Bell Labs Consulting

Future of cyber defense center

White paper

Contents

Executive summary

The level of complexity and funding behind cybersecurity threats is on the rise. Cyberattacks have increased in recent years in both the public and private sectors. The annual global costs of cybercrime were $8.4 trillion USD [1] in 2022 and expected to reach $23.84 trillion USD [1] by 2027. Geopolitically, as per the World Economic Forum [2], countries are using cyberattacks for proxy conflicts to strengthen their respective spheres of influence.

With this rapid increase in cyberattacks, enterprises need to increase their investment in cyber defense strategies. Traditionally, enterprises have relied on security operations centers (SOCs) for maintaining security operations. A SOC is a physical or virtual facility where cybersecurity experts work together to continuously monitor and investigate security events in real time. Their primary objective is to prevent, detect and respond to cyber threats by employing a combination of advanced technologies, streamlined processes and human expertise.

Cyber defense centers (CDCs) are a natural progression from traditional SOCs. A CDC is an entity responsible for continuously preparing, planning, monitoring and building a defense system against potential threat actors. A simpler definition is provided by FIRST (Forum of Incident Response and Security Teams): a CDC combines a SOC with a CERT (computer incident response team)/CSIRT (computer security incident response team) and strategy [3]. The ITU-T recommendation X.1060 defines a CDC as an entity that implements security policies (i.e., CDC services), which consist of security activities that are performed by teams responsible for security. CDC services may specify security functions as capabilities of a system to perform security-related processing [4].

A CDC also takes a proactive approach to hunt threats and uses artificial intelligence and machine learning (AI/ML) models, including advanced automation capabilities, to manage its cyber security posture. CDCs should also include activities such as proactive monitoring of networks for signs of intrusion or attack, responding to security incidents, providing security assurance by conducting vulnerability assessments and penetration testing, implementing security controls, and enforcing security policies across the enterprise.

CDCs will become a necessity for any modern organization with digital operations. Government agencies, large-scale industries and service providers will need to develop and maintain CDCs. In contrast, small and medium enterprises (SMEs) will tend to rely on a hybrid model that combines in-house experts with outsourced expert services or security as a service.

Introduction

The frequency of cyberattacks continues to grow. Along with phishing, ransomware, malware, man-in-the-middle, and DDoS (distributed denial of service), which are still all-too common, there are new kinds of cyberattacks related to AI/ML, cloud, blockchain, robotic process automation, IoT, edge computing, augmented reality and virtual reality, telecom 5G and 6G networks, and quantum technology.

In this report, we examine CDCs that prioritize proactive strategies and implement cyber defense policies across organizations, supplementing conventional reactive methods based on incident response. Further, we will discuss various aspects of building CDCs, including resource and organizational models, technology requirements, and success criteria. To start, we will look at industry trends and market insights in cyber defense.

Industry trends

By 2025, collective human data will be 175 zettabytes (175x1021) [5]. Some of the key industry trends are listed below:

1. The Verizon 2022 Data Breach Investigations Report [6] found that ransomware breaches increased by 13% in 2021. In 82% of data breaches there was human involvement, primarily due to stolen credentials, phishing, misuse, or simple human error.
2. The Nokia Threat Intelligence Report 2023 [7] highlights that 60% of attacks in telecom mobile networks are linked to Internet of Things (IoT) bots scanning for vulnerable hosts to expand their botnets for use in distributed denial-of-service (DDoS) attacks. It found that communications service providers (CSPs) are struggling to keep up with the latest threats. More than 30% of CSP respondents to the Nokia/GlobalData survey said they had experienced eight or more breaches in the last 12 months.
3. According to the IBM/Ponemon Institute report [8], the average total cost of data breaches in 2022 was USD 4.35 million, and the average duration for security teams to identify and contain a data breach is 277 days (about 9 months).
4. According to the World Economic Forum's Global Cyber Security Outlook 2022 report [9], 87% of executives are planning to improve cyber resilience at their organization by strengthening resilience policies, processes, and standards for engaging and managing third parties. This report also highlights that 84% of respondents' organizations consider cyber resilience their business priority, with support and direction from leadership.
5. Fortune Business Insights [10] expects the global cyber security market to grow from USD 155.83 billion in 2022 to USD 376.32 billion by 2029, a CAGR (compound annual growth rate) of 13.4%.

