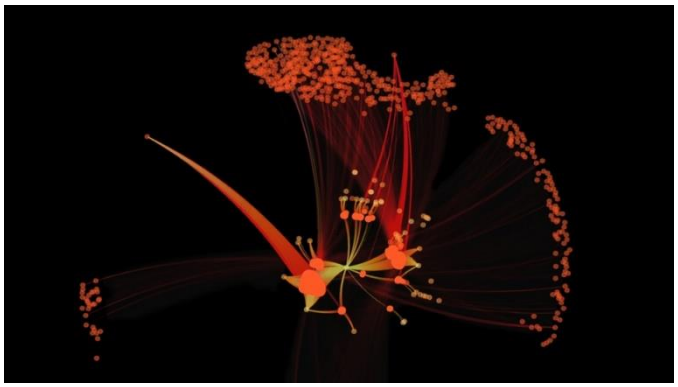
Knight Technology Solutions
A Division of Knight Technology Group, LLC.

CYBERSECURITY



Knight Technology Solutions Cybersecurity

Cybersecurity-related risk remains one of the top sources of risk in the enterprise. This has been exacerbated by the global pandemic, which has forced companies to accelerate digitization initiatives to better support a remote workforce.

This includes not only the infrastructure to support a distributed workforce but also automation through robotics, data analytics, and new applications. Unfortunately, this expansive digital footprint has led to an increase in cybercriminal attacks. If you are considering a new cybersecurity solution for your business, it is important to understand how traditional prevention methods differ from modern AI solutions.

Are traditional cybersecurity methods still feasible for enterprises? The proliferation of endpoints in today's more distributed environments makes traditional cybersecurity methods, which create perimeters to secure the infrastructure, much less effective. In fact, it's estimated that for at least half of all attacks, the intruder is already inside.

Manual data collection and analysis process
Implementing rules-based tools or supervised machine-learning systems to combat cyberattacks is ineffective. The number of logs collected on devices and added to networks continues to increase and can overwhelm traditional collection mechanisms. Petabytes of data are easily amassed and must be sent back to a central data lake for processing.

Due to bandwidth limitations, only a small sample is typically analyzed. This might be as little as five percent of the data, so one in every 2000 packets can be analyzed. This is a suboptimal way of analyzing data for cybersecurity threats.

Most enterprises have the means to look at only a small percentage of their data. This means they are likely missing valuable data points that could help identify vulnerabilities and prevent threats. Analysts may look to enrich their view of what is happening in and around the network by integrating tools and data, but this is often a manual process.

Lack of AI capabilities leads to longer threat detection times
It is estimated that it can take up to 277 days to identify and contain a security breach. Being able to quickly triage and iterate on a perceived threat is crucial, but also typically requires human intervention. These problems are magnified by the global shortage of cybersecurity professionals.

Supervised ML systems also can't detect zero-day threats because that is a "look back" cybersecurity approach. Traditional software-driven approaches like these can impede security teams from responding quickly to cybercriminals.

A better way to address threat detection challenges is with AI technology. For example, a bank institution may implement an AI cybersecurity solution to automatically identify which customer transactions are typical and which are potential threats.

AI cybersecurity use cases include:

Analyst augmentation technology using predictive analytics to assist with querying for large datasets.
User behavior risk scoring using AI algorithms to mine network data to identify and stop potential threats.
Reducing the time required to detect threats through faster, automated AI model updates.

Adopt an enterprise AI cybersecurity framework
NVIDIA Morpheus enables enterprises to observe all their data and apply AI inferencing and real-time monitoring of every server and packet across the entire network, at a scale previously impossible to achieve.

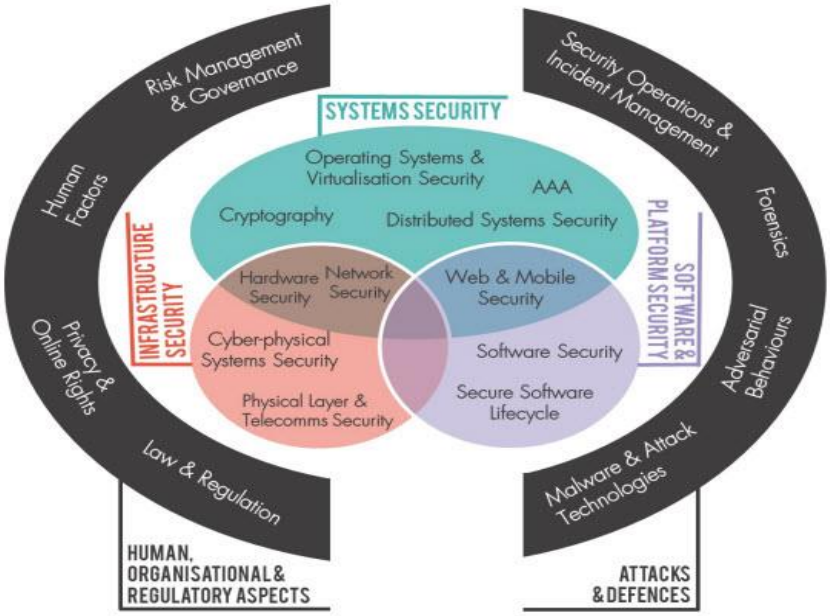
The Morpheus pipeline, combined with the NVIDIA accelerated computing platform, enables the analysis of cybersecurity data orders of magnitude faster than traditional solutions that use CPU-only servers.

Additionally, the Morpheus prebuilt use cases enable simplified augmentation of existing security infrastructure:

Digital fingerprinting uses unsupervised AI and time series modeling to create micro-targeted models for every user account and machine account combination running on the network, detecting humans posing as machines and machines as humans.
Phishing detection analyzes the entire raw email to classify it into ham, spam, or phishing.

Sensitive information detection finds and classifies leaked credentials, keys, passwords, credit card numbers, financial account information, and more.

Crypto-mining detection addresses the issue, reported by more than 69% of enterprises, of crypto-mining malware resulting in malicious DNS traffic and over-utilization of compute resources. This model determines crypto-mining, malware, machine learning and deep learning workloads, and more.



Get in Touch

Email:
information@knightgroup.tech
Website:
https://knighttechnologygroupllc.com
Phone:
(316) 928-3656 or (614) 563-2857