Google Cloud | Deloitte.

Unify your cyber threat hunting with predictive analytics

Organizations are awash with cybersecurity tools, creating significant complexity, cost and confusion. Most importantly, many organizations are struggling to make sense of the alerts generated from numerous security applications, appliances and services. A modernized, risk-based approach to cybersecurity using predictive analytics can help push organizations beyond simply maintaining cybersecurity parity with other organizations and instead place them a strategic step ahead.

As cybersecurity challenges have dramatically increased and diversified in recent years, many organizations have scrambled to come up with countless point solutions for new threats. Not only has this dramatically bloated their cybersecurity budgets, but the swelling number of tools may have also added daunting complexity to the jobs of security professionals.

The escalating number of security alerts have created more and more data, but those alerts may often provide limited insight into the organization's state of cyber readiness. And the traditional bastion of organizational cybersecurity—the Security Operations Center (SOC)—typically was not designed for today's challenges of ubiquitous mobility, escalating remote work, cloud-first processes and the managing of dozens or even hundreds of security tools.

The implications of not adequately managing cyber risk have never been greater. This goes far beyond the cost of remediating data breaches, the total cost of which are expected to reach $6 trillion globally in 2021[1]—more than double the economic impact of those breaches in 2015. Organizational cybersecurity risks may also carry substantial loss of competitive position, including potential loss of employee productivity, diminished customer experience and damaged brand reputation.

Far too often, organizations suffer from a pronounced lack of the applicable analytics to properly address the growing number of cyber threats. Security teams need more help in order to determine whether an alert is high priority and is actionable. They also should promptly understand which attack surfaces have been compromised and how those attacks impact operations and compromise enterprise-wide risk management.

Chronicle

TechTarget | Custom Media
White Paper

Uncovering the risks that matter most

Organizations of all sizes, industries and geographies are literally buried in cybersecurity tools. As new threats have surfaced, so have new tools purporting to address the latest flavor of cyber risk. But those tools usually have been purpose-built, making them well suited for one kind of threat but inappropriate for others.

The result: Cyber tool sprawl. This is an expensive, inefficient and personnel-intensive approach to cybersecurity. This point-product-centric strategy also results in a cascade of cybersecurity telemetry, which often adds to the confusion. For instance, it is not unusual for a **large enterprise SOC** to receive dozens, hundreds even thousands of alerts daily, and SOC engineers may often lack the context necessary to sort out what is actionable from what is simply background noise.

Now, add to that mix the rest of the contributing factors of cybersecurity telemetry that must be captured, analyzed, evaluated and acted upon—or not. These include more and more devices, including many non-standard formats like sensors, wearable computers, vehicle-mounted computers and every other manner of mobile device. Also, in the mix are the dozens or hundreds of cloud services and SaaS applications organizations use, and that their employees often use for both personal and professional needs.

These and other data sources represent countless points of potential intrusions and penetrations, making it more difficult than ever to make smarter, more confident security decisions in real time. That's because the data lacks context, making it far more challenging to prioritize risk, assign the applicable resources and take the right action.

Clearly, a new, more inclusive and modernized approach is needed.

Cybersecurity "parity" isn't good enough

Let's face it: Keeping up with security risks is challenging, both operationally and financially. Recent high-profile hacks and cybersecurity compromises have reminded everyone that the need for a modernized threat management and analytics solution is greater than ever. Everyone is well aware of the dramatic global **"cyber skills gap,"** with approximately 4 million cybersecurity jobs currently unfilled[2]—a number that has grown even faster than normal during the COVID-19 pandemic. One important reason why this gap exists, and is expanding, is

the changing role of the SOC to appropriately enable a security platform, rather than a collection of point products.

Those resource constraints, plus the reality that new zero-day attacks and similar never-seen-before threats are emerging all the time, have prompted many organizations to make just enough investments to achieve security parity with competitors and others in their industry. After all, many CFOs and other business decision-makers are wrestling every day with tough decisions on how much to invest in cybersecurity and in what areas.

But would it make sense to take a parity approach to other essential organizational disciplines, such as product development, sales, marketing and supply chain management? Of course not. Organizations strive to be best in class for each of those in order to achieve and sustain competitive advantage. Cybersecurity must be viewed in the same manner.

That's why a future-forward, contextualized and data-driven risk-based security framework based on predictive, quantifiable risk is essential. By assessing threats on the basis of risk can enable organizations to make the necessary advances in hardening their defenses and improving their security profile. Organizations need to proactively find, assess and steer clear of the next threat, and doing that demands not just more data, but the right data in the proper context.

The focus should be on "anticipate and prevent," not "see and react."

Organizations need to proactively find, assess and steer clear of the next threat, and doing that demands not just more data but the right data in the proper context.

What to look for in a predictive analytics solution

The exponential growth in cyber risk means that new functionality is needed for a cloud-based predictive analytics platform. With threats to organizational security coming from everyone from organized cyber-criminal gangs, malicious insiders, competitors and rogue hackers bent on making a name for themselves, organizations need a new defensive stance.

