International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Information Overload to Informed Action: Applying AI and ML Data-Driven Threat Intelligence and Risk Management Frameworks

Vinay Dutt Jangampet
Staff Ops Engineer, Intuit, Plano, USA, yanivdutt@gmail.com

Abstract

As the cybersecurity threat landscape continually evolves and cyber threats grow progressively more complex, information security has become a more significant challenge in the modern digital age. Legacy security measures cannot satisfactorily defend against persistent, sophisticated, and dynamic threats as they are fundamentally intuitional. Luckily, one promising method to solve the current problem is by leveraging the power of data-driven threat intelligence. This technique augments human capacity with helpful insights, enhanced decision-making, and predictive analytics, hence enabling security teams to better comprehend and address the concerns. Additionally, effective collaboration between data-driven threat intelligence and risk management frameworks enhances the cybersecurity posture of an organization, guarantees business continuity, and improves the risk resilience of specific projects.

Keywords: Data-driven threat Intelligence, threat intelligence, Risk Management Frameworks, risk management, AI, ML, cyber threats, malicious actors, security incident.

Introduction

In the convoluted network of digital ecosystems, threat intelligence surfaces as a tremendously vital sentinel, protecting infrastructural sanctities against intricate cybersecurity threats. Nevertheless, with the exponentially increasing number of digital footprints, security professionals are grappling with a formidable adversary – an overwhelming rise of data, usually termed "information overload." In terms of threat intelligence, information overload implies the flooding of intelligence inputs characterized by the relentless flow of logs, feeds, reports or notifications; that security teams should refine through. Typically, the inundation is caused by the inclusion of new devices in a digital environment, the evolution of sophisticated cyber threats (malware), and the rise of cyber activities. The consequences are manifold, including security analyst burnout, failed threat detection, delayed response, et al. The solution, notwithstanding, lies not in minimizing the vast influx but in sifting the sieving method through informed (intelligent) action.

AL and ML Data-Driven Threat Intelligence and Risk Management Frameworks

Before delving into the correlation between data-driven Intelligence and risk management frameworks, it is important to recall that '*threat intelligence'* is a process by itself. Basically, '*threat intelligence'* is a cycle of direction, analysis, processing, assessment, and feedback. *Data-driven threat intelligence* is equated to food for malnourished cyber-risk models. According to [1], data-driven threat intelligence is a process of leveraging data points to understand enterprise threats. [2] Define data-driven threat intelligence as evidence-based knowledge regarding threats, intended to prevent cyber-attacks or compress the period between data system penetration and threat detection.

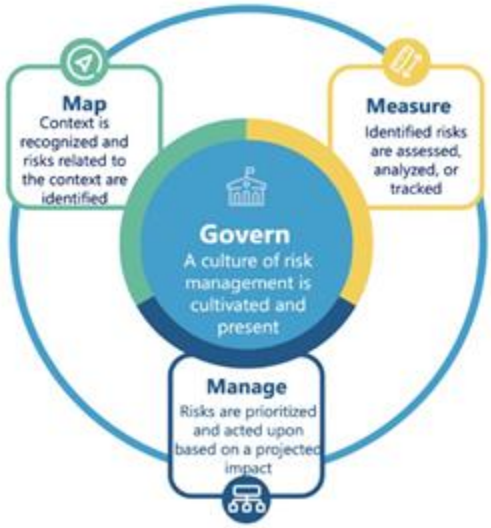
Map
Context is recognized and risks related to the context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact

Figure 1. NIST Risk management

A typical cyber-risk model has to be input such as *high-medium-low* or *red-yellow-green*, thus you shouldn't be shocked when they do not mature or perform as you want them to. The rule of the thump is: good intelligence always makes smart models; smart models cause informed decisions; informed decisions result in great practice; great practice enhances risk posture; and this done effectively, ultimately develops an effective cybersecurity plan [3].

Data-driven threat intelligence involves the integration of data analytics into the information security fabric by leveraging vast datasets to spot patterns, anticipate potential cyber-attacks, and prescribe appropriate preventive security controls [4].

It employs an extensive amount of data generated by organizations and converts it into actionable intelligence, surpassing the reactive standards of legacy cybersecurity solutions. Recently, data-driven threat intelligence is transforming the way organizatopms safeguard their digital assets. This surfaces from the necessity to adapt to the continually evolving threat ecosystem where cyber-risks have become exceedingly dynamic and sophisticated.

