الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies

Cybersecurity Quarterly Bulletin

Q3 2020

Classification: Public
TLP: White

Contents

Highlights from the Quarter

Q3 2020 (July - September)

- From a local perspective, the National Cybersecurity Strategy was approved – on the 15th of September – by the Cabinet. The National Cybersecurity Strategy developed by the NCA aims at building a resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity.
- From a global perspective, although the pandemic is still affecting the cyber industry, some noteworthy recommendations to address cybersecurity risks emerged in this quarter. In addition to good practices to protect organizations against a cyber pandemic, key guidelines were also issued. MITRE released the 'Shield' Active Defense Framework to counter network intruders, while new roadmaps were created to help organizations deploy the 'Zero Trust' model.

Bits and Bytes

Key statistics from the quarter

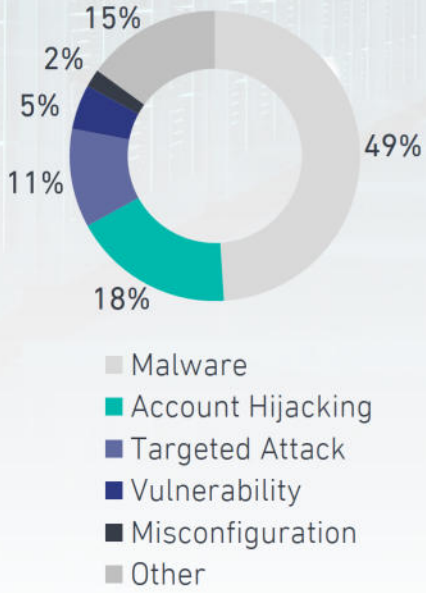
The average time to identify and contain a data breach[1]
This average "lifecycle" combined 207 days to identify a breach with 73 days to contain one.

The average savings for containing a breach in less than 200 days[2]
For over 200 days, the average cost is SAR 16.2 million vs. SAR 12 million for less than 200 days.

Of organizations faced a cybersecurity breach due to insecure remote working[3]
This increased cyber incident response costs.

The healthcare sector has the longest lifecycle across all sectors globally[4]
The average time to identify and contain a breach varies widely between sectors.

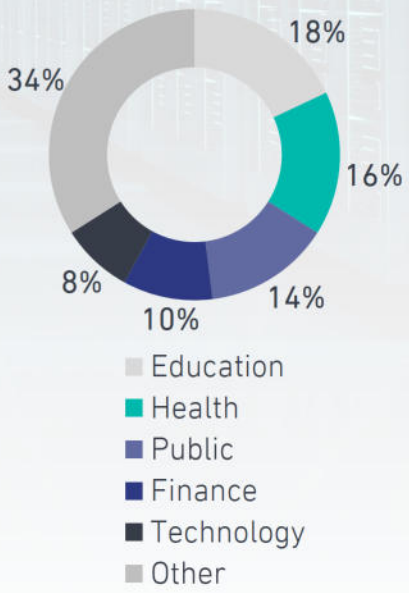
Top 5 global threats in Q3 2020 *



Top 5 threats in KSA in Q3 2020 **

#1	Malicious Code
#2	Intrusions / Attempted Intrusions
#3	Unauthorized Access, Modification, and Usage
#4	Information Leakage / Abuse
#5	Phishing Attacks

Top 5 targeted sectors globally in Q3 2020 *



* Numbers show the distribution (%) over the total number of cybersecurity threats registered worldwide for Q3.

