LYNX TECHNOLOGY PARTNERS

The Economics of Threat

INTRODUCTION

Technology is evolving at a break neck pace. Unfortunately, cyber-criminals, nation-state hackers, and foreign competitors are adopting new technologies quicker than we could ever imagine. Within the cybersecurity space, it is not adequate to simply improve our current workflow and threat analysis capabilities. We must make generational leaps into the next level of threat detection to be able to defend our data and our networks.

There is a broad and ever-changing array of threat-space solutions that promote capabilities which overlap, confuse, and attempt to drown out each competitor's messaging. As a result, organizations today are having a challenging time understanding ultimate value and defined outcomes.

GENERATIONAL CAPABILITIES WITHIN THREAT DETECTION

An important evolution has occurred within the threat detection space. Unfortunately, end users of these security solutions tend to not recognize where in the evolution a solution truly lies, and thus what the capabilities and limitations are. As attackers are always ahead of the defenders, it's important to understand the generational model in order to determine the capabilities that are right for an institution and its networks.

3RD GENERATION SYSTEMS

3rd Generation platforms provide a category of technology called Security Incident and Event Management or "SIEM" solution. SIEM solutions rely on pre-determined "rules" or policies where a human decides what alerts to produce given a set of pre-defined indicators. This is where the vast majority of the industry is today. There are several critical shortcomings of 3rd Gen platforms, which include an inability to handle large volumes of data (requiring data reduction and loss of threat indicators), expensive labor and expertise required to tune the system, a very high false positive rate, and more.

4TH GENERATION SYSTEMS

The 4th Generation platforms in the marketplace today are essentially SIEM platforms with missing add-on capabilities bolted onto the platform to address detection blind spots. These solutions are often marketed as Next Generation SIEM or "SIEM-less" technology products, due to the fact that their objective is to improve the labor efficiency of managing the SIEM platform. Threat detection limitations for 4th Generation systems still have the same shortcomings of 3rd generation systems, but now include a licensing expense with all of the non-native add-on features.

5TH GENERATION SYSTEMS

5th Generation platforms do not use SIEM technology, but use Threat Analytics as their technology paradigm. Threat Analytics platforms do not depend on rules to identify threats, but instead use behavior and machine learning to evaluate all of the available data without data reduction. They natively correlate user, asset, and network behavior, include advanced correlation use cases, and use machine learning to not only detect unknown threats but also to evaluate their accuracy. A key capability for a 5th Generation system is the ability to ingest, process and analyze ALL of the log data. The system cannot be allowed to reduce the data into subsets that make it easier for databases to process, because this reduces that breadth of potential threat indicators that might be used for post-processing threat analysis, hunting, and forensic analysis.

6TH GENERATION SYSTEMS

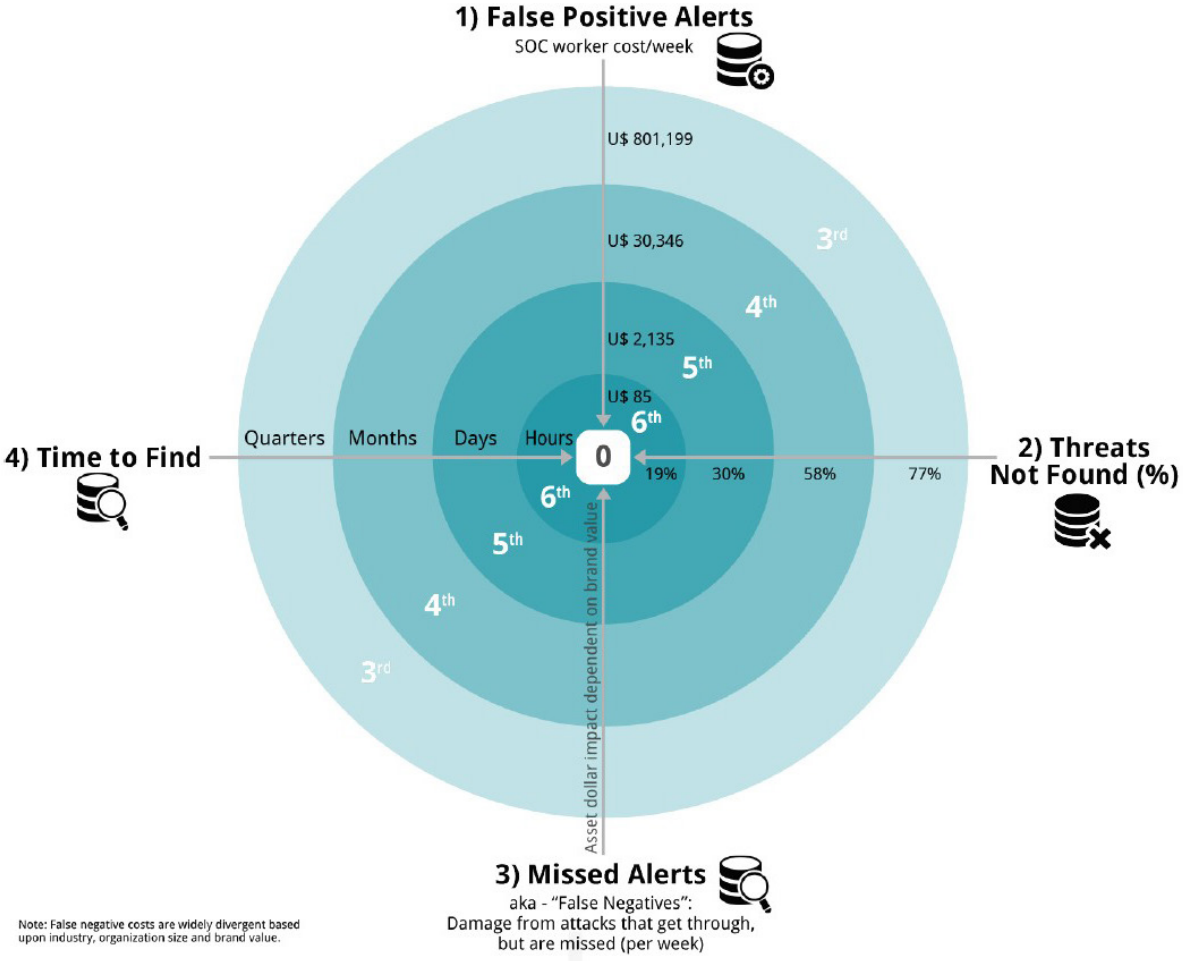
Sixth Generation platforms utilize threat analytics as their detection approach, but have extended capabilities into "Full Spectrum Threat Analysis". Full Spectrum Threat Analysis (FSTA) is the current desired state within the industry and is not yet available in the marketplace.

