解决方案简介
智能学习风险行为分析与SIEM

Datiphy的分析引擎弥补现有SIEM方案的不足。

有SIEM工具和日志管理系统的企业可以利用Datiphy的扫描引擎,大幅度提高敏感数据的可视性。

在市面场上有许多资安产品是透过检测大量的日志来识别威胁,Splunk就是其中的一种。随着Datiphy DDNA 分析引擎的发明,其审计能力能够在日志流运用,因此安全分析师对数据库事件的掌握能达到前所未有的广度,深度和细度。

Splunk	Datiphy + Splunk
SYS logs from applications	Database logs directly from databases
Indexing of events	Indexing of events and risk metrics
Network feeds: message queues, change monitoring, etc.	Data-centric feeds: SQLi, access privilege, data integrity
Data sources: active directory, MS Windows event logs	Data sources: databases, big data, and active directory
Requires add-ons and plug-ins	Agents and taps talk directly to the database

- 依赖现有日志整合技术,提高数据库活动可见性
- Datiphy的安全事件能简易的整合入Splunk以及SIEM监控工具
- 发现风险度量,资产清单,敏感数据元素,和用户访问
- 所实施的即时检测可以直接针对数据本身,而不仅是网路封包或是事件日志。
- Datiphy制成的审计报表是以自然语言表示,可以直接送给审计人员和数据库管理员,不需要透过资讯人员翻译整理。

专利认证的智能行为风险分析引擎

Datiphy的扫描引擎会考虑到访问异常,漏洞和威胁等不同层面的安全问题,为企业做整体的风险评分。安全分析师和审计师（内部和外部）均可以利用Datiphy生成的报表做出一个全面的计划来控制和减轻数据外泄的损失。Datiphy的专利技术是属於非侵入性的,企业可以事制定一个行为模式,在黑客有意图攻击敏感数据之前,Datiphy的智慧行为模式技术就能立即判别出可疑的行动并通知相关人员采取因应措施。检测威胁是必要的,但是知道敏感数据所在并事先做保护才能真正确保数据的安全。请试用Datiphy的风险评估扫描以检视企业的最大安全隐患之所在。

DATIPHY简介

Datiphy解决方案填补了单点式数据安全解决方案的缺点。他有效的整合了各种数据安全保护功能，让企业能够清楚的看到数据生命周期的各阶段。Datiphy的关键技术是其智慧学习数据行为模式TM（也称为DatiDNATM），能够实时分析整个数据池的数据，在事件发生时，立即提供有效的对策以保护数据安全。Datiphy 的集中管理架构和自然语言查询能够让用户在几秒钟内就能找到任何一笔想要查询的数据资产，并看到每一笔资产和其他资产之间的互动和关系。

ADDRESS
2290 N. First Street, Suite 204
San Jose, CA 95131

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938