WHITE PAPER

Next-generation Cyber Defense Center – Are You Ready?

Lead Analyst:

Wolfgang Schwab

PAC, September 2021

Commissioned by

Infosys

PAC

a teknowlogy group company

CONTENTS

CYBER SECURITY IN THE AGE OF DIGITALIZATION – ARE YOU READY?

Cyber security is one of the most dynamic topics in the IT industry. As advanced threats and technologies are introduced, security managers often find themselves a step behind. It is not easy to separate the wheat from the chaff – to distinguish between the next buzz word and the next really important topic that should be evaluated for their own organizations and, if useful, further observed or deployed. With the rapid adoption of digitalization, organizations need to accommodate new and technologically advanced elements to ensure that their businesses remain relevant. Some of these include:

- **Smart products**: Smart products are key elements of many digitalization strategies. They often enable new services and business models and, as a result, strengthen customer loyalty. Users of smart products are offered benefits such as predictive maintenance functionality or are provided with new features during the lifetime of a product. From a security perspective, communication between the product and the manufacturer is critical.
- **IT/OT integration**: For decades, operational technology (OT) and information technology (IT) used to be separate, as there was simply no reason to integrate those two areas. Stable OT systems were basically left untouched during the lifetime of a production plant, while IT has always needed frequent changes and has been vulnerable to cyber security issues. Nowadays, the concepts of digitalization, Industry 4.0, and IIoT make the convergence of IT and OT mandatory, in order to optimize business models and production agility. From a security

80%

of companies worldwide indicate that digitalization triggers further security measures.

PAC CxO Survey

47%

of companies worldwide indicate that IoT makes it harder to control operational technologies such as ICS and SCADA.

PAC CxO Survey

perspective, the risk of exposing potentially unprotected and outdated systems to external threats is unthinkable.

- **Ecosystem integration**: Digital transformation must not be confined to physical offices. Companies must quickly think one step further and push the development of digital ecosystems beyond corporate boundaries. In terms of digital transformation, many companies still focus on operational efficiency: 58% of organizations say the main goal of their digital transformation project is the optimization of internal processes. In the long run, this is just not enough. Businesses provide access to critical internal systems to partners over the internet, without evaluating the security risks. Statistics show that from a global perspective, companies in Europe in particular are lagging behind in this regard. In order to safeguard their operations and keep breaches at bay, businesses must ensure they have robust security strategies in place.
- **Working from home**: In 2020, the COVID-19 pandemic made it necessary to quickly move the workforce to remote working in order to maintain business continuity. In January 2021, it became clear that this situation would continue for some time and that at least some of the employees would like to maintain this modus operandi even after the end of the pandemic. Corresponding advantages in terms of office space, efficiency, and employee satisfaction, among other things, often make home offices interesting for companies even in normal times, but only if technical possibilities for efficient collaboration have been created and all organizational measures have been taken care of. From a security perspective, remote access to data and applications, as well as any endpoints used (even those not owned by the company) need to be secured.

"As cloud usage increases significantly, security aspects will be very important now and in the future."

CIO, public sector, Austria, 1000-2499 employees

In addition, there are numerous threats from hacker groups that are steadily growing and constantly challenging security managers. Ransomware, APTs, and social engineering attacks are just a few examples of a wide range of threats.

Cyber security has become an important strategic imperative and enterprises today need to defend and monitor their information technology assets and systems from the ever-changing cyber threat landscape. A robust and comprehensive Cyber Defense Center (CDC) is core to building an effective cyber security program.