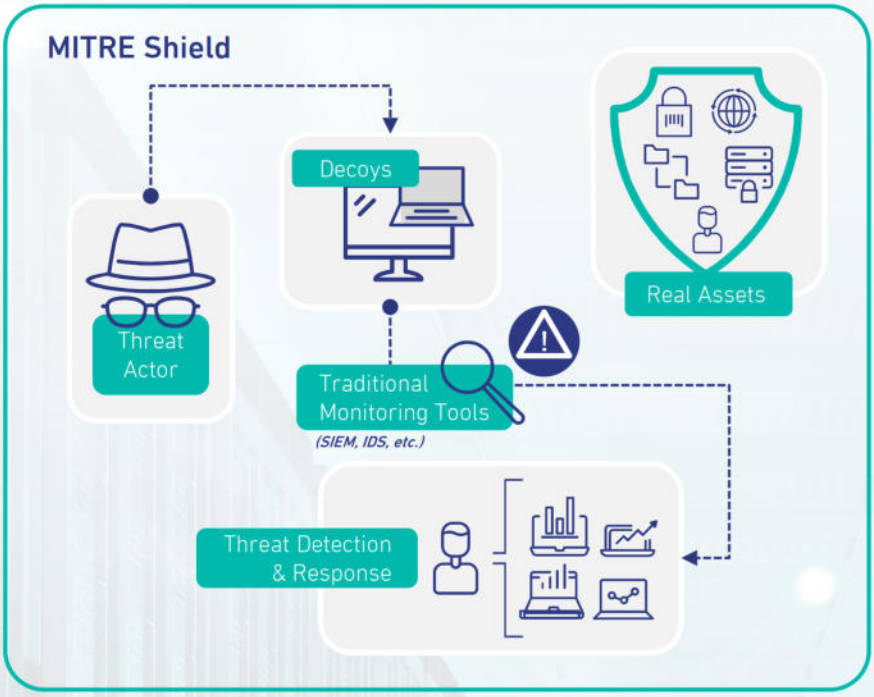
**NCA analysis. Numbers show the top cybersecurity threats registered in the Kingdom of Saudi Arabia for Q3.

Global Cyber Outlook

Cybersecurity headlines from around the world

MITRE Shield: An active defense against network intruders

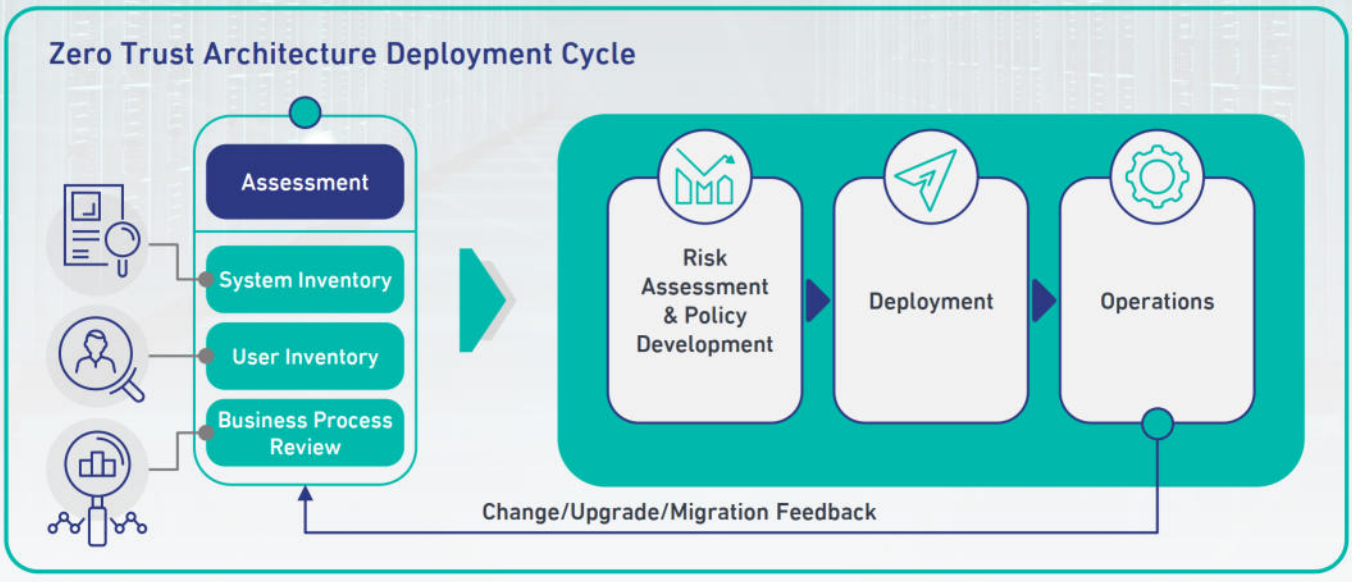
MITRE Shield is a knowledge base that provides cyber professionals with techniques and tactics to deal with intruders and prevent them from attacking the organization's network.[5]



