THE CISO'S GUIDE

to Machine Learning & User and Entity Behavioral Analytics

SNEAK PEEK

aruba

a Hewlett Packard Enterprise company

SALLY | ENGINEER

logged into the source code repository at 10 pm last night and downloaded 500 Megabytes of data

JOE | ATTORNEY

logged into the network from San Francisco and New York—at the same time

PETE | ANALYST

is accessing a critical finance application that he has never used before

JOHN | SYS ADMIN

has been accessing the customer database after normal work hours every evening for the last two weeks

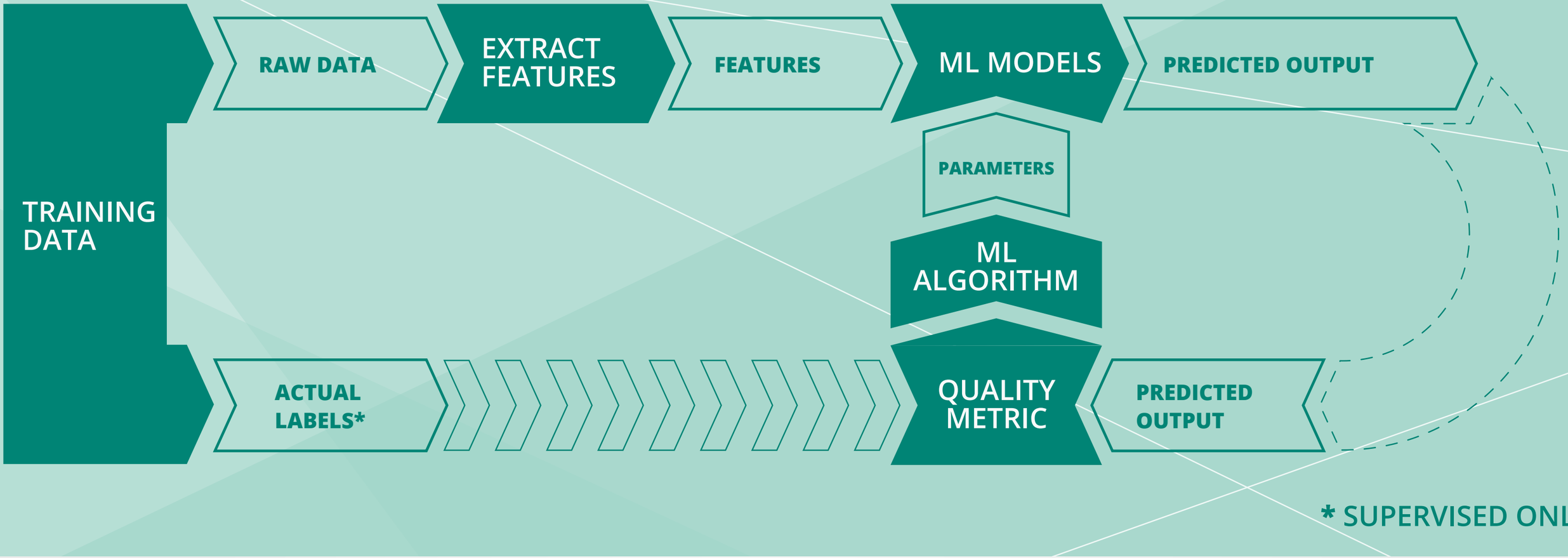
Are all of these legitimate scenarios or are they anomalous behaviors that threaten the brand, reputation and finances of your organization? Can your current security tools detect these types of threats? How will your staff respond? What else are they missing?

SNEAK PEEK

	TRAINING DATA	APPROACH	EXAMPLE MODEL TYPES	DETECTION TYPE & FOCUS	ATTACK STAGES	EXAMPLE USE CASES
UNSUPERVISED	Unlabeled	Training onsite Classification onsite	SVD K-means clustering Neural network	**TYPE** Anomaly **FOCUS** Unknown threats	Lateral movement Exfiltration	Abnormal server access, lateral attack spread, flight risk, data exfiltration etc.
SUPERVISED	Labeled	Training offsite Classification onsite	Naïve bayes Logistic regression SVM	**TYPE** Maliciousness **FOCUS** Known threats	Infection Command & control	Malicious object download, email phishing/spam, DNS DGA, etc.