WHAT YOU REALLY NEED IS A COMPREHENSIVE CYBER SECURITY FRAMEWORK IN THE FORM OF A NEXT-GENERATION CYBER DEFENSE CENTER – INTERNALLY OR AS CONSUMER SECURITY AS A SERVICE

In order to design, operate, and manage cyber security in an enterprise effectively, it is necessary to have a clear overview of the topic, and actions have to be taken in a consistent and correlated manner. CDCs bring together best-in-class skills and constantly updated solutions, providing noiseless security operations round-the-clock through a world-class network of interconnected, global facilities. These entail:

- **Cyber security strategy**: The cyber security strategy needs to be an integral part of the overall IT strategy of an organization. It has to be aligned with the mission and vision of the organization and embedded at the design stage while developing a system or a product. It holistically protects information and systems from cyber attacks and is a business enabler that defends networks, data, and infrastructures from threats, risks, damage, and unauthorized access.
- **Governance, risk & compliance**: GRC summarizes the three most important levels of action for the successful management of a company. This concept is also important for security. **Governance** is the management of cyber security according to defined guidelines. This includes the definition of corporate security goals, the methodology to be applied, and the planning of resources required to achieve them. **Risk** refers to the management of known and unknown risks through defined,

"Most enterprises need professional help in the cyber security field as talent is rare and expensive and the risk vectors are often overwhelming. Capable service providers are a handy option!"

Wolfgang Schwab, Head of Cyber Security, PAC

regular risk assessments. An important factor here involves dealing with risks at an early stage, and providing strategies to minimize risks. **Compliance** refers to adhering to internal and external standards for the provision and processing of data. This includes, among other things, specifications with regard to standardization efforts and access regulations for data, as well as legal framework conditions. GRC for security must be aligned with the enterprise-wide GRC model and is the core business of the Chief Security Officer in collaboration with the board and the CIO. Nevertheless, external service providers and consultants can help with methodologies and frameworks and provide specific knowledge around external compliance regulations such as the NIS directive, GDPR, ISO 27001, ISO 22301, or IEC 62443, to name but a few.

- **Monitoring existing and emerging technologies**: Most cyber incidents and breaches occur due to poor security hygiene in an organization's technology ecosystem. Also, new technologies such as AI, RPA, IoT, and IT/OT integration are important from a business perspective, but they introduce new risks which need to be addressed by embedding security controls into design, implementation, risk assessment, and overall security operations. Service providers are usually far ahead of single customers with respect to experience and knowledge of how emerging technologies can be secured or directly used for security purposes, and this knowledge should be valued.
- **Vulnerability management**: Vulnerability management is one of the foundational cyber hygiene elements for a CDC. This function is no longer limited to the identification and communication of vulnerabilities to the different stakeholders. Next-generation CDCs take a more comprehensive view of this function in order to influence the overall detection and also the remediation of any vulnerabilities. The key aspects include:

  (a) Identifying the threat surface area of the enterprise and ensuring that the asset database is kept current;

  (b) Effective vulnerability identification, leveraging continuous scanning and authenticated scans;

  (c) Prioritization of the identified vulnerabilities based on an inside-out view, which includes threat activity, exploit availability, placement of the asset within the client network, and last but not least, the business criticality of the asset;

  (d) Effective stakeholder identification and management to improve the vulnerability remediation SLAs and governance, supported by metric reporting and issue discussion involving the cyber security team, technical support teams, and the business owners.

  KPIs need to move from scan coverage, speed and effectiveness of vulnerability identification, to remediation rates and remediation SLA

"Cyber security is mission-critical for regulatory compliance."

CISO, automotive, Germany, 10,000+ employees

43%

of companies worldwide agree that they lack internal cyber security skills.

PAC CxO Survey

compliance. Effective vulnerability management is a shared responsibility of the cyber security team, technology teams, and business teams, and the establishment of a governance structure to enable collaboration is a key ingredient that can help enterprises to prevent >80% of breaches.

- **Identity & access management/ identity governance & administration**: IAM is a pretty mature topic in cyber security, but in times of digitalization, new challenges do arise. Not only do employees need identities and access rights to systems, applications, and data, but also to ecosystem partners, customers, IoT devices, and smart products. Most legacy IAM systems are simply not able to manage these new challenges efficiently. With operations and data rapidly shifting to the cloud, organizations are facing a mammoth challenge of continuous governance and adhering to compliances across cloud and hybrid infrastructure, especially related to identity and accesses. Service providers can enable their clients to build, operate, and evolve their identity lifecycle and governance processes with risk-based intelligent authentication and authorization across the digital ecosystem and provide and manage solutions in an as-a-service model. This leads to modern and future-proof identity governance & administration solutions.