First, the dramatic advances in cloud computing security have made that environment a more agile, scalable and cost-efficient way to deploy predictive analytics based on contextualized risk assessment. Leading cloud platforms such as Google Cloud have been engineered and enhanced over time to withstand industrial-strength attacks from a wide range of threats. And related cloud tools such as Google Cloud Chronicle[3] deliver robust threat-hunting capabilities and support for big data analytics.

Additionally, a modernized, cloud-based predictive analytics security platform must enable:

- **Scalability.** Not only are data volumes growing at faster-than-ever rates, but new threats themselves are emerging all the time. Plus, the very definition of "enterprise" has evolved from primarily a physical facility or set of facilities operated by the organization to the full ecosystem of suppliers, partners and customers.
- **Contextualization.** Data points are not the goal; insights are. With contextualization that stratifies risk and helps prioritize action, organizations may be able to save time and money.

- **Support for pervasive mobility.** More and more of the workforce—and in fact, the extended, virtual enterprise—is now mobile. Predictive analytics platforms must support different device form factors and must work reliably and flexibly over long distances and different networking environments.
- **Easy training of, and use by, non-technical teams.** It's been said that security is an organizational imperative and must be embraced by everyone, not just those in the SOC. Customized dashboards and visualizations are needed.
- **Architectural flexibility.** Cloud computing, of course, is not a one-size-fits-all solution. Nearly all enterprises have a multi-cloud architectural layout, often including hybrid cloud/on-premises architectures. A predictive analytics security solution should operate seamlessly and flexibly across all enterprise clouds in order to properly analyze behavior and threats across all workloads, applications and data, regardless of location.

Leveraging Deloitte's knowledge, experience and Google Cloud technology

Organizations looking for a powerful, flexible, contextualized and high-performance predictive analytics platform need to find an advisor with technical experience, business acumen and a third-party ecosystem of relationships that leverages other security knowledge. **Deloitte's Predictive Analytics for Cyber in Enterprises (PACE™)** is a cloud-native platform built on Google Cloud's tech stack that combines multiple security and analytics tools in a single-pane-of-glass management framework.

It is built upon Deloitte's own cyber risk quantification and reporting engine, enabling persona-driven decision-making that increases visibility, enhances insight and speeds response and action time. PACE also uses the powerful threat-hunting functionality of Google Cloud Chronicle, as well as BigQuery[3] machine language algorithms and the Looker[3] data discovery and visualization business intelligence platform.

To address the many security-related data challenges, PACE offers:

- Complex, sophisticated reporting that combines contextualization with actionable reporting
- Support for certain new workforce models that require new types of perimeter defenses and align with "radically decentralized" user locations
- Intelligent alignment of proliferating security telemetry, such as signals emanating from devices, applications, cloud services and internet of things (IOT) systems

The result is actionable insights that allow technical and non-technical teams alike to take steps to improve the organization's security posture before threats hit and do damage. PACE provides sophisticated, yet easy-to-understand dashboards and visualizations, powerful machine learning models and a risk-based decision-making framework.

This culminates not only with an improved security posture, but also with a more efficient use of personnel, existing tools and budgets.

Finally, Deloitte complements this cutting-edge technology platform with its vast global resources, including more than 5,500 cyber professionals and 1,000-plus Google Cloud-certified practitioners. This has allowed Deloitte to be recognized as Google Cloud's Global Services Partner of the Year for three consecutive years, with specializations across security, machine learning, managed services and more.

PACE provides sophisticated yet easy-to-understand dashboards and visualizations, powerful machine learning models and a risk-based decision-making framework.

Conclusion

As cybersecurity becomes an increasingly vital and strategic part of all organizations' business operations, it is essential that security professionals are enabled to take smart, focused and timely action on the right signals and not be overwhelmed by all the noise generated by huge numbers of data sources. Organizations that embed predictive analytics into their security frameworks can benefit from better context to ensure that their security isn't just "as good as everyone else's" but is actually a source of competitive advantage.

Deloitte's PACE platform is designed for today's increasingly noisy security environment, and helps organizations optimize scarce security resources for better detection, prevention and remediation.

For more information on Deloitte PACE, please visit: **www.deloitte.com/us/pace**

1 Tunggal, Abi Tyas. "What is the Cost of a Data Breach in 2021?" UpGuard, https://www.upguard.com/blog/cost-of-data-breach. Accessed 14 May 2021.

2 Cennatan, Ron. "The Coronavirus Pandemic is Widening the Cybersecurity Skills Gap." Security Boulevard, https://securityboulevard.com/2021/02/the-coronavirus-pandemic-is-widening-the-cybersecurity-skills-gap. Accessed 14 May 2021.

3 "Cloud Computing Services | Google Cloud". Google Cloud. https://www.cloud.google.com. Accessed 14 May 2021.

Deloitte.

This content was commissioned by Deloitte and produced by TechTarget Inc.