exabeam PRODUCT ABOUT BLOG LIBRARY CONTACT GET A DEMO

Information Security Blog › Information Security › Understanding the Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cybersecurity

INFORMATION SECURITY MAY 18, 2018

Understanding the Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cybersecurity

DEREK LIN - CHIEF DATA SCIENTIST

SHARE

When it comes to artificial intelligence (AI) and machine learning (ML), there's no shortage of buzz and hype. Often referred to interchangeably, artificial intelligence and machine learning are part of our daily reality and technology lexicon—whether it's in a product marketing pitch or a Netflix recommendation for which movie to see.

AI, ML, and Deep Learning in Cybersecurity

In cybersecurity, as these and other emerging technologies like deep learning (DL) evolve, their capabilities have become a driving force shaping modern cybersecurity solutions. At the same time security practitioners, fatigued by the barrage of artificial intelligence and machine learning messaging, are raising suspicions about vendor claims.

At the recent InteropITX conference, panelists echoed the same sentiment about the hype, asking what can be legitimately claimed as artificial intelligence. The audience was encouraged to look beyond the marketing spin and find out what's really being offered.

I'm glad to see the hype cycle has reached its peak. It's a healthy sign that security practitioners are asking the right questions and demanding to know what constitutes reality.

In order to ask the right questions, let's start with a correct understanding of the terminology. Despite all the marketing messaging, for many of us it's not always clear what some terms mean.

Subscribe

Email address SUBMIT

TRENDING INFORMATION SECURITY ARTICLES

1 Understanding the Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cybersecurity

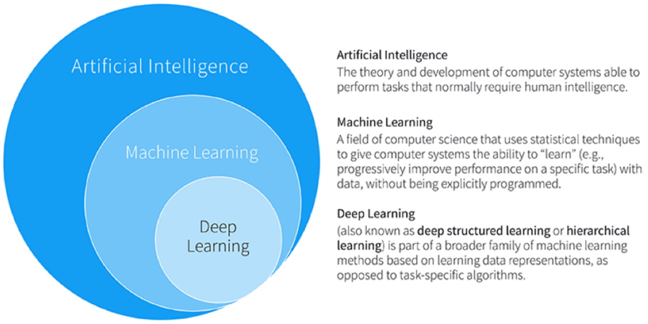
2 How Criminals Can Build a "Web Dossier" from Your Browser

3 GDPR and the Security Monitoring Challenge

4 Complying with NY State DFS Regulations with Exabeam

5 Extracting Actionable Information from Windows Events

TRENDING INFORMATION



Artificial Intelligence
The theory and development of computer systems able to perform tasks that normally require human intelligence.

Machine Learning
A field of computer science that uses statistical techniques to give computer systems the ability to "learn" (e.g., progressively improve performance on a specific task) with data, without being explicitly programmed.

Deep Learning
(also known as **deep structured learning** or **hierarchical learning**) is part of a broader family of machine learning methods based on learning data representations, as opposed to task-specific algorithms.

Figure 1: The relationship between artificial intelligence, machine learning, and deep learning

Artificial Intelligence

AI is often misunderstood, and not everyone agrees on what it means. The term artificial intelligence first appeared in the 1950s to describe systems comprising a set of human-defined, if/then decision rules—which have always been easily broken and hard to maintain.

For example, static correlation rules that raise alerts—used in traditional security information and event management (SIEM)—cannot learn and adapt. This results in a high number of false positives. Such AI systems appear to be intelligent in their decision-making because they make decisions. But in reality, they're 100% predetermined (based on static rules) and are drafted by humans.

But the word "intelligence" has stuck with the public since AI's introduction. Why not? It sounds cool. Yet today AI is often little more than a catchy marketing label, liberally applied to any system that performs tasks having some semblance of automated decision-making.

Contrast this with the modern Exabeam SIEM that dynamically learns from the behavioral patterns in data in order to make its decisions.

Machine Learning

Machine learning is often expressed in the same breath as AI. But machine learning is more specific. To learn from collected data, it uses algorithms for prediction, classification, and insight generation.

With machine learning, a formal body of methods are grounded in solid mathematical foundations. Applied to cybersecurity, the right problems must be matched with the right machine learning tools.

But not all problems require advanced machine learning tools. For example, some popular indicators used in user behavior analytics (UBA) are based on simple statistical analysis, such as p-value hypothesis testing used for rare event detection.

On the other hand, many cybersecurity problems cannot be solved without machine learning. Consider the phishing scam domain detection shown in Figure 2. Here, the URLs, WHOIS data, other properties, as wells as the known (legitimate or malicious) labels of URLs are examined in a supervised learning setting to predict whether a domain is malicious. It does so without resorting to conventional, but less effective, blacklist-based matching.