42%

of companies worldwide agree that in general, their employees do not pay much attention to cyber security.

PAC CxO Survey

- **Infrastructure security**: Infrastructure security is one of the most comprehensively addressed topics in cyber security. However, new trends such as micro-segmentation, zero trust, and SASE, along with cloud adoption, IT/OT integration, etc., bring additional complexity. Service providers can enhance cyber defense by offering cyber security skills and deploying best-in-class protection controls and operational capabilities, which is hard for companies to handle internally.
- **Data privacy & protection**: Data privacy & protection is a segment of data security that deals with the proper handling of data – including permission, notification, and regulatory obligations. Data privacy & protection concerns cover whether or how data is shared with third parties; how data is legally collected or stored; and compliance with regulatory restrictions such as GDPR, HIPAA, GLBA, or CCPA. Relatively frequent changes, varied region-specific laws, and tightening of legal requirements make it difficult, especially for international companies, to keep up with all the different requirements and implement them in accordance with the law without hindering business operations in the long term. Therefore, collaboration with an experienced service provider can help to improve visibility and control of sensitive data in compliance with regulatory and business requirements.

81%

of companies worldwide agree that deadlines for becoming compliant with new regulatory obligations trigger security measures.

PAC CxO Survey

- **Threat detection and response**: The topic of threat detection and response is closely linked to security operation centers and security information and event management, in combination with incidence response. In recent years, the idea has gained acceptance that while all security measures are necessary, it must still be assumed that they are not sufficient to intercept all threats. SOCs have been built accordingly. AI has recently been used to develop more ways to improve monitoring of network traffic, user behavior, and anomalies on the one hand, and to automate appropriate countermeasures on the other. While only very few enterprises are able to deploy and run such automated threat detection and response systems on their own, an experienced service provider can.

- **Cloud security**: With the rise in cloud adoption across the globe, cloud security is a particularly vital aspect that needs to be considered. It involves strategies and policies that are formulated for the protection of data and IT infrastructures with regard to cloud computing. With the introduction of Bring Your Own Cloud (BYOC)/ remote working, employees use applications to store the enterprise's data, which makes the data vulnerable to being breached. Factors such as diminished customer trust, loss or theft of intellectual property, and cloud services used as means of data exfiltration urge the need for a strong cloud security architecture in an organization. Clearly, the responsibility for security should be an integral part of the different models applied in the cloud – SaaS, PaaS, and IaaS.
- **Security architecture**: Cyber security architecture is the foundation of an organization's defense against cyber threats and ensures that all components of its IT infrastructure are protected. Environments that are secured by cyber security architecture include cloud, networks, IoT, endpoints, and mobile. The security architecture helps to position security controls and breach countermeasures and establishes how they relate to the overall systems framework of the company. The main purpose of these controls is to maintain critical systems' quality attributes such as confidentiality, integrity, and availability.

In order to secure a company in the best possible way and to mitigate possible threats or breaches as quickly as possible, all of the aforementioned aspects need to be addressed. Only very few enterprises will be able to do so efficiently internally. While security strategy and GRC should be driven by the company itself – with the methodological help of a service provider, the other tasks can be efficiently outsourced to a service provider. Usually, the internal security team is busy with strategic questions and collaboration with different service lines of business and IT. Therefore, it makes sense to free them from the day-to-day standard operations. Depending on the size of the internal team and its capabilities, service providers can either be used selectively, or entire blocks of tasks can be outsourced.

In any case, the contract design should be as flexible as possible and should reflect a pay-per-use model.

81%

of companies worldwide are planning additional investments in governance, risk & compliance tools and services.

PAC CxO Survey

87%

of companies worldwide are planning additional investments in infrastructure-based solutions and services.

PAC CxO Survey

INTERESTING INFOSYS SUCCESS STORIES

Success Story 1: Managed security services for a leading global resources company

The client is an Australian company and a leader in the mining and energy sector, with a complex environment of multiple tools and security solutions. It wanted to consolidate its services with fewer vendors. Infosys helped with the smooth transition, delivered global support, streamlined processes, and enhanced the security posture of the organization.