THE ECONOMICS OF THREAT

In this new era of threat, we must continuously advance to new generations of technology to stay current with the attackers. That is what drives Lynx Technology Partners's perspective of the generational model and its economics. As part of this effort, we offer a four dimensional analysis of how organizations can evaluate the threat detection capabilities of third party MSSP/MDR providers or their own in-house capabilities.

The cost of threat detection can be a significant expense to an organization, particularly when there is insufficient definition of economic outcomes of the effort. When evaluating any technology, platform or service, there is essentially a tradeoff between cost and risk that must be used as part of the purchasing decision. Lynx offers a tradeoff analysis as a four-dimensional cost benefit analysis that can help every organization better understand their defined outcomes.

We refer to this analysis as “The Economics of Threat”. The diagram below identifies four dimensions or quadrants of the model which describes how the efficacy of threat management has on risk and cost to the business.



Within the diagram, each of the four quadrants represents a continuum of capability or maturity. The goal for the organization in each quadrant is to advance to the center where achieving zero is the intended goal, but with the understanding that that primary focus is to “leap” to the next generation threat model along the continuum.

FALSE POSITIVE ALERTS

Using 3rd Generation toolsets the cost is quite high to perform all of the alert triage necessary due the manpower required to address the detection gaps. A 2016 Ponemon study (Cost of Data Breach Study: Global Analysis) evaluated several hundred companies and quantified the financial cost of triaging false positive alerts. The study found that false positive alerts cost enterprises an average of $1.2M annually, while further commenting that the vast majority of the alerts go unassessed due to the overwhelming volume and lack of manpower to adequately review. 5th & 6th Generation platforms can dramatically reduce false positive alerts allowing more time for analysts to investigate and validate high probability threat indicators.

PERCENTAGE OF THREATS NOT FOUND

No system is risk free or impervious to attack. As long as humans are in the systems loop, some percentage of threats will get through. However, it is extremely difficult to ascertain the efficacy of a particular solution or platform because they cannot determine what threats are being missed. There is also a tradeoff between security policy rigor and flexibility needed to conduct business. Our countermeasures and technology need to be flexible in order to be effective in real-world business scenarios, while managing risk and protecting data assets.

MISSED ALERTS

The longer a compromise or breach remains undetected, the more damage will be caused from a missed event. The cost of a missed alert or "false negative" is directly tied to time to detection. There have been numerous examples in the press of costly breaches that were not particularly cost prohibitive to fix, however the resulting brand impact and loss of trust of the organization was 80% of the loss. Organizations should consider the brand, reputation, and operational impact that a missed alert would have on your organization.

TIME TO FIND

Attackers only have to be right once, but defenders have to correctly detect and respond every time. One key distinction is the ability to analyze all of the data in later generation platforms which is a key advantage in finding a larger range of threat indicators using behavioral means.

WHERE LYNX TECHNOLOGY PARTNERS FITS

Lynx Technology Partners is currently utilizing a 5th Generation platform and is moving into 6th Generation powered by Security OnDemand capabilities throughout 2019. With the release of Lynx's version 5.1 ThreatWatch platform in May of 2019, the company is enhancing existing 5th Generation capabilities in the areas of user and asset behavior analysis with improved correlation, new portal tools that display a timeline-based view of user and asset activity, IOT threat detection use cases, new cloud connector APIs, and more.

Over the last year, Lynx Technology Partners has been investing in a new extension of its data analytics technology, called "AQ String". This new analytics engine will allow Lynx to fully analyze raw log data without normalization, data reduction, or further manipulation, which can bias the analysis results. Lynx's AQ String analytics technology is the basis for our 6th Generation full-spectrum threat detection and will power a new application of unsupervised machine learning. That application will automatically identify hidden patterns in the data, behavior anomalies, and baseline outliers not detected by other means.

Lynx Technology Partners provides 24x7 advanced cyber-threat detection services for businesses and government agencies.

Lynx Technology Partners
LetsTalk@LynxTP.com
1 (800) 314-0455
www.LynxRiskSolutions.com

Lynx Technology Partners is the leading provider of advanced managed security services. Our solutions help organizations protect against security threats, adhere to compliance requirements, and manage risk. Our scalable architecture eliminates capital outlay, provides 24x7 support/monitoring coverage, and lowers management, maintenance and staffing costs.