Based on cybersecurity techniques for deception and adversary engagement, Shield aims to lure attackers into targeting decoy systems while keeping them away from the organization's real assets. In contrast to traditional security techniques, such as firewalls, adversary engagement allows cybersecurity professionals to learn about attackers' behavior and capture some of their tools.

A roadmap for deploying 'Zero Trust'

Zero Trust assumes that no one – from inside or outside the network – can be granted access rights by default. With its principle of user, device, and infrastructure verification before granting conditional access based on least privilege, the Zero Trust security model is growing as part of the key initiatives to mitigate cyber risk.[6] The NCA has included the zero-trust concept in the recently published "General Principles of Secure-by-Design."[7]



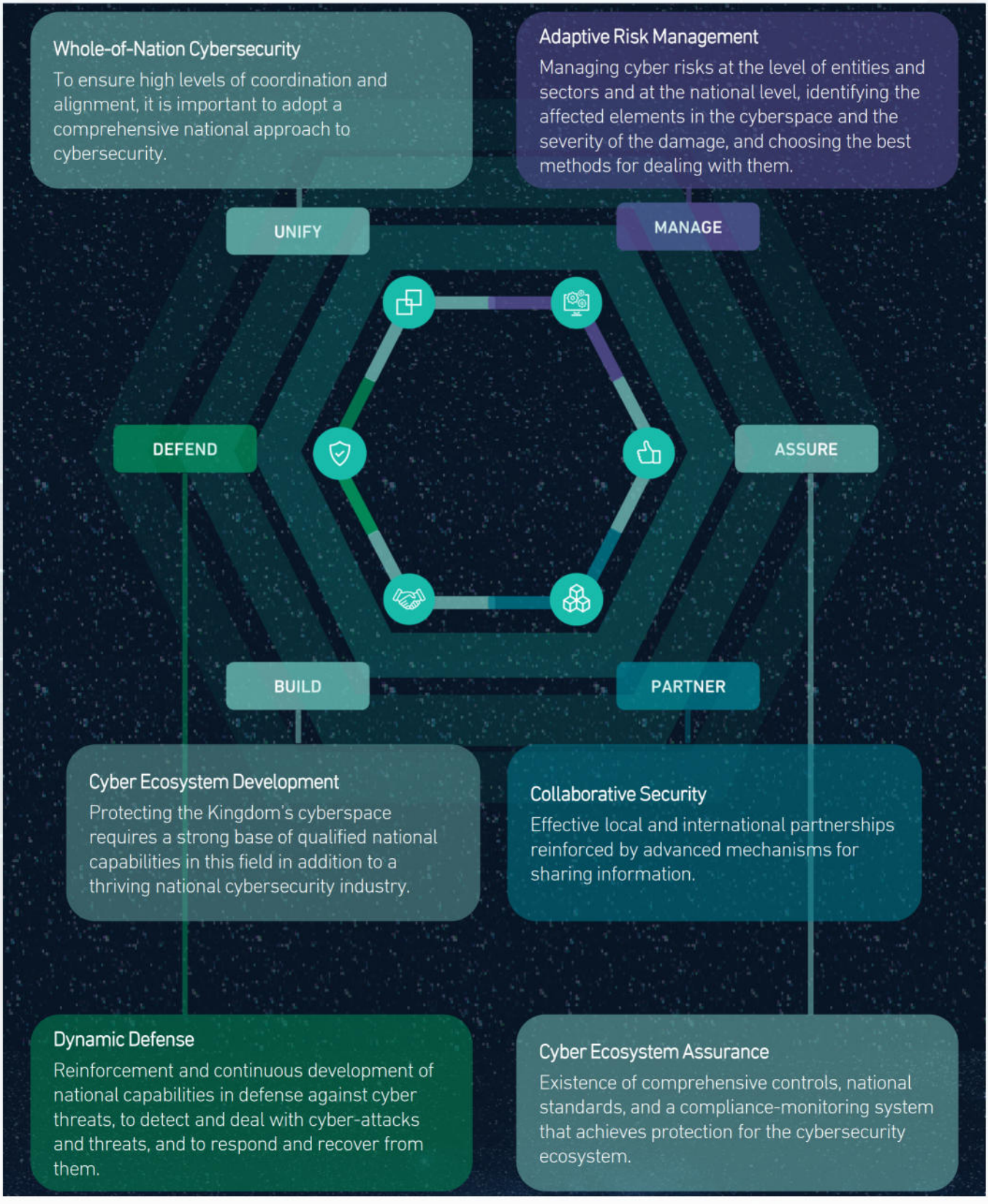
The National Institute for Standards and Technology unveiled the Zero Trust Architecture (ZTA) publication,[8] which provides a roadmap to deploy ZTA from the identification of critical assets to operation. The publication also discusses ZTA's threats and mitigation techniques.