Challenges faced by the client:

- Lack of a robust solution providing threat intelligence, threat hunting, and malware analysis
- Lack of updated asset inventory of target hosts and a well-defined vulnerability management (VM) process for the end-to-end VM life cycle
- Complex security platform with 300+ firewalls from multiple solution providers
- Difficulty complying with clients' organization policies and guidelines, as well as with regulatory compliance requirements

Solution provided by Infosys:

- Established a 24x7 global SOC team to monitor and defend security incidents. Implemented and set up threat intelligence and hunting platforms for proactive security monitoring.
- Asset classification, risk model finalization, scanning, and patch advisory
- Set up a technical security assessment team to help inculcate security in the design and architecture stage of the project
- Provided 24x7 firewall support to transition and manage complex network operations

Value delivered to the client:

- 24x7 operational support in security monitoring and network operations
- Improved security posture by providing active threat indicators collected from sources across the globe
- Reduced open vulnerabilities, automated scanning, and enhanced remediation processes
- Provided services to ensure that client is Secure by Design

Success Story 2: Effective threat detection and response framework for a US-based healthcare organization

The client is a US-based, multi-state healthcare organization that wanted to revamp its infrastructure security services and set up operational processes with an effective threat detection and response framework. Infosys helped by providing end-to-end infrastructure security, cloud security, threat detection, and response services.

Challenges faced by the client:

- Difficulty in migrating to the cloud with end-to-end infrastructure and cloud security
- Adhering to domain-specific security audit and compliance requirements
- Unable to provide converged threat detection and response services to the hybrid environment with specific use cases and security monitoring processes

Solution provided by Infosys:

- Implemented a security information and event management (SIEM) solution
- Provided 24x7 threat detection and response, security operations & real-time monitoring
- Supported endpoint security, data loss prevention (DLP), SIEM, and GRC solutions
- Established and implemented OS hardening standards for Windows and Unix/Linux platforms

Value delivered to the client:

- From no SLA to measurable SLA metrics for response & recommendation time
- Processes and policies aligned and compliant with HIPAA and ISO27001
- Extended coverage for 24x7 real-time security incident management, security tool management, and critical server security management

Success Story 3: Cyber Watch services for an American beverage company

The client is an American multinational corporation, manufacturer, retailer, and marketer of non-alcoholic beverages. It was lacking a transformation environment for consolidation of services and tools. Infosys helped by providing managed security services via Cyber Next Platform.

Challenges faced by the client:

- Limited threat detection and intelligence capability to keep pace with the increasing threat landscape
- Infrastructure and administrative overheads increasing at a fast pace
- Unable to implement a standardized security solution for the large bottler community, leading to perceived business risks

Solution provided by Infosys:

- Transformed existing solution to multi-tenanted Cyber Watch solution with 24x7x365 security monitoring services
- Enabled 150+ advance use cases for threat detection
- Provided cyber threat intel and brand monitoring services to improve security posture
- Integrated assets on Azure, AWS Cloud, and in data center
- Provided a standard and scalable solution for the bottler community
- Initiated SLA-based, scalable global delivery models

Value delivered to the client:

- Attained faster time to value by onboarding to Cyber Watch in just 4 weeks
- Managed services now provided to secure 30,000+ internal users, 50,000+ external users, and 27,000+ endpoints and 2,000+ servers
- Pay per use – EPS-based OPEX and predictable charging model

Success Story 4: Data privacy and protection solution for a leading building material manufacturer

The client is a leading building material manufacturer. Its main area of concern was to have effective security controls for prevention and remediation of data loss incidents. Infosys helped by proposing and implementing data loss prevention (DLP), cloud access security broker (CASB), and data classification solutions to holistically address the client's data security concerns.

