How Security Analytics Can Be Used to Detect Security Threats

The Threat Landscape

In today's business world, there is no doubt that Cyber-attacks are one of the main fears be dealt with. In fact, it can be likened to a cat and mouse game. For every new security software patch, upgrade, or new tool that comes out, the hackers have already found a way to circumvent it.

Consider the gravity of these recent attacks:

- In the Sony security breach of 2011, almost 80 million customer records were hijacked;
- When Adobe Systems was hacked into in October 2013, 152 million customer passwords were stolen;
- Target Brands was a very ripe target for the Cyber hackers-over 110 million customer records and credit card numbers were hijacked, due to malware targeted at the vulnerabilities of the Point of Sale Terminals;
- In the medical world, Anthem Blue Cross/Blue Shield was hacked into, resulting in the theft of almost 80 million Social Security numbers;
- Just recently, in October 2015, over 15 million accounts of T-Mobile customers were hacked into.

The Reality

Given these alarming statistics, you may very well be wondering, how is this all continuing to occur? In other words, isn't just one major security breach enough to learn a valuable lesson?

To a certain degree, yes, businesses and corporations are implementing new lines of security to protect both their own intellectual property and customer base. But the problem is that the mindset of today is just focused upon prevention, rather than being proactive in terms of detection and response.

In other words, as a society we only act ***when*** a Cyber-attack happens, not ***before*** it happens. This is the weakness that the Cyber attacker of today is preying upon, and taking full advantage of in order to inflict the maximum amount of damage possible. A major part of this reactive mindset also lies in the current technology which is being used. It cannot predict the attack vectors of tomorrow. Here is a sampling of today's security tools:

- Logging:

  Centralized logging mechanisms and tools are heavily relied upon today. While they are good in collecting large amounts of data, it still takes a great amount of time and effort for the IT security staff of a business or a corporation to successfully mine through all of it, and find those hidden trends which are most applicable to their particular environment. In other words, it can take a very long time to effectively formulate analysis rules and alerts when combing through these huge datasets.

- Network devices which include Firewalls and Routers:

  These tools are very good in creating very detailed and specific system administrator logs (also known as a "syslog"). However, the sheer volume of network traffic can be extremely overwhelming even for the most experienced IT staff. Once again, it can take large amounts of time and labor to piecemeal through all of the data in a syslog, in order to create meaningful security alerts which do not result in false positives.

- Network Intrusion Devices and Intrusion Prevention Systems:

  This type of technology can detect well known attack profiles and any types of unusual and anomalous patterns of incoming network traffic. But, the problem is that these systems generate a very high amount false positive alerts. It can take an enormous amount of time to fine tune these alerts, so that the network administrator will be notified of only the relevant ones. Also, these tools are only meant to detect attacks, ***not predict*** attack profiles.

- Antivirus:

  The use of Antivirus software and its related tools is fast becoming obsolete. This is primarily due to the fact that these mechanisms can only detect the attack signatures of well-known spyware, malware, or adware; it cannot detect the covert ones at all. Also, it takes a lot of processing power in order to successfully contain any of these threats.

- Security Information and Event Management (SIEM) devices:

  These tools are very good at collecting and compiling information and data from a number of different security tools, which are networked together. But once again, the problem is the time which is needed to analyze all of this information; also they can be quite complex to manage and properly configure.

So, we can see a common thread here. That is lots of information and data being collected, no time to analyze it, and the inability to predict covert Cyber-attacks. What can a corporation or business do to stay ahead of this proverbial cat and mouse game? The answer lies in the use of Security Analytics.

The Wave of the Future-Security Analytics

This is the science of analyzing extremely large security datasets in real time, thus allowing for the very quick and extremely accurate revelation of the hidden trends which reside in them.

With the ability now to conduct such types of very sophisticated research, IT teams can now predict future Cyber based threats based upon these variables:

1) The timing of a Cyber based attack;
2) The specific sequences of such instances and occurrences;
3) Any discernable differences which have been gleaned from the security datasets;
4) Plotting the trends of risk and Cyber attacker behavior in real time.