Incident Response Team

2 Insider Threats: How to Stop the Most Common and Damaging Security Risk You Face

3 2018 State of the SOC Report

4 5 Best Practices for Your Incident Response Plan

5 How Criminals Can Build a "Web Dossier" from Your Browser

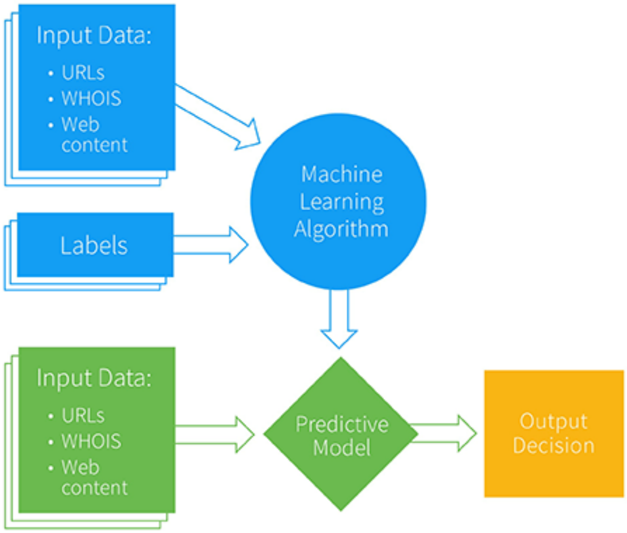


Figure 2: Supervised learning for phishing domain detection

Deep Learning

This is all the rage today. As with AI, deep learning evokes an air of sophistication, but it's also subject to misunderstandings. As a tool within machine learning, deep learning is highly dependent on matching the right problems to the right tools.

Deep learning applications are best suited in the image processing and natural language processing fields. In cybersecurity, it has found a home in packet stream and malware binary analysis. These benefit most from supervised learning, when labeled (i.e., legitimate vs. malicious) data is available.

But for insider threat detection, deep learning doesn't enjoy wide adoption for several technical reasons. One is the black box nature of the model, where it's impossible to explain the causes of the alerts. This renders investigations difficult.

Peer behind the messaging and examine what's under the hood

The cybersecurity marketplace is buzzing with AI and ML terminology. This isn't surprising, as data-driven approaches do lead to exciting applications that were never possible before. That said, it's all too easy to get confused—and lost in the hype.

Ask how are the problems or use cases being framed? Which analytical approaches are being used and why? Transparency and a thorough understanding of the terms and their use cases will help you demystify the hype.

#DATA SCIENCE

DEREK LIN
CHIEF DATA SCIENTIST

Explore more

INFORMATION SECURITY

Operation Aurora – 2010's Major Breach by Chinese Hackers

JANUARY 8, 2019 — TIM MATTHEWS

Exabeam's Cybersecurity History Review: Read about Operation Aurora and the series of cyberattacks in 2010 conducted by the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army.

INFORMATION SECURITY

Exabeam's Top Cybersecurity Blog Posts of 2018

JANUARY 2, 2019 — MARITZA MARIE DUBEC

2018 was a memorable year for cybersecurity. Millions of people were impacted as we saw more companies hit by megabreaches—from a major hotel chain to a social media platform used by billions. Here are our top 10 blog posts that had the biggest readership and were the most noteworthy.

UEBA

User Behavior Analytics (UBA/UEBA): The Key to Uncovering Insider and Unknown Security Threats

JANUARY 2, 2019 — ORION CASSETTO

Learn about UBA technology, and its extension UEBA (User Entity Behavior Analytics), how it works, and which threats it uncovers that no other tool can see.

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information.

REQUEST A DEMO

PRODUCT
Exabeam Advanced Analytics
Exabeam Cloud Connectors
Exabeam Data Lake
Exabeam Entity Analytics
Exabeam Incident Responder
Exabeam Spectrum
Exabeam Threat Hunter

ANALYST CORNER
PARTNERS
SUPPORT

SOLUTIONS
Compliance
Threat Detection
Cloud Security
IoT Monitoring
SOC Automation

ABOUT
CAREERS
MEDIA KIT

LEARN
Library
Newsroom
Glossary
SIEM Cost Comparison

BLOG
Information Security
SIEM
UEBA
Security Operations Center
DLP
Incident Response

SIEM GUIDE
What is SIEM?
SIEM Architecture
Events and Logs
UEBA
SIEM Use Cases
SIEM Analytics
The SOC, SecOps and SIEM
Incident Response and Automation
SIEM Buyer's Guide

CONTACT
2 Waters Park Dr., Suite 200
San Mateo, CA 94403

1.844.EXABEAM
info@exabeam.com