Challenges faced by the client:

- Loss of intellectual property
- Adoption of cloud platform solution for scalability and operational flexibility
- Effectiveness of security controls in addressing data loss incidents
- Remediation of data loss incidents and reduction of false positives

Solution provided by Infosys:

- Rolled out endpoint DLP implementation pilot for 400 business users
- Set up Symantec Elastica CloudSOC CASB solution to monitor Office 365 applications
- Integrated Symantec DLP and Elastica CloudSOC to provide centralized DLP incident monitoring capabilities
- Implemented Titus Data Classification solution for business users to classify sensitive enterprise data and large volumes of historical data
- Provided post-implementation support along with policy management for DLP infrastructure, data classification, and CASB solution

Value delivered to the client:

- Effective management of data loss risks via the implementation of a DLP solution
- Increased data security and efficient handling of sensitive data by business users via proper classification of data
- Enhanced data security through the augmentation of data classification capabilities to strengthen DLP detection
- Reduction of false positives by fine-tuning DLP policies

ANNEX

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE

The creation and distribution of this paper was supported by Infosys.

For more information, please visit www.sitsi.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in September 2021 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

This study is protected by copyright. Any reproduction or dissemination to third parties, including in part, requires the prior explicit authorization by Infosys. The publication or dissemination of tables, graphics etc. in other publications also requires prior authorization.

Independence

This study was produced by Pierre Audoin Consultants (PAC). Infosys had no influence over the analysis of the data and the production of the paper.

ABOUT INFOSYS

Infosys is a global leader in next-generation digital services and consulting. We enable clients in 45 countries to navigate their digital transformation. With over three decades of experience in managing the systems and workings of global enterprises, we expertly steer our clients through their digital journey, by enabling enterprises with an AI-powered core that helps to prioritize the execution of change. We also empower businesses with agile digital at scale to deliver unprecedented levels of performance and customer satisfaction. Our always-on learning agenda drives continuous improvement by building and transferring digital skills, expertise, and ideas from our innovation ecosystem.

Digital transformation and increased adoption of emerging technologies have led to the attack surface being broadened significantly, and defense has become more complex. Enterprises today need to invest in a next-gen packaged solution and avoid the complexities and overheads of multiple point solutions, in order to build a cost effective and secure IT landscape. There are also many other roadblocks in establishing a secure and holistic enterprise IT architecture, including a lack of integration in security products, managing licenses of each product, long procurement cycles, and a lack of skilled people to manage and operate ever-evolving technologies.

Today's businesses need a proactive and preventive security solution that can cater for all kinds of incidents, threats and vulnerabilities. Infosys Cyber Next – Platform Powered Services is a comprehensive package of security products and associated services that provides a ready-to-use managed protection, detection and response solution to organizations. It is a fully managed security-as-a-service package that comprises 6 applications or modules, offering:

- Detection and proactive hunting of security incidents and automated responses for containment and remediation
- Intelligence of the latest threats that could damage the business and the names and signatures of threat actors actively targeting the organization or similar organizations
- Vulnerability management across all threat surfaces
- Metrics, architecture and controls that enable effective security governance

In the event of a lack in coverage of security needs, Infosys is able to compensate thanks to its indigenous technologies, enhanced with Infosys' proprietary content gained from vast research and rich experience. These come from use cases, playbooks, SOPs, security metrics and architecture.

Built on a modern software stack, comprising technology solutions and Infosys IPs created in collaboration with the Infosys Innovation Hub, Cyber Next brings the power of technology and cyber security excellence to our customers to fulfil the promise of securing their future.

Contact:

Infosys Limited

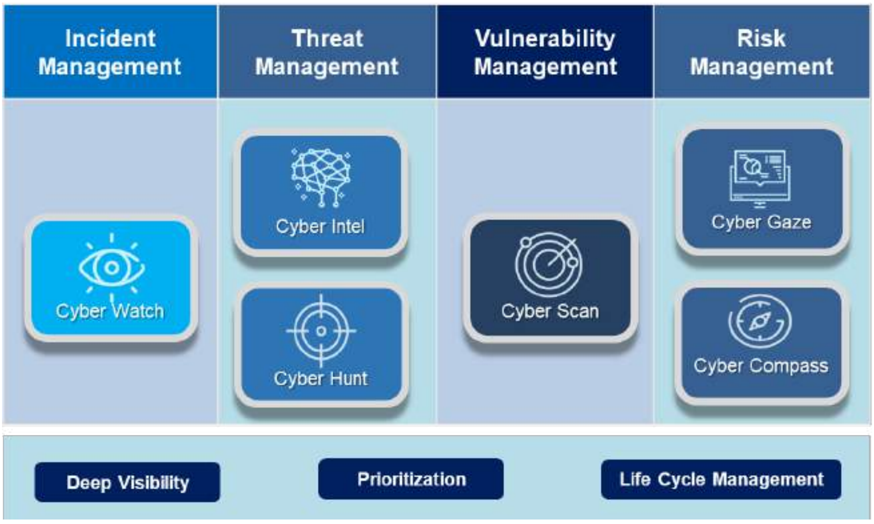
Infosys Bangalore, Plot No. 44, Hosur Rd, Konappana Agrahara, Electronic City, Bengaluru, Karnataka 560100

