New cyberscapes call for new approaches towards cyber security. Today's enterprise systems comprise a variety of architectures, devices and diverse sets of participants. It is a cyber ecosystem of sorts – a dynamics of processes, communication technologies and data flows. It is also an ecosystem with new vulnerabilities going hand in hand with its complexities. Guarding such a dynamic, multi-layered, moving target is challenging.

As our digital world opened a world of possibilities for code makers and code breakers alike, cybersecurity companies are seeking new approaches to address the challenge of the growing number of new cyber threats and system vulnerabilities exploited by cyberattackers.

A Deloitte's Transforming Cybersecurity report puts it aptly:

> The question is whether today's industry can create a dynamic, intelligence-driven approach to cyber risk management not only to prevent, but also detect, respond to, and recover from the potential damage that results from these attacks.

An Aegis Built of Connected Data About Cyber Threats

Detection and prediction of cyber attacks is a challenging task for enterprise data and the architectures built to keep and manage these data. Towards that end, enterprise security systems have to be vigilant for a diverse array of cyber attacks and the impact related to the various security breaches.

With complexity building up in business IT systems, a corresponding level of sophistication is needed for the system that monitors the ecosystem and renders an up-to-date picture of the monitored elements and the potential attacks towards them. Translated into data, this means that a system is needed that can spot cyber threats across a landscape of terabytes of data and a flood of security alerts.

In other words, it takes the same dynamic, multi-layered shield to protect the enterprise ecosystem.

Picture the legendary aegis of Athena with its multiple interwoven tassels hanging from it;

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com

> [The aegis of Athena] produced a sound as from a myriad roaring dragons and was borne by Athena in battle … and … is ageless and immortal: a hundred tassels of pure gold hang fluttering from it, tight-woven each of them, and each the worth of a hundred oxen. – Homer

Now imagine that shield crafted of data fabric.

This will be a shield made of connected data and protected by sending credible information to security analysts to detect, or find patterns indicative of cyber attacks.

Strategically, this approach is about vigilance and resilience. As Deloitte's model about new approaches towards cyber security and cyber risk management suggests, this is as much about security as it is about vigilance and resilience, powered by early detection of risk. According to the model, a well-rounded cybersecutiry capability is built with two levers: a. Actionable threat intelligence and b. Strategic organizational approach

In Deloitte's research's words:

> Incident detection that incorporates sophisticated, adaptive, signaling, and reporting systems can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on an enterprise-wide basis.

But how are the described potential harmful activities to be detected by this, let's call it sentient (to penetrations) shield? And further what data fabric is this shield to be made of?

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com

Meet your New Cyber Security Guard: The Live Knowledge Graph

As we saw, the ability to detect emerging threats and anomalous patterns amidst terabytes of data and thousands of alerts within a dynamic and highly complex environment is what new cyberscapes call for when it comes to protection of systems. There is a need for automated systems that can monitor upcoming data flows and serve security analysts as a "sentient" shield signalling various threats and potential risks to the organization.

Case in point, Ontotext built such a shield of connected data to help a global cybersecurity and defense organization monitor, analyze and ultimately protect their client's data, applications and IT infrastructures. The challenges the organization was facing were related to the substantial volumes of security threats data that needed to be not only easily monitored and accessed but also quickly and efficiently analyzed, in real time.

To stay in control, they built a live shield "sensing" vulnerabilities and penetrations. The shield was actually a knowledge graph comprising various types of data about malware,

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com

ransomware threats, viruses, vulnerabilities and other potential breaches. Being live, that is, fed with real-time data, this cybersecurity knowledge graph allowed security analysts to access the up-to-date dynamic representation of relevant cybersecurity data.

Such a knowledge graph served the organization to build an expansive threat-aware system that could reinforce better cyber attack responses and quicker recovery actions.

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com

Epilogue: Forewarned is forearmed

There is a Latin proverb that has been transferring the wisdom of “being prepared” for many ages. The proverb has it that the ones who know that something is coming are better prepared to face it.

And this is what a knowledge graph for cybersecurity is built for – forwarning by forearming.

Built on semantic data a knowledge graph allows cybersecurity experts to protect infrastructure, applications, and data by staying in control of each and every threat and vulnerability. It helps analysts capture knowledge and further act upon that knowledge – as swiftly and aptly as possible, thus enhancing the processes of monitoring, tracking and detecting security breaches and potential risks.

Intrigued by the potential of using a knowledge graph for cybersecurity data?

Book a Discovery Call

Copyright: Ontotext New York | Sofia | Basel
Reach out to us: info@ontotext.com