WHITE PAPER–SEPTEMBER 2020

Five Cyberattacks That You Would Miss Without AI

vmware®

Introduction: Why Cybersecurity Will Fail Without AI

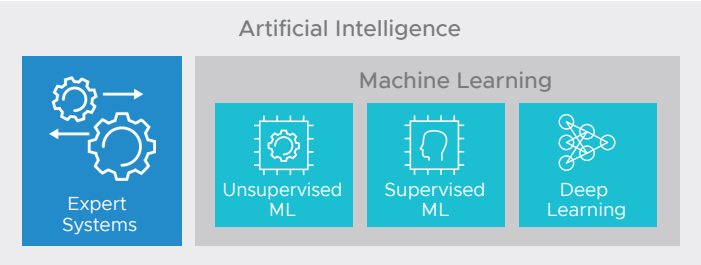
If you look at what's happening in enterprise security and computing environments, the number one element that IT teams and Security Operations Centers (SOCs) are struggling with is the sophistication of threats.

Adversaries can obfuscate and automate their attacks, and leverage polymorphic delivery vehicles so that nothing looks the same twice in a row. IT environments are becoming more complex: a LogicMonitor survey predicts that 83 percent of all IT workloads will run in the cloud by the end of 2020. More and more users, working from home, are connecting to these workloads. Billions of devices are added every year to the IoT population. As a result, security teams can no longer patrol the cloud as they did with conventional perimeter on-premises deployments. They simply cannot lock down the edge anymore. And what's making this even more challenging is that there is a tremendous cybersecurity talent shortage.

Taking together, all this suggests that AI is not only a viable solution, it may be the only solution. When faced with a flood of traffic and the requirement to dispatch it in some sort of an intelligent way while being short-staffed, AI fits the bill.

The Various Types of AI

When people say AI, they think all AI is the same. But it's not. Organizations struggle to understand what AI is capable of and what vendors mean when they say they're using AI.



AI is a big science. It includes expert systems in which an expert trains the computer to make certain determinations. AI also includes machine learning (ML). **Unsupervised ML** autonomously looks for anomalies or changes in behavior or activity.

Another type of AI, **supervised ML**, is different in that it's trained on what to look for. This training data may, in many cases, be automated as part of developing a system that can determine if something needs to be surfaced.

Deep learning is the Holy Grail: it uses all these types of AI capabilities. For instance, a character recognition program using deep learning could use one AI engine first to identify the edges of characters and then another AI engine to determine the language based on the initial findings about the shapes of letters.

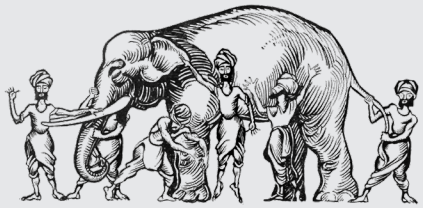
With this foundation in the different types of AI, this paper will now show how different combinations can effectively detect some of the most challenging attacks.

Attack 1: Emotet

Emotet is a modular banking Trojan that's been going on for years, and it's still gaining speed. **US-CERT** reported that Emotet is "a million dollar per incident type of an attack."

What's interesting about Emotet is that it's completely disposable—it has a one-time use. It's also polymorphic, meaning it looks different every time. And it's self-obfuscating, making it particularly difficult to detect.

VMware NSX Advanced Threat Analyzer first detected Emotet back in 2015, but now, years later, it is peaking because of a polymorphic nature that makes it impossible to detect using any type of a normal signature model.



HINDU PARABLE ABOUT SIX BLIND MEN

To explain how NSX Advanced Threat Analyzer uses AI to detect Emotet, consider an ancient Hindu parable about six blind men who come across their first elephant. Each of them puts out their hand and experiences the elephant in a different way.

One grabs the tail and is convinced that he's holding onto a rope. One grabs the tusk and is convinced that he's holding onto a saber. One touches the leg and is utterly convinced that he's holding onto a tree.

All of the blind men are wrong because their ability to sense the elephant is very limited. They don't see the full picture. They don't collaborate in such a way that they are able to use their communal experience of knowing what an elephant is—or, in the case of Emotet, knowing what a piece of malware is—to make an accurate determination.

NSX Advanced Threat Analyzer uses supervised ML and a combination of expert systems to detect Emotet. Think of supervised ML as people touching different parts of the elephant and collecting different pieces of data. It's only through this supervision, having trained the AI engine on what an elephant looks like, that the software is able to make this determination.

This is exactly how VMware NSX Network Detection and Response detects Emotet. The software sees individual characteristics in context—the context of knowing what an elephant (Emotet) looks like.

One may see a suspicious data upload and a remote task being scheduled, but those two incidents together are not suspicious. But when they are put together with a malicious document attachment in an email server, it becomes clearly recognizable as an Emotet attack. NSX Advanced Threat Analyzer uses supervised ML to put the pieces together to make determinations.

Attack 2: Mirai

The **Mirai** botnet was a particularly nasty one. Almost everyone was impacted and almost no one saw it coming.