Comparison of Supervised and Unsupervised Machine Learning

SNEAK PEEK



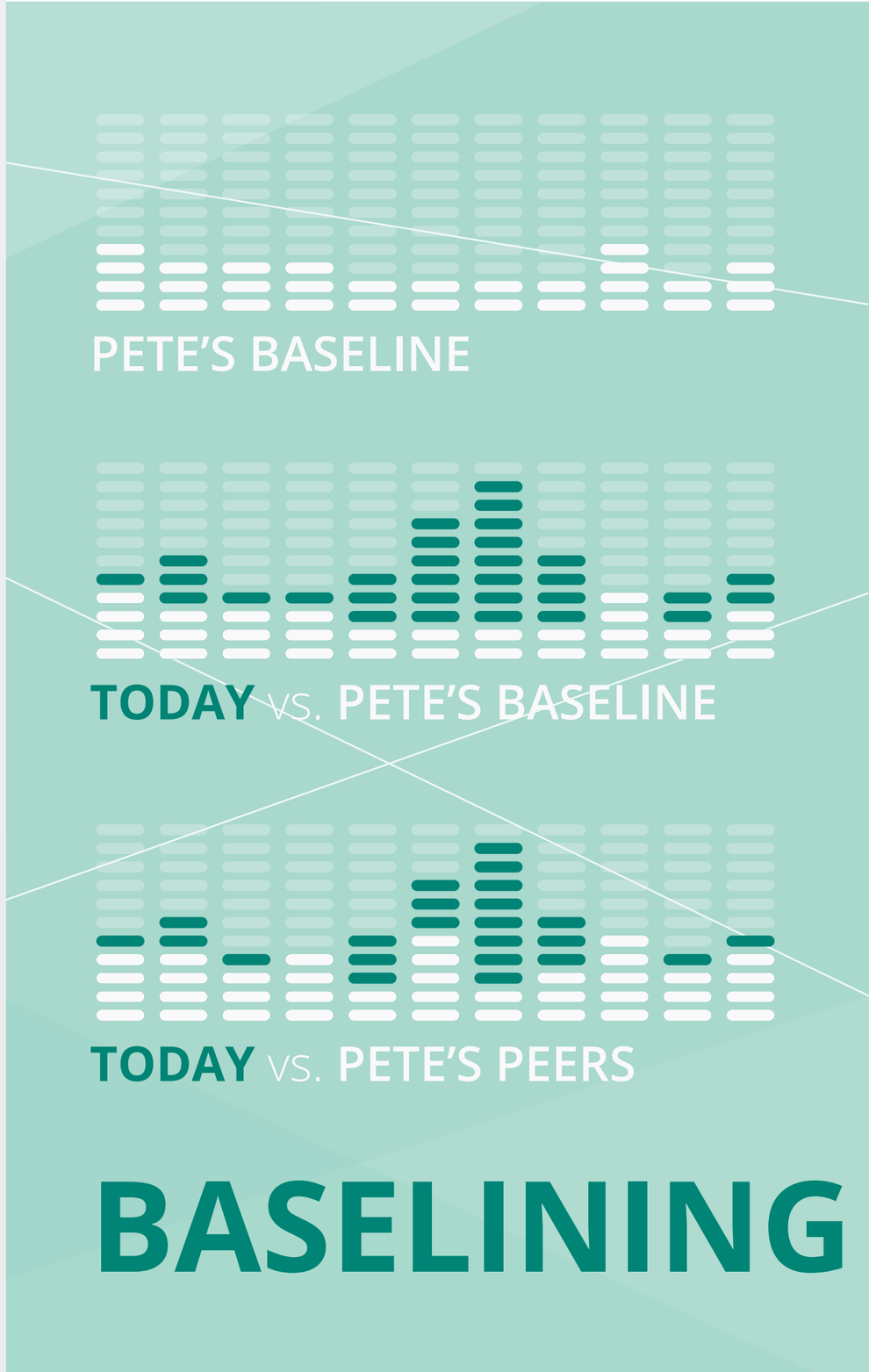
Machine Learning Architecture

SNEAK PEEK

Let's take a deeper look at how machine learning finds attacks that have **evaded other real time systems**.

Earlier, we described the example of Pete, the analyst who clicked on the wrong email attachment and had his credentials compromised and access stolen. Machine learning can detect **behavioral changes** against the backdrop of "normal" using probabilities to reflect the deviation from the norm. "Features" characterizing Pete's **use of IT resources** — such as systems and applications accessed, time and duration of access, and volume of activity; i.e. number of transactions, upload/download bytes etc. — can be utilized in an unsupervised ML model to build a baseline of his "normal" behavior. With this in place, access to systems that he has never accessed would be **flagged as anomalies**. Pete's behavior can also be compared to his peer group. If Pete is a financial analyst and the other analysts had not exhibited **comparable behavior,** his access patterns would stand out as abnormal.

SNEAK PEEK



If you find this interesting and would like to learn more about machine learning and behavior analytics, you can download the **full CISO Guide here.**

aruba
a Hewlett Packard Enterprise company

About Aruba IntroSpect
Aruba IntroSpect's security analytics platform automates the detection of attacks within organizations by applying advanced machine learning to network and security data. By combining big data technologies with machine intelligence and forensics, IntroSpect surfaces attacks that have evaded real-time defense systems and accurately discovers compromised users and malicious insiders, speeds threat hunting efforts, and reduces the time for incident investigation and response by focusing security teams on the threats that matter. For more information, visit www.arubanetworks.com. GUIDE_CisoSneakPeek_110917