Machine Learning and Advanced Analytics to Address Today’s Security Challenges

Today’s security professionals—seemingly always under pressure to keep their organizations protected against attacks—are facing an unprecedented level of challenges, as well as opportunities. Certainly, there is no lack of data coming into organizations’ security systems about potential threats and vulnerabilities, which can ultimately help security professionals do their jobs more effectively. Security alerts can enable organizations to minimize the damage of data breaches.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Host of Challenges</td>
<td>1</td>
</tr>
<tr>
<td>Solutions Based on Intelligence</td>
<td>4</td>
</tr>
<tr>
<td>Conclusion: A Call to Action</td>
<td>5</td>
</tr>
</tbody>
</table>
This white paper examines some of the key challenges many security teams are facing today, and how the deployment of a solution based on machine learning and analytics can help organizations address many of these issues.

Unfortunately, security teams receive an overwhelming amount of alerts every day, sending them on scavenger hunts for real threats. The lack of a cohesive strategy—and the technology to help make sense of all the data and simplify the analysis of alerts—can lead to higher costs, loss of productivity, and less-than-optimum security.

Some of the latest security solutions take advantage of advances in machine learning (ML) and data analytics to deliver meaningful insights to cybersecurity teams.

This white paper examines some of the key challenges many security teams are facing today and how the deployment of a solution based on ML and analytics can help organizations address many of these issues.

A Host of Challenges

Organizations are facing a security threat landscape that seems to be growing ever-more menacing. Bad actors are finding new and more sophisticated ways to break into systems and networks to steal data, or otherwise wreak havoc on organizations and their customers and business partners.

The past few years have seen a dramatic increase in ransomware attacks, which can bring an organization’s systems to a standstill. According to statistics provided by the U.S. federal government, ransomware is the fastest growing malware threat and is aimed at users of all types. Every 14 seconds, new organization is falling victim to a ransomware, according to Cybersecurity Ventures. The same research indicates that damages from global ransomware attacks cost around $8 billion in 2018 and is expected to surpass $11 billion in 2019.

Major organizations continue to be victimized by data breaches that leave sensitive data such as customer information exposed. In one of the more recent incidents, an attack against credit reporting agency Equifax from May through July 2017 resulted in the exposure of the personal data of 143 million American consumers. Hackers accessed individual’s names, Social Security numbers, birth dates, and other information.

These types of security incidents are costly. The average cost of a data breach is $3.62 million, according to the 2017 Cost of Data Breach Study by IBM Security and Ponemon Institute. The average cost for a lost or stolen record was $141, and the numbers are even higher for industries such as healthcare ($380) and financial services ($245). The figures are based on information gleaned from 419 companies worldwide that participated in the research.

Organizations not only face costs related to the data breach itself, such as incident response and investigation, but the expense of any legal settlements that might result from the breach. Then there are the costs to the company’s brand and reputation to consider.
Damage can also come from failing to comply with government and industry regulations that call for the protection of data. Regulations such as Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA) have been in place for years, and newer rules such as the General Data Protection Regulation (GDPR) have been put in place to protect the data of European citizens.

These regulations have strict requirements regarding access limits to data, as well as protection of the information itself. Research showed that many organizations—particularly smaller firms—were not prepared to meet the requirements of GDPR, which became enforceable in May 2018.

Making matters worse in terms of data loss and regulatory fines, it can take a long time for organizations to determine that they have suffered a security breach. More than half of data breaches take months or longer to discover, according to the 2018 Verizon Data Breach Investigations Report.*

Companies have deployed tools to monitor network activity and gather data about security events. But all the alerts and information coming into organizations keeps security teams on continuous scavenger hunts or trapped in mazes, searching for the answers that will keep the organization from experiencing a damaging breach.

* Sources: 2019 Data Breach Investigations Report (Verizon); 2017 Cost of Data Breach Study (IBM Security and Ponemon Institute); M-Trends 2017: A View From the Frontlines (Mandiant)
There are lots of paths to go down, but not all of these will lead to the solution the team needs. This process results in a lot of wasted time and money.