Apart from this, Security Analytics can also be used by the IT staff to even find the root cause of any type or kind of security breach (or breaches) which may occur.

Also, predictive models can be created to build the profiles of future Cyber-attack vectors and comparing them to baselines of normal behavior in order to establish the appropriate risk level.

One method that is currently being used is that of Machine Learning. This is a process where building predictive models is fully automated, and specialized mathematical algorithms are used to literally comb through all of the security datasets in order to iteratively "learn" from it.

From here, any hidden insights can be discovered, because these algorithms have not been programmed to look at a specific time period, rather they look at the entire time frame.

In fact, other threat intelligence tools can be implemented into them as well, thus providing a comprehensive view of what the threat landscape will look into the future.

Although the benefits of using Security Analytics is enormous, there is one huge potential downfall to using such a system: It can be very expensive not only to procure, but it can quite cost prohibitive to maintain as well.

For example, large amounts of computing resources are required. This includes more memory and disk space, extra CPU processing power, etc.

Also, the attack profiles left by a Cyber attacker are very covert in nature, and thus, it may take the Machine Learning system a series of iterations in order to discover them at first.

The Four Business Use Cases of Security Analytics

There are four main areas where Security Analytics will prove to be the most useful for a business or a corporation:

1) Reduction in the Mean Time to Detect ("MTTD") a Cyber-attack:

   Security Analytics can be used to predict, under certain conditions, when an attack is imminent. This will give the critical time needed in order for the IT staff to beef up its layers of defense. Of course, there will always be that chance that such an attack may never even happen, but undertaking this process will enforce and yield a much more proactive security mindset in the long term.

2) Greatly enhancing the level of Internal Security Monitoring:

   There is a common misconception that security threats can only come from the external environment. For example, take the case of ABC Corporation. It has fortified its layers of security to thwart off any future Cyberattack which can from the outside. But in doing so, the management team has neglected of what could perhaps be the weakest link in the chain: Those security threats which can exist in the ***internal*** environment of a business or a corporation. Security Analytics can also be used to detect and prevent these risks as well, which is also known as "Internal Security Monitoring". For example, the mathematical algorithms can be programmed (coupled with the usage of Penetration Testing techniques) to detect any hidden vulnerabilities from within the IT infrastructure itself, and determine which threat poses the most risk to a particular IT asset.

3) Assist in IT Asset Configuration Management:

   Apart from detecting threats and risks, Security Analytics can also be used to help ascertain the most effective deployment and optimization of IT assets across a businesses' or a corporation's entire internal network. For example, it can be used to help answer some of these questions:

   *Which of the physical servers can be moved to the Cloud in order to streamline the flow of network traffic?

   *What is the longest period of time that a business or a corporation can withstand if a certain part of its network went down?

   *Are there any legacy IT assets which can be taken down from the internal network?

4) The Management Team has a much better understanding of what is going on:

   Many C-Level Executives often complain that they are the last ones to be kept in the loop on what the threat landscape looks like. But, with the use of Security Analytics, this is no longer the case. The management team can now be kept apprised of what is going on in real time. Thus, they will be able to answer these kinds of questions and more:

   *What is the overall risk level that we face?

   *How prone are we to a major Cyber based attack?

   *How quickly can we restore operations at the back up site if the primary systems are impacted by a major security breach?

   *What will be the most cost effective way to reduce our overall risk level?

Conclusions

As it has been discussed, the use of the present Security tools is simply not enough to thwart off any Cyber based attacks. Businesses and corporations must analyze their datasets in real time in order to predict what could happen in the future.

This is where the role of Security Analytics will come into play. But, despite the promise that it holds, experts are warning not to rely on it solely in order to fortify the defense perimeters of a business or a corporation.

This is due to two reasons:

1) The sheer volume of online IT assets is growing at an exponential rate, and the data which is needed to account for them is also evolving even quicker;
2) The Cyber hacker of today is becoming very sophisticated in terms launching covert attacks through using a Cloud Computing infrastructure.

As a result, it is predicted that the use of Artificial Intelligence, especially in the way of Neural Networks, will be needed in order to keep up with analyzing and interpreting all of these huge security datasets in real time.