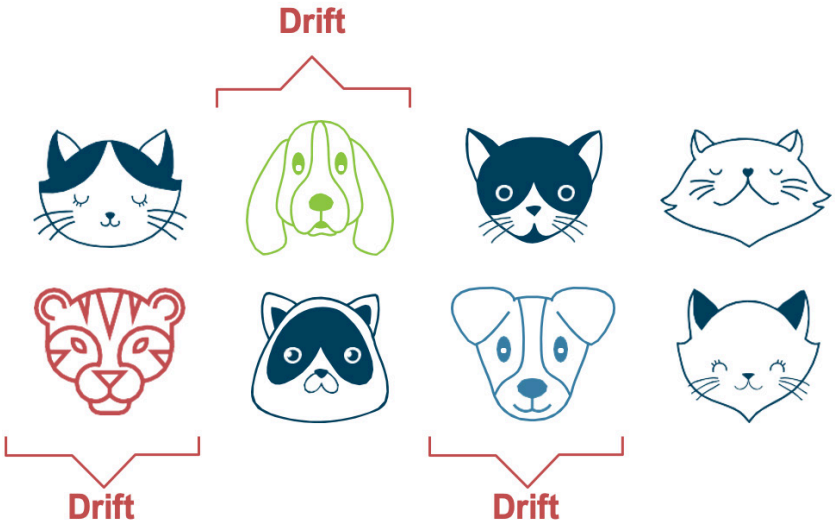
It was an IoT botnet assault that installed remotely, largely on personal computing devices or on things such as cameras, thermostats, or remote doorbells in the home—simple devices that may have used a UNIX kernel.

The Mirai botnet caused organizations to lose access to applications like Twitter and Netflix, plus some more business-critical systems such as industrial automation and control systems. But what type of AI insight could determine if a Mirai botnet attack was afoot?

NSX Network Detection and Response uses unsupervised ML. Our AI engine trains on data all day long looking at the Internet, and normal traffic moving from north to south and east to west.

To explain this using an analogy, look at cats. They may be different colors, different breeds, and different sizes, but they're all recognized as cats. The system doesn't know if a cat is good or bad, but it is baselined as a cat:

From the baseline data, changes occur that AI experts call drift. A few dogs enter the flow, or a tiger comes in. They have some of the same characteristics, such as fur and whiskers, but they're different.



These are things that look like anomalies. The system may not be able to determine if they're good or bad, but it knows they're anomalous and need further examination. And if the changes are small, the system may not recognize them as malicious.

Criminals can intentionally pollute the training data in this way so that their activity, initially anomalous, starts to look normal—it's called **adversarial machine learning.**

VMware NSX Network Detection and Response looks at the normal flow of traffic from a service that's collecting data from an IoT device and can see that the traffic is inbound to the IoT device manager. NSX Network Detection and Response also uses unsupervised ML in the malicious environment and may surface a disproportionate amount of traffic

moving in different directions and to devices that have not necessarily authenticated with that IoT concentrator.

A good example of abnormal traffic flow would be a web-enabled thermostat that has traffic moving in both directions. The user updates the temperature occasionally, but for the most part, there's only telemetry coming from the device. All of a sudden, with Mirai, there's a change to this typical behavior; there's much more traffic moving in the "wrong" direction.

NSX's software would pick up activity like a suspicious port scan. Why would an IoT device be doing this to begin with? NSX Network Detection and Response detects Mirai botnets because the software, using unsupervised ML, sees things that are happening away from the established baseline data.

Attack 3: LokiBot

LokiBot is a Trojan credential stealer that installs on Windows but is more famous for installing on Android machines. It beacons keylogs that it's able to capture from what the user is doing, whether on a phone, another Android device, or a PC keyboard.

Biometrics and dual factor authentication have beaten LokiBot, but not everybody has these for every application or device. In fact, in what was heralded as something that virtually no one could defend against, in March of 2017, LokiBot was preloaded with the standard Android operating system onto many telephone and tablet shipments. How could anyone defend against that?

AI is the perfect technology to detect LokiBot, not by using supervised or unsupervised ML, but by using both. Think of an atomic collider, like the CERN Collider in Europe, where atoms are smashed into each other at high velocity. This collision causes a spray pattern of the atom in the hopes of breaking it into its elemental components. Sometimes little particles spin off as well, which are unexpected anomalies. These undiscovered things weren't supposed to be there. What also might appear is the telltale sign of certain atomic elements. Both types of AI are being used—supervised ML to detect what is expected, and unsupervised ML to detect what is not.

Now, how does this work in the case of LokiBot? NSX Network Detection and Response can see anomalies in an unsupervised way that deviate from the baseline. The software also sees anomalous behavior based on how the algorithm has been trained, from supervised ML. Combined with NSA ATA, it can detect a similarity to a known malicious object such as a code segment that has been seen before anywhere across the NSX customer base. The software analyzes a file, detects elements of lateral traffic, and looks for things that may be malicious such as code segments—reused elemental components from somewhere else—from an earlier attack. This is the element of supervised AI.