What is a CDC?

Cyber defense centers (CDCs) are evolving as successors to security operations centers (SOCs) and will continue to evolve further. A CDC protects an organization's information systems, networks and data from cyberattacks and other security threats. A traditional SOC does not manage strategy, policies or procedures, and it suffers from design, communication, and collaboration challenges between different organizational units, which adversaries can take advantage of. A CDC attempts to resolve these challenges by treating strategy management as an integral function.

CDCs consist of individual teams such as strategy management, engineering and automation, threat hunting, forensic investigation, security competence development with traditional security operations, security assurance, and incident/emergency response.

The CDC strategy management team focuses on risk management, policy management, security architecture, quality control and security assurance as part of strategy management. The CDC engineering and automation team focuses on security architecture design, implementation of security controls, security automation, and tool selection and development.

The CDC threat hunting team focuses on sensing, detecting, orienting and engaging adversaries to assure mission success and outmaneuver them. A major focus on intelligence and reconnaissance techniques used by adversaries is also necessary for this transition from security to defense methodologies. CDCs address challenges faced by traditional SOCs, like context-based threat detection, loss of human productivity due to manual investigation, and too many false positives and alert systems due to a lack of analytics and automation.

CDC competence management must ensure that the organization and interested parties (employees, contractors and suppliers) understand organizational procedures and best practices for maintaining the security of sensitive information and system. The CDC regularly communicates with all interested parties about recent security updates that will affect the organization's security posture.

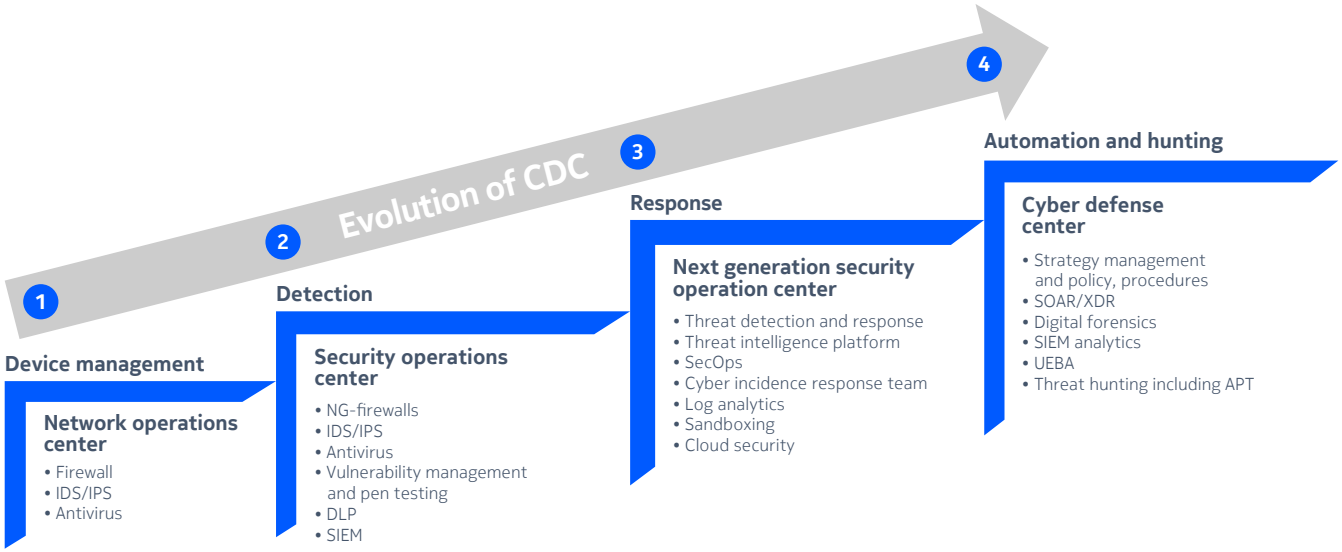
The CDC forensic investigation team collects forensic evidence for deep analysis. The security assurance team focuses on the continuous evaluation of security posture using processes such as vulnerability management and penetration testing. An incident or emergency response team is responsible for the management of security incidents and emergencies.