A risk management framework (RMF) is a guide that establishes the policies that organizations should comply with in order to successfully manage cyber-risks. NIST (National Institute of Standards and Technology) cybersecurity framework (CSF) is a U.S.-based RMF formulated to mitigate cyber-risks related to information infrastructures. Modern RMFs are used to manage security risks across critical organizational operations, such as enterprise, financial, compliance, litigation, and information infrastructures.

Significance of Data-Driven Threat Intelligence and Risk Management Framework

A. Identifying high-risk vulnerabilities

Data-driven threat intelligence "brilliantly" sifts signals to spot high-risk areas. With advanced analytics, these state-of-the-art approaches prioritize vulnerabilities that may potentially cause devastating breaches so security teams can remedy the flaws promptly and seamlessly. Additionally, it adopts local intelligence to devise security techniques that are uniquely customized to an organization's distinct risk profile.

Security teams can leverage these approaches to prioritize cyber threats based on what the data reveals about the specific vulnerabilities of an organization rather than relying on industry trends.

B. Predictive Threat Mitigation

This is a futuristic thinking aspect of data-driven security systems that predicts and thwarts cyber threats before they happen. These advanced approaches leverage data to contextualize and comprehend the peculiar cybersecurity narrative of an organization. This specificity allows adequate resource allocation, focused on data trends and previous security incidents associated with the organization, to develop a robust, preventive, and responsive security plan.

C. Adaptive Security Posture

In today's continually evolving cyber threat landscape, an adaptive defense system stands as a sturdy beacon for the organizations cybersecurity operations. Data-driven security techniques / systems use real-time data analysis and algorithms that evolve synchronously with emerging threats. These systems are characterized by superb agility that is crucial for firms whose cybersecurity decisions may be overwhelmed by other enterprise priorities. By constantly inputting real-time data into security infrastructures, data-driven security mechanisms guarantee that the security posture remains sturdy, relevant, and informed by the most recent intelligence.

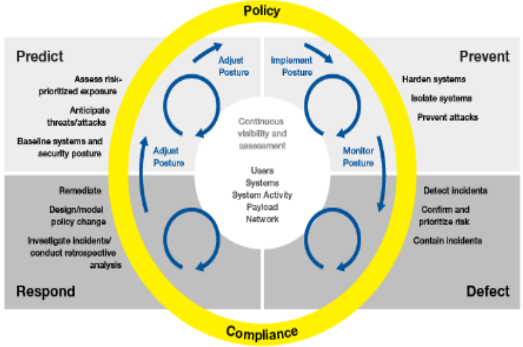
Policy
Predict
Prevent
Assess risk-prioritized exposure
Anticipate threats/attacks
Baseline systems and security posture
Adjust Posture
Implement Posture
Harden systems
Isolate systems
Prevent attacks
Continuous visibility and assessment
Adjust Posture
Monitor Posture
Users
Systems
System Activity
Payload
Network
Remediate
Design/model policy change
Investigate incidents/ conduct retrospective analysis
Detect incidents
Confirm and prioritize risk
Contain incidents
Respond
Defect
Compliance

Figure 2. Stages of adaptive security posture

D. Optimized Resource Allocation

After data is collected, what follows is distilling it into actionable insights. Here, security teams can leverage an amalgam of rule-based protocols to refine the data. Security professionals are tasked with overseeing the analysis processes, verifying findings, and expounding the outcome to differentiate between actual threats and false positives.

E. Executing solutions

Helpful insights extracted from data analyses are translated into protective security measures to bolster the cybersecurity posture of an organization. This stage requires tactical implementation and strategic planning where solutions range from basic patch management to intricate system overhauls.

IV. Conclusion

Data influx has triggered cybersecurity transfiguration, enabling much more informed decisions powered by evidence-based, data-driven mechanisms. Businesses can no longer rely on presumptions and gut feelings to make critical security decisions – not when vulnerabilities can be reviewed, risks quantified, investments justified, and teams offered confidence, all by data. Data-driven threat intelligence and risk management frameworks promised improved visibility, minimized risk, and informed decisions.

V. References

[1] M. Bromiley, Threat intelligence: What it is, and how to use it effectively. SANS Institute InfoSec Reading Room, 15, 172, 2021.

[2] Chismon, D., & Ruks, M. , Threat intelligence: Collecting, analyzing, evaluating, MWR InfoSecurity Ltd., 2020.

[3] M. Tappin, The link between Threat Intelligence and Risk Management., Available at: https://m.digitalisationworld.com/blogs/56243/the-link-between-threat-intelligence-and-risk-management, 2021.

[4] Rikkeisoft, Data-Driven Security: Transforming Protection Through Analytics., Available at: https://rikkeisoft.com/blog/data-driven-security-transforming-protection-through-analytics/, 2023.