You need both supervised and unsupervised ML to detect LokiBot. It's not enough to do one or the other.

Attack 4: DMSniff

Many have fallen victim to **DMSniff**, a Point-of-Sale (POS) installer. It resides on devices that everyone uses to make payments in stores, gas stations, restaurants, and elsewhere. DMSniff has impacted a lot of retailers and was undiscovered for more than four years. Combating DMSniff requires using both deep learning and supervised ML.

To explain DMSniff detection using a metaphor, recall the TV show "Cold Case." There are all these unsolved cases, and the police have DNA samples that they've collected from the crime scene. Even though DNA is a great way to pair up an attacker with a victim, a sample can come back inconclusive (that is, without a match) if there is not an existing sample of the culprit's DNA.

Then something interesting happened a few years ago–23andMe. It and other companies offer home genetic test kits where anyone can find out exactly what their DNA makeup is, what their ancestry looks like, and what their susceptibility is to certain illnesses. Millions of people have done this, greatly expanding the database of DNA samples. Now when police do a DNA search, they may not have a direct hit, but they can get very close. Leveraging AI, particularly deep learning, the police can determine, with a high degree of confidence, that the person whose DNA was collected at the crime scene is related to someone who has voluntarily submitted a DNA sample to 23andMe. There is not necessarily a 100 percent match, but leveraging AI, investigators are able to determine a subset of family members to whom the unknown suspect may be related.

What is very common in the hacker world is code reuse. Hackers are highly collaborative and share elements of code and routines that are effective. These bits of code have telltale signals or characteristics.

In the case of DMSniff, this essentially is how NSX Advanced Threat Analyzer AI detection works. The software detects obfuscated traffic in DMSniff because the command-and-control traffic, the beaconing, is essentially the carrier, where the keylogging or the credit card information is going to be contained. This would be the element, the re-used code, that would be seen repeated over and over again. Even though it's not an exact match, it's got the same brown eyes.

Supervised ML, utilized by NSX Network Detection and Response , detects things like abusive domain generation and low-bandwidth data exfiltration, which are known bad behaviors. Combine this with deep learning capabilities, and we help the analysts to determine if the behavior is DMSniff, so they can step in and remediate.

Attack 5: Cloud Workloads

There are many under the impression that public **cloud workloads** are safer than traditional deployments of computing capabilities on-premises or in private clouds.

This may well be the case, but as companies move large volume of workloads—and increasingly business-critical workloads—to the public cloud, the frequency of cyberattacks is increasing. Perhaps Equifax is the most prominent and well-known example, with the most significant impact.

One of the elements of the public cloud is that data traffic is both north of compute capabilities in, for instance, AWS, Azure or GCP, and then some of it is south of the edge interface. Different anomalous behaviors happen both in the plumbing as well as in the edge of the network.

However—and here's the tricky part—anomalous things are not all bad, and bad things are not all anomalous. This is why anomaly detection is not enough. It needs to be done in context.

Take, for example, a connection received on an unusual port. This is an anomalous, telltale sign that something may be wrong in a public cloud environment, but not enough perhaps to set a trigger. This is the problem with anomaly detection. It tends to lead to lots of false positives.

NSX Network Detection and Response checks for anomalies happening in the VPC logs, but also analyzes them in context with the type of traffic and the elements comprising the traffic that's moving north-south. Correlating this data with something seen at the north-south edge of the cloud provides confidence that an anomaly is truly malicious and an attacker has been detected in the public cloud instance of a hybrid computing environment.

NSX Network Detection and Response uses AI to identify anomalous activities that are related and part of the same attack by adding context to identify the difference between an isolated alert that's a false positive and other activities that are real threats.

Summary: Don't Believe the Hype About AI

While AI has its limitations, and the hype has caused some to write it off as snake oil, this is not a good reason to overlook its capabilities when properly applied.

Ultimately, effective cybersecurity is about using different types of AI, each tuned to a specific task, to come up with a composite of what's happening in your network and understand whether an attacker is present.

With more than 70 percent of all email being spam, 50 percent of traffic on the Internet today being bots, and 40 percent of that traffic being malicious, attacks will continue to overwhelm security teams.

The ability to continue computing, using intelligence to improve the human condition, and enjoy all the benefits of the Internet and available computing capabilities, depends upon doing so in a safe environment.

AI is definitely part of the answer, but understanding AI is critical. To leverage it for detecting advanced threats and streamlining security operations requires an understanding that not all AI is the same. Different types of AI help with different types of security. Ultimately, effectively applying AI to cybersecurity is going to help everyone regain control and get back to doing things that are more productive than threat chasing—like helping companies achieve their larger business goals.

NSX Network Detection and Response and NSX Advanced Threat Analyzer together leverage deep academic expertise in data science to apply AI to cybersecurity. The creators of this technology, the top two most published cyber researchers in all of academia, came together and said, "We have to look at a fundamentally different way of approaching this." AI is a critical component of their answer. They aimed AI at what's occurring on the network to determine what is malicious and what is not, versus trying to lock down the entire network and to anticipate everything that the bad actors are capable of.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com