The CDC must regularly monitor and enforce critical organizational processes related to the organization's business. It must regularly monitor and enforce the following processes:

- Users' access management
- Information sharing, access and processing
- Incident response plan, metrics and procedures
- Risk assessment and treatment plan
- Security assurance processes such as vulnerability management and penetration testing
- Security operations tools such as security incident and event management (SIEM), firewalls, IPS/IDS, information security systems, and processes
- The compliance management process related to regulations and industry standards.

A modern CDC must effectively utilize AI/ML capabilities to hunt for vulnerabilities in the overall information security program. In addition, a CDC uses well-established security controls such as physical, management and technical controls and regularly monitors their effectiveness. A modern CDC must be able to predict human behavior, account for AI system bias, and protect infrastructure and information systems. The modern CDC must have a SOAR (security orchestration and automated response) system that can take the right actions based on preconfigured incident response playbooks. Figure 1 depicts a journey from a traditional security operation center to a CDC.

Figure 1. The evolution of a CDC



How to build a CDC

The right CDC design is key to the success of a CDC program. One must ensure several principles while designing a CDC.

Identify customer and business objectives

A CDC's charter must identify stakeholders, customers and business reasons for building the CDC. Stakeholder examples are enterprise risk management and departments such as legal, human resources, finance, audit, engineering and the business operations team. The organization must write its mission statement following its objective and strategy. The mission statement should have a written scope of the CDC and the roles and responsibilities of CDC resources.

The CDC must design its framework to satisfy its customers' needs after identifying the potential customer. Organizations must assess their security posture and analyze potential threats and vulnerabilities that could harm them, and the organization must document the results of this assessment. This initial assessment will function as a baseline for the CDC program's design.

Scope of the CDC

The CDC must document the systems and networks that will be in scope. The CDC scope documentation helps the CDC organization with its tasks and objectives.

The CDC scope document must define the following:

- The budget secured for the CDC program
- A defined schedule and timelines for execution of the CDC organization
- Physical locations containing the elements in scope
- Identified endpoints, servers, devices and applications
- The technologies and tools included and excluded in the scope
- The number of resources, efforts considered per resource, and roles and responsibilities performed by each resource — a must for framing service level agreements and upfront budget calculations
- The regulations and standards governing the CDC organization, which enterprises can use to define their policies, procedures, guidelines, and organization for overall security posture — some notable industry standards and best practices are NIST Cyber Security Framework [11], ISO/IEC 27035, the Center for Internet Security (CIS) Controls, and SANS Critical Security Controls (CSC).

Define processes and procedures

The CDC must maintain defined processes and procedures for responding to, reporting and documenting security incidents. These processes and procedures must be adapted to meet the needs of the organization. Key CDC processes are risk management, asset management, incident management, secure configuration management, vulnerability management, cryptography management, identity and access management, and advanced threat hunting management.

Organizational models

The right organizational model and structure are key to having a successful security program. Bell Labs Consulting has defined three approaches to organizational structure for the CDC organization.

De-centralized CDC

Organizations with a legacy structure may adopt this model due to existing segregation of IT and OT domains in their organizational structure. OT (operational technology) is primarily a business domain that provides services related to business operations. The IT (information technology) domain primarily provides corporate internal IT services and infrastructure. In this model, the IT and OT domains each have their own CDC.

Centralized CDC

In this model, the CDC organization is under the leadership of one leader, irrespective of the mode of business. The new