SECURE YOUR DATA FROM THE INSIDE OUT

THWART INSIDER THREATS WITH MACHINE LEARNING

Potentially the most lethal kind of threat to an organization's security, **insider threats** can pose risks as significant as—if not more than—external attacks. Because insiders are granted trusted access to sensitive data, these threats often fly under the security radar.

/ THREAT LEVEL /

INSIDER

Insiders don't need to break into your network—they're already in, with access to all your company's valuable data.

There are three types of insider threat profiles:

001 MALICIOUS USERS

Act out of malicious intent, stealing data such as intellectual property (IP) for economic gain

002 CARELESS USERS

Accidentally expose data, such as inadvertently sharing private health information

003 COMPROMISED USERS

Are victims of an outside attacker, whose credentials are stolen by attackers who then access sensitive data, such as employee records

By examining how users access your data and identifying when inappropriate or abusive access takes place, **machine learning** can help you secure your data from insider threats.

/ MACHINE LEARNING /

DEFINED

Machine learning is a type of artificial intelligence that enables computers to detect patterns and establish baseline behavior using algorithms that learn through training or observation.

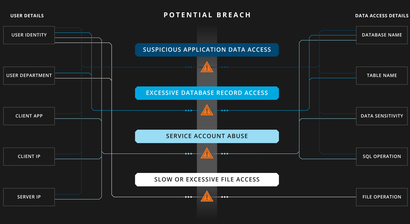
DO MACHINES DREAM OF INSIDER THREATS?

Machine learning is ideal for detecting insider threats. The vast amounts of data required to identify nuanced, out-of-baseline behavior are impractical for humans to process.

/ BASELINE BEHAVIOR /

ESTABLISHED

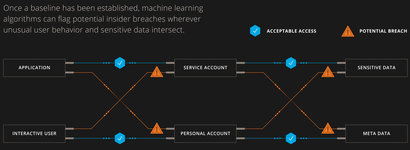
Data breaches occur at the intersection of users and data. Using granular details about how employees interact with data, machine learning algorithms can establish a baseline of typical user behavior across enterprise data stores, then ultimately detect potential breach scenarios.

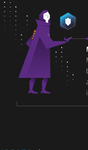


/ DATA BREACH /

DETECTED

Once a baseline has been established, machine learning algorithms can flag potential insider breaches wherever unusual user behavior and sensitive data intersect.





MACHINES, NOT MAGIC

Machine learning is only as good as the domain expertise behind the algorithms. Data security-specific knowledge and technology will more accurately find insiders that inappropriately access data.

/ INSIDER THREATS /

IDENTIFIED

By analyzing the actors, accounts, and data in the environment, machine learning can detect unusual data access behavior and immediately flag suspicious activity, including:

001

SERVICE ACCOUNT ABUSE

User logs into a database using a highly privileged service account.

002

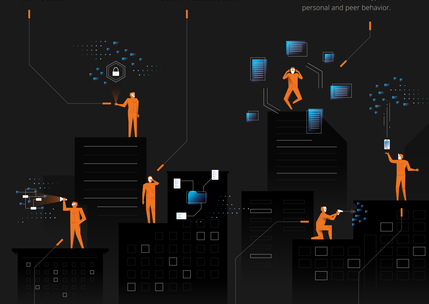
SUSPICIOUS APPLICATION DATA ACCESS

User directly accesses sensitive database data.

003

EXCESSIVE DATA ACCESS

User accesses an unusually high number of database records or files, as compared to typical personal and peer behavior.



004

SLOW RATE FILE ACCESS

User accesses or copies an abnormally high number of personal or departmental files from the network file share over the course of one day.

005

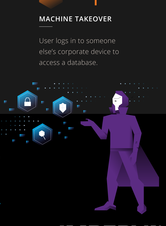
EXCESSIVE FAILED LOGINS

User fails to log in to multiple databases for a number of times.

006

MACHINE TAKEOVER

User logs in to someone else's corporate device to access a database.



Using algorithms to identify patterns and learn baseline behavior, Imperva CounterBreach machine learning technology can save your team time and keep your sensitive data more secure.

WE'LL KEEP AN EYE OUT FOR YOU.
Learn more at **imperva.com/products/breach-prevention**.

IMPERVA

*Insider Threat Study," 2016, Gatepoint Research/Imperva

CREATED BY COLUMN FIVE