CyberSecurity@infosys.com

www.infosys.com/services/cyber-security

Infosys Cyber Next – Offerings

Cyber Next – Platform Powered Services is made up of the following six services, which ensure holistic security at any given point in time, handled and deployed by highly skilled security analysts in our niche globally distributed Cyber Defense Centers (CDCs) network.



Key Features

The platform ecosystem enables enterprises to leverage pre-built, scalable infrastructure security platforms that can be extended for enterprise specific requirements in security monitoring, security analytics, threat intelligence and advanced security controls such

as EDR, deception technology and malware analysis. The unique features of Cyber Next are as follows:

- Comprehensive – A one-stop-shop solution for enterprise security, including multiple security solutions that address the full spectrum of security requirements
- Scalability - The platform will scale to accommodate increasing numbers of customers and increased usage
- Includes Infosys IP - Home-grown analytics platform using AI and ML to perform deep correlations and advanced analytics to detect anomalies
- Multi Tenancy - Supports multiple tenants with logical segregation to provide economies of scale
- Orchestration & Integration - The platform orchestrates and automates security responses to contain damage from incidents by integrating with customers' security devices
- Faster Solution Set-Up - Development, testing and production of tenant available as "Ready to Use" model, demonstrating faster business value to stakeholders

- Deep Research - Malware analysis, adversary tools and customer abilities analysis to protect the enterprise
- Pay per Use - OPEX model of pricing allows customers to pay only for capacity utilized

Benefits

- Reliable IT infrastructure and systems, providing interruption-free business operations for the enterprise
- Access to a range of on-demand SLA-based Managed Security Services, leading to minimized cyber security risks and reduced costs of compliance
- Availability of real-time dashboards and reports, providing insights on a range of key cyber security metrics on a regular basis
- Trusted advisory services to keep the enterprise up to date to prevent cyber security breaches
- End-to-end services handled in a unified manner, providing peace of mind to stakeholders

Business Value

- Comprehensive platform capabilities to cover the security operations life cycle
- Prepackaged, integrated, validated and ready to onboard customers
- Delivered from CDCs (Cyber Defense Centers) at scale with constantly upskilled and cross-skilled expert professionals
- Subscription-based and outcome-oriented pricing model
- Monitoring and advanced threat hunting capabilities to eliminate tool gaps

ABOUT TEKNOWLOGY GROUP

teknowlogy Group is your partner of choice for European focused IT market data, insights and advice. It brings together the expertise of two research and advisory firms, each with a strong history and local presence in the fragmented markets of Europe: CXP and PAC (Pierre Audoin Consultants).

We are a content-based company with strong consulting DNA. We are the preferred partner for European user companies to define IT strategy, govern teams and projects, and de-risk technology choices that drive successful business transformation.

We have a second-to-none understanding of market trends and IT users' expectations. We help software vendors and IT services companies better shape, execute and promote their own strategy in coherence with market needs and in anticipation of tomorrow's expectations.

Capitalizing on more than 40 years of experience, we are active worldwide with a network of 50 experts.

For more information, please visit www.teknowlogy.com and follow us on Twitter or LinkedIn.

a teknowlogy group company

Contact:

PAC GmbH

Holzstr. 26
80469 Munich, Germany

+49 (0)89 23 23 68 0
info-germany@teknowlogy.com
www.vendor.teknowlogy.com
www.sitsi.com

PAC

a teknowlogy group company