Consider a typical scenario at many organizations and the various steps involved. The security team notices an alert and takes a chance that it is the right one to spend time following. It checks the security operations center (SOC) dashboards for context to get an overall sense of what’s going on. Then it checks the security information and event management (SIEM) system and finds two IP addresses.

For each IP address, the team checks another console to find out which systems the IP address matches. It does a Web search to determine who owns the address and if it’s a good or bad IP address, then checks an asset inventory system to find out if something is a legitimate application and who owns it. Then the team emails the owners for details, because the asset inventory information is probably out of date or incomplete.

Next, the team checks another console to find out when the alert system was last scanned, and another console to find out if the system was patched after the scan, and yet another console to see if the system has been backed up. The process continues on and on with more emails, more console checks, more paths to follow. And at the end of the process—two hours after it began—the answer is that the alert was a false alarm.

Still, the aggravation is not over. Hundreds of other alerts might be coming in and clamoring for attention. So the security team picks another one to look into and begins the process all over again. Only those security professionals who’ve been through this process can truly understand how frustrating and time-consuming it can be.
The mathematical and analytics capabilities of a modern security solution identifies such factors as the riskiest users within an organization, and the potential threats those users represent.

Solutions Based on Intelligence

The latest security solutions help teams effectively address these challenges. By leveraging ML and big-data analytics capabilities, these tools can greatly ease and speed up the process of identifying and analyzing important trends, better protecting against genuine threats.

Companies need technologies such as machine learning and artificial intelligence (AI) today in order to solve the problems their security teams are facing, because existing processes can't scale and are not efficient in dealing with the demands of today’s security environment.

ML and AI enable teams to distill all the information that’s coming into them, identify the right places to look, and deliver the answers they need to find cyberthreats within minutes or days, not weeks or months.

The mathematical and analytics capabilities of a modern security solution identifies such factors as the riskiest users within an organization and the potential threats those users represent.

For example, the solution can detect a full-stage attack against an organization via advanced analytics in combination with Active Directory, IP Repository Logs, Web Proxy, and DLP data. With the solution, the security team can quickly view and understand the current state of users, repositories, endpoints, and network traffic.

They can optimize the time, resources, and budget spent on the investigation; spend less time gathering data and more time understanding an attack; and back up all of their findings with ML and analytics. The security team can see, at a glance, the current risk posture of an entity such as a user, file, client device, server, IP address, or other IT component.

When presented in an intuitive, interactive dashboard, security professionals can directly drill down into the details of why an entity’s characteristics, usage patterns, and behaviors are deemed higher risk than others. The system’s intelligence gives it the ability to dynamically learn contextual-behavior patterns for each unique entity, and how those entities interact with each other. The machine learning analytics clearly differentiates normal from anomalous activity. This leads to an extremely high-quality risk assessment and reduces the false positives characteristic of other risk measurement models.

It’s important to remember that strong security is not just a matter of deploying tools and letting them do the work. Security teams need to work closely with colleagues on the business side to gain better understandings and context of the data being that’s analyzed.
Also, keep in mind that what makes a solution like this so effective is the data. The more data available, the better the math works. The better the math works, the faster teams can detect a real threat. And the faster they can detect a threat, the faster they can respond. So bringing in more data from disparate sources can help organizations detect threats when advanced technology such as ML is applied to the data.

Conclusion: A Call to Action

In today’s cybersecurity landscape, attack vectors are becoming increasingly stealthy and multifaceted, enabling bad actors such as hackers and cybercriminals to avoid detection via traditional security tools. In order to truly understand the impact of a threat, security teams need to holistically evaluate the threat by all relevant angles and data points.

New security tools based on ML and advanced analytics allow security teams to directly access a prioritized list of high-quality security leads, so they can quickly identify threats such as compromised accounts, insider incidents, and intellectual property theft. The security leads deliver a distilled view of measured risk generated through dynamic ML and advanced mathematical models. Because no security professional is capable of matching the rate at which a computational system can process and correlate vast amounts of data from multiple sources, the analytics capability provides an unprecedented level of efficiency and productivity to the security team.
The stakes are too high for organizations to continue relying on outmoded and ineffective methods of detecting and stopping threats before they can cause damage. Businesses owe it to themselves and their customers to use the latest technology to outsmart the bad actors and keep information safe.