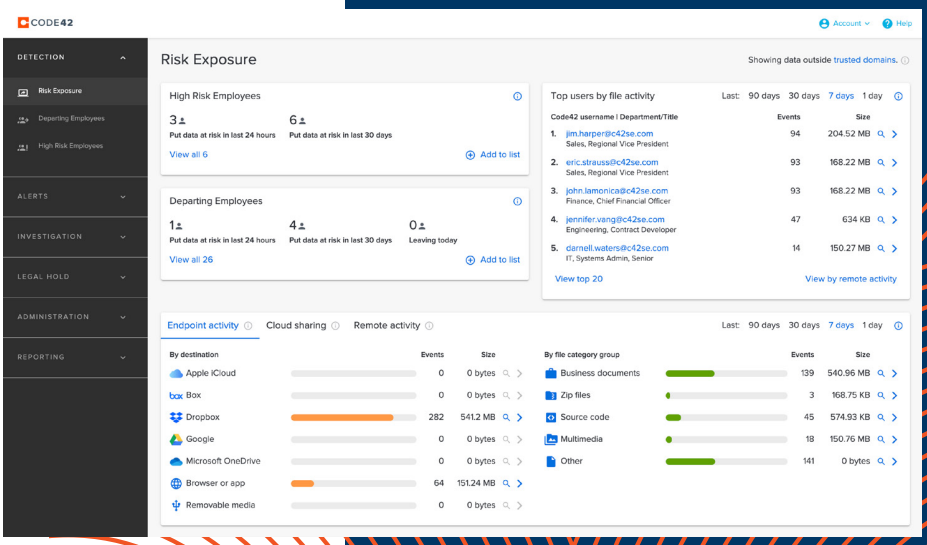
O INCYDR monitoriza o movimento e a partilha de ficheiros entre os computadores, Cloud e email utilizando um agente e integrações diretas.

INCYDR

Deteção: mostra o risco a que estão expostos os dados, usando dashboards e alertas

Investigação: simplifica as investigações aos riscos internos através da criação de perfils de utilizador e procuras forenses

Response: compila, documenta e dissemina provas. Remedia riscos com SOAR playbooks (Security Orchestration and Automation Solution), treino dos utilizadores, ações legais e outros.



CODE42 QUICK FACTS

Founded in 2001

Locations:

Minneapolis (HQ) | Denver
Washington, DC | London

Trusted by:

Customers include leading security brands such as CrowdStrike, Splunk, Ping Identity, Palantir and Okta.

6 of **10** of the largest tech companies

13 of the worlds most valuable brands

7 of **8** Ivy League schools

IMPLEMENTAÇÃO RÁPIDA E FÁCIL

- Cloud-based
- Mac, Windows e Linux
- 2-tempo médio de implementação de uma semana
- 230% ROI em 3 anos
- Apoio ao cliente baseado nos EUA e no Reino Unido

O QUE DIZEM OS NOSSOS CLIENTES

"If it wasn't for the Code42 ability to actually see the files, we wouldn't really understand what the person is doing... It provides us both speed and thoroughness of investigations."

– Tim Briggs, Director of Incident Response and eDiscovery at CrowdStrike

"It's crucial that we are able to detect and respond if employees are transferring data to personal accounts, or publicly sharing documents, especially when they depart. The Code42-Box integration gives us quick visibility into what is shared outside of our domain."

– Mark Campbell, Senior Director at Xactly

"Code42 is the only solution we have found that gives us the visibility we need to understand where data is moving, while still letting our team work how – and where – they need to."

– Dustin Fritz, Sr. Security Architect at UserTesting

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (PO2009201)