Saudi Cyber Outlook

Cybersecurity headlines regarding the Kingdom of Saudi Arabia

National Cybersecurity Strategy (Approval date: 15 September 2020)[9]

The NCA has developed a national strategic vision for cybersecurity which reflects the ambition of the Kingdom in a manner that balances security, trust, and growth. The national vision that the NCA aims to reach is: a resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity. In order to achieve this, the NCA has set six main goals:



Top Cybersecurity Stories

Social Media Cybersecurity Incident

Location: Worldwide (mostly US)

Sector: Web / Social Media

Date of disclosure: July 15, 2020

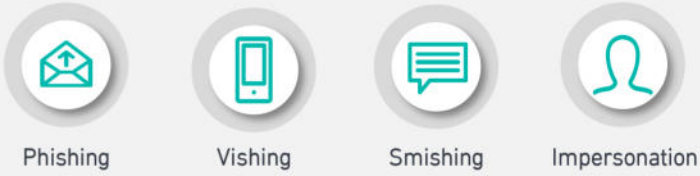
Type of attack: Social engineering

Description: Social media accounts of influential people began tweeting malicious messages to their followers. Malicious messages reached almost 350 million users. From the company's administration panel, the intruder could reset the email address associated with an account and disable the two-factor authentication.[10]

Impact: Out of the 130 targeted accounts, intruders used 75 of those to tweet scam messages and were able to view personal information such as email addresses, phone numbers, and other sensitive data.

Lesson learned: Social media platforms need to cross-check their security measures. Companies should put in place periodic training to raise employee' awareness of social engineering techniques and manage employees' access privileges to limit data use to the scope of their roles.

Different types of social engineering



Tesla Insider Breach

Location: US

Sector: Transport

Date of disclosure: August 19, 2020

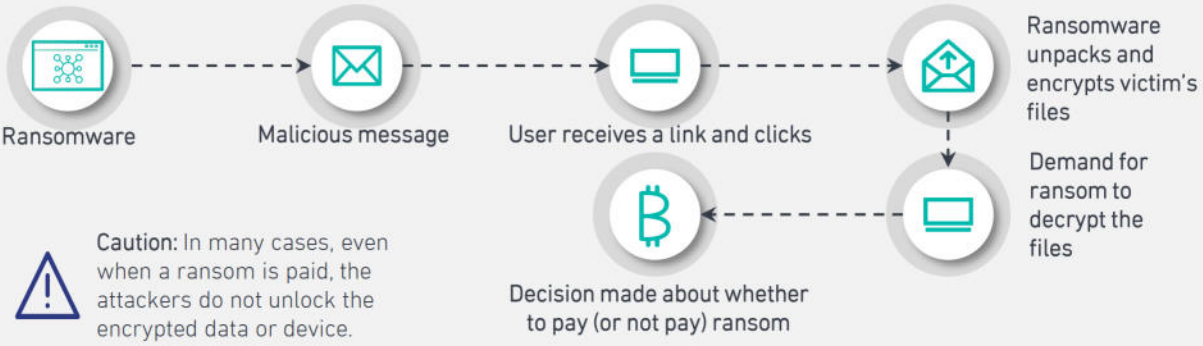
Type of attack: Ransomware

Description: The attempted cybersecurity attack consisted of persuading a Tesla employee to insert malware into the Nevada factory network. After inserting the malware, a DDoS was launched to extract data from the company's network, threatening to make it public unless Tesla paid a ransom.[11]

Impact: This attempted attack was a near-miss. This attempt serves as a cautionary tale to companies.

Lesson learned: Companies should implement an anti-ransomware plan, which includes providing regular updates to employees on the current status of crisis response activities, enhancing their security policies, and monitoring employee accounts to detect unusual activities.

Life-cycle of a ransomware attack



Cyber Secure

How to deal with a cyber pandemic

Saudi CERT released guidelines on cybersecurity awareness for remote education

The Saudi Computer Emergency Response Team (Saudi CERT) has issued guidelines on safe computer use. As a result of the global health crisis, KSA has accelerated the e-learning process through its accredited platforms, in line with national measures to counter the COVID-19 pandemic. The Learning Securely cybersecurity campaign aims at educating students, their parents, and their teachers about online learning good practices.[12]

Tips to protect your organization against a cyber pandemic

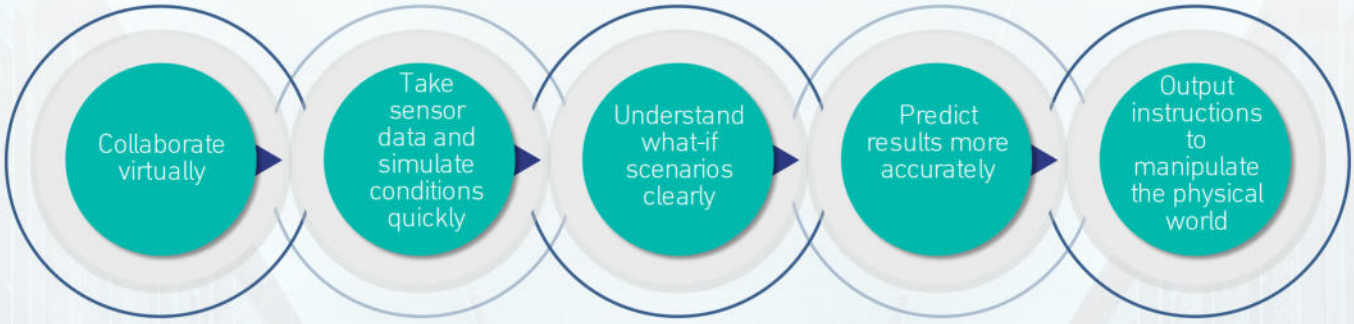
A cyber pandemic can cause business disruptions to soar exponentially. On the bright side, each year, organizations are increasingly acknowledging the indispensable role of cybersecurity in digitalization. Cybersecurity controls can help organizations pave the way to cyber-preparedness. These include:

To protect from...	Organizations can...	
Human Error	Foster a Cybersecurity Culture	Through a partnership between HR and cybersecurity departments, organizations can develop awareness training to help workers identify suspicious emails and comply with cybersecurity policies.
Endpoint Vulnerabilities	Deploy Zero Trust Model	By assuming that all devices connected to the organization's network are untrusted, organizations can mitigate the risks pertaining to multiple attack surfaces. This model is highly relevant now as remote working and dependence on cloud services become commonplace.
Cybersecurity Threats	Collaborate and Share Information	A cyber pandemic is a collective issue, so organizations will be better off if they share information. A collective situational awareness plays a crucial role in overcoming cybersecurity threats.
Third-Party Cyber Risks	Adopt a Third-Party Risk Management (TPRM)	By adopting a Third-Party Risk Management (TPRM), organizations can identify, monitor, and manage the risks posed by vendors that play a critical role in the organization's activities.

Looking Ahead: New Trends

A glance at the digital twins and cybersecurity

Among the new trends it is noteworthy to mention the digital twin (DT), which can be defined as: *the virtual representation of a physical object or system across its lifecycle. It uses real-time data and other sources to enable learning and dynamic recalibration for improved decision making.*[13] DT enables companies to optimize operating processes in a virtual world before applying them in the real one. Implementing DT consists of introducing a software model that mirrors a unique physical object, process, or entity. Its process can be described as follows:[14]



Main cybersecurity risks from digital twins[15]

- Cybersecurity gaps between the DT and the actual system can expose valuable and sensitive business information;
- The aggregation of massive data stores could increase the risk of attackers corrupting data;
- The DT that is subject to a cybersecurity attack could serve as a blueprint to the real system; and
- The inclusion of new partners in the DT production cycle increases the risk of insider threats.

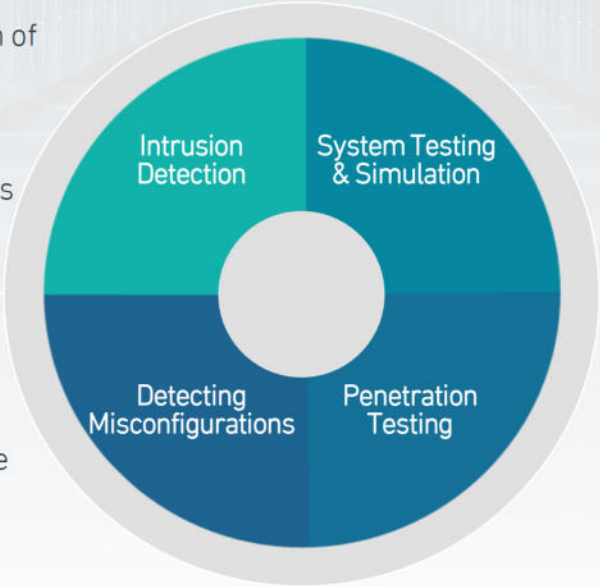
Essential standards for digital twins

- ISO 23247 - supports the creation of DTs of observable manufacturing elements;
- IEC 62832 – defines the principles of the digital factory framework;
- ISO TS 18101-1 - provides guidance for an architecture of a supplier-neutral industrial digital ecosystem.

Digital twins in practice[16]

Examples of using digital twins to improve an organization's cybersecurity:

Using a detailed specification of the production system as a template for digital twins allows the organization to monitor and report deviations from the original system.



Digital twins can be used to experiment on a clone in the virtual environment instead of relying on documentation and theoretical attack vectors.

The digital twins detect the mismatch between the real environment and the maintained specification, due to misconfiguration or manipulation by an attacker.

With a virtual mirror of the production environment, it is possible to identify weaknesses and test countermeasures before implementing them in production.

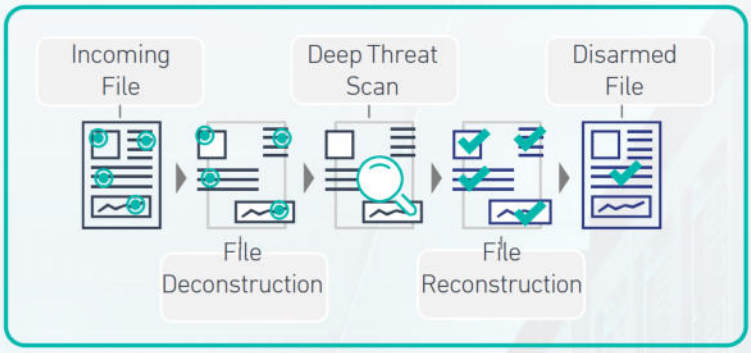
Spotlight on Cyber Innovation

Innovative solutions to cybersecurity challenges emerging from accelerator programs

By 2021 worldwide spending on cybersecurity innovations is expected to grow to **USD 1 trillion**, cumulatively over the last five-year period.[17] Accelerator programs provide a great platform for identifying potentially successful cybersecurity startups and also contribute to convening industry leaders to explore the most pressing cybersecurity issues.

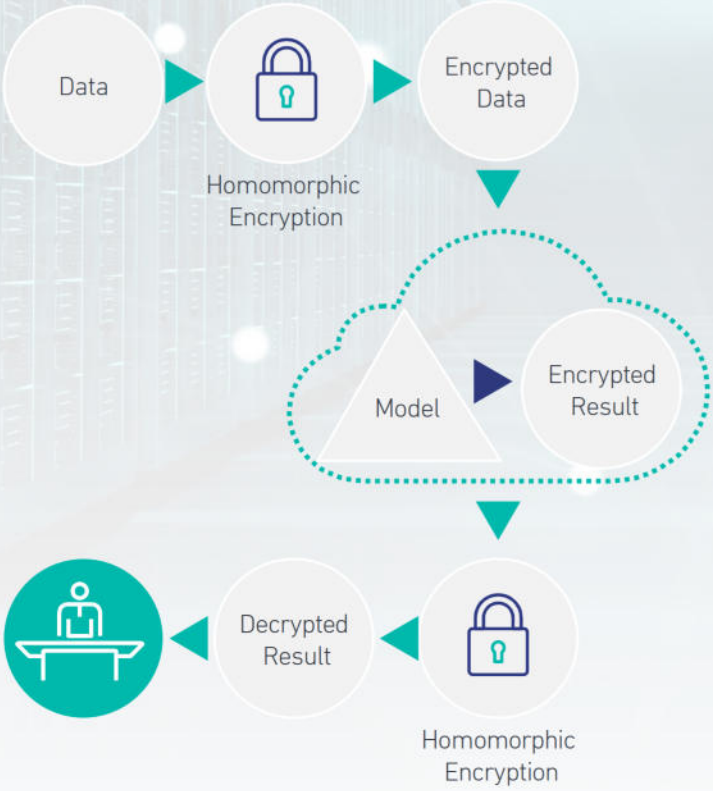
Rather than relying on traditional threat detection tools, some startups are offering cybersecurity solutions based on Content Disarm and Reconstruction (CDR) technology. CDR examines the different components of incoming files by deconstructing them and removes the components that do not comply with the organization's cybersecurity policies.[18]

Content Disarm and Reconstruction Process



Other startups are focusing on homomorphic encryption.[19] This allows organizations to share data for business analysis and generate encrypted results without handing the data's encryption key. The possibility of securely outsourcing data computing has accelerated the development of standards for this technology.

Homomorphic Encryption Explained



Homomorphic encryption can increase the level of cybersecurity and privacy controls by processing and analyzing data that is encrypted.[20]

The following business drivers are pushing for data processing that does not expose sensitive information:

- The need for cloud data outsourcing so that data processing is possible without knowing the data;
- Homomorphic encryption contributing towards secure multi-party computation.

References

[1] Cost of a Data Breach Report 2020, IBM, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/CostofaDataBreachReport2020

[2] Cost of a Data Breach Report 2020, IBM, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/CostofaDataBreachReport2020

[3] Enduring from home COVID-19's impact on business secure, Malware Bytes, 2020, https://blog.malwarebytes.com/reports/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-worker-labs-report-reveals/

[4] Cost of a Data Breach Report 2020, IBM, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/CostofaDataBreachReport2020

[5] Mitre Website https://shield.mitre.org/

[6] 2020 Zero Trust Progress Report, Plus Secure, 2020, https://www.pulsesecure.net/resource/2020zero-trust-report/

[7] General Principles of Secure-by-Design, NCA, (SBD – 1: 2020), https://nca.gov.sa/files/sbd_en.pdf

[8] Microsoft Zero Trust deployment guide for your applications, Microsoft, 2020, https://www.microsoft.com/security/blog/2020/08/27/zero-trust-deployment-guide-microsoft-applications/

[9] National Cybersecurity Strategy, NCA, 2020, https://nca.gov.sa/en/pages/strategic.html

https://twitter.com/nca_ksa/status/1306226229943640064?s=24

[10] An update on our security incident, Twitter Blog, 2020, https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

[11] Tesla employee foregoes $1M payment, works with FBI to thwart cybersecurity attack, Tesla, 2020, https://www.teslarati.com/tesla-employee-fbi-thwarts-russian-cybersecurity-attack/

[12] A guide for students on aspects of cybersecurity in distance education, NCA, 2020, https://cert.gov.sa/ar/awareness/online_learning_guide/

[13] Cheat sheet: What is Digital Twin?, IBM, January 2020,

https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/

[14] Digital Twin, Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/digital-twin;

Digital twins Bridging the physical and digital, Deloitte, 2020, https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/digital-twin-applications-bridging-the-physical-and-digital.html

[15] Expecting digital twins Adoption of these versatile avatars is spreading across industries, Deloitte, 2020, https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/understanding-digital-twin-technology.html;

Digital Twins: Understanding what they are and why they need to be protected, Security Infowatch, 2020, https://www.securityinfowatch.com/security-executives/article/21082742/digital-twins-understanding-what-they-are-and-why-they-need-to-be-protected

[16] Digital Eckhart, M. and Ekelhart, A., Towards Security-Aware Virtual Environments for Digital Twins https://www.sqi.at/resources/Towards_Security-Aware_Virtual_Environments_for_Digital_Twins.pdf

[17] https://cybersecurityventures.com/cybersecurity-market-report/

[18] https://medium.com/@adam_20838/top-content-disarm-and-reconstruction-cdr-solutions-companies-2020-9aade28f6e15

[19] Homomorphic Encryption Standardization, HomomorphicEncryption.org, 2020, https://homomorphicencryption.org/

[20] Chapter Ten - Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities, RakeshShresthaShihoKim, 2019, https://www.sciencedirect.com/science/article/pii/S0065245819300269

This quarterly bulletin has been compiled by the National Cybersecurity Authority (NCA) of the Kingdom of Saudi Arabia (KSA). Its goals are to provide readers with an overview of the most important cybersecurity events and data from the quarter and to highlight the most interesting facts related to the focus of this issue. Aiming to :

- Elevate cybersecurity knowledge and capabilities
- Provide an outlook on the latest cybersecurity trends, threats and risks

This report contains information from several parties and individuals, noting that all information included in the report is indicative only. Also, the NCA does not bear any responsibility - under any circumstances - towards any party as a result of any decision or action taken or that will be taken by that party based on the content of this report. The NCA asserts that it is not completely or partially responsible for any direct or indirect prejudice that may occur.

About the NCA

The National Cybersecurity Authority (NCA) was established in 2017. The NCA is the government entity in charge of cybersecurity in Saudi Arabia and it serves as the national authority on all related affairs. It has both regulatory and operational functions related to cybersecurity and works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities

https://nca.gov.sa/ @NCA_KSA