imperva

CAPABILITY BRIEF

Data Risk Analytics

Spot risks before they become breaches

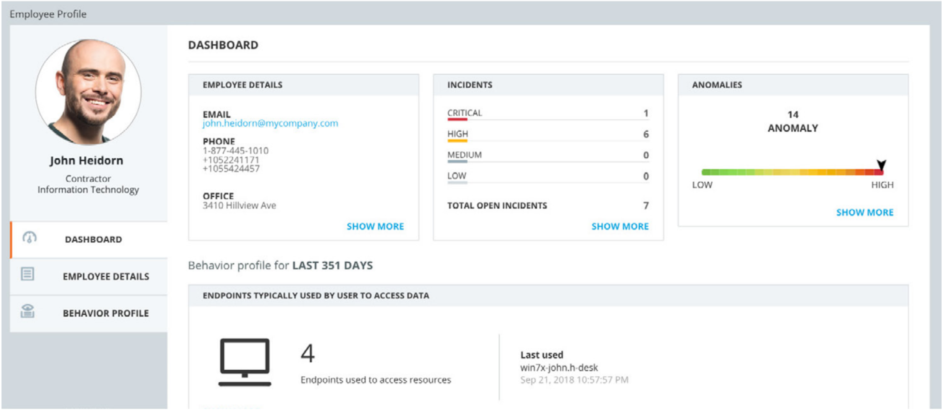
Data is a critical business asset that must be protected. It can be a daunting task for Enterprise security groups with limited resources and tools.

Ironically, many security tools are sometimes part of the problem. Security staff are often overwhelmed by an avalanche of security tool alerts, many of which are false positives, making it hard to know what to do or where to even begin.

To more effectively mitigate data risk, organizations need advanced security analytics, that help security staff gain actionable insights to threats and accelerate breach detection.

Data Risk Analytics

Data Risk Analytics, a key feature for Imperva Database Security, provides security insights that can be immediately acted on. Unlike typical user behavior analytics tools, Imperva data risk analytics creates a contextual behavior baseline by analyzing both user behavior and data access activities. By learning and correlating data details like what sensitive data has been touched, by whom and when, and how data is used and accessed, Imperva data risk analytics can accurately identify critical threats to the data and eliminate false positive anomalies. It cuts through the noise, and prioritizes only the few high-risk incidents that require immediate investigation, allowing security teams to stay focused and contain a potential threat more effectively.



John Heidorn
Contractor
Information Technology

DASHBOARD

EMPLOYEE DETAILS

EMAIL
john.heidorn@mycompany.com

PHONE
1-877-445-1010
+1052241171
+1055424457

OFFICE
3410 Hillview Ave

INCIDENTS	
CRITICAL	1
HIGH	6
MEDIUM	0
LOW	0
TOTAL OPEN INCIDENTS	7

ANOMALIES
14
ANOMALY

Behavior profile for **LAST 351 DAYS**

ENDPOINTS TYPICALLY USED BY USER TO ACCESS DATA

4
Endpoints used to access resources

Last used
win7x-john.h-desk
Sep 21, 2018 10:57:57 PM

Figure 1: The dashboard provides the visibility security team needs to investigate suspicious user data access that could indicate a data breach.

KEY CAPABILITIES:

Detects critical incidents among billions of audit events using machine-learning

Peer group analysis that uncovers suspicious user data access

Provides actionable insights in plain language

Executive dashboard that helps accelerate threat investigation and response

Out-of-the-box analytics with minimal tuning required

Actionable insights that make staff more effective

Pinpoint risk to your data enterprise-wide

To mitigate the risk of a data breach enterprise-wide, you need to be able to detect and pinpoint threats to your data across all your sensitive databases. Data risk analytics utilizes machine learning and behavior analytics to uncover suspicious data access and bad practices that other security analytics miss. It automatically processes massive amounts of database activity logs and correlates across them to surface related threats. Continuously learning the details of who the users are, how they typically access databases and use enterprise data, the analytics engine creates a contextual behavior baseline to help discern behaviors that are normal if you look at just one database log, from behavior that is not normal if you look at all the logs. This would be very hard for a human to do.

Prioritize what matters most

Data risk analytics prioritizes critical incidents by applying grouping and scoring algorithms. Each incident is assigned a risk score based on a sophisticated algorithm that factors in various variables, such as amount of sensitive data, privileged account, prevalence and more. If the incidents are related (e.g. they are all associated with the same user account or multiple users are abusing the same service account), they will be grouped into one issue. As a result, only few high-risk incidents are bubbled up and far less alerts get sent to your SIEM.

Accelerate and streamline incident response

Investigating data threats often requires deep database knowledge to know if any sensitive data has been misused or if users are accessing data inappropriately. Data risk analytics interprets security incidents in plain language and provides actionable insights and risk context, so security professionals can quickly understand what happened to the data environment and respond to threats even with little to no database knowledge. While the dashboard is intuitive and easy-to-consume, it contains all the visibility and information a security professional needs to carry out an investigation.

Summary

Data risk analytics is a key component of Imperva Database Security. It helps security teams detect and pinpoint critical threats to your data, prioritizes what matters most, and provides actionable insights allowing you to accelerate threat investigation and response. You can start seeing the benefits and changes in weeks, not months. Imperva Data Risk Analytics helps you spot and mitigate data breach risks before they become damaging incidents.

IMPERVA DATA SECURITY

Data Risk Analytics is a key component of Imperva Data Security, which reduces breach risk while enabling digital transformation. The solution safeguards data on-premises and in the cloud by:

Discovering sensitive data

Monitoring all data activity

Stopping unauthorized access and activity

Uncovering risky users and suspicious actions

Providing actionable security insights

Masking data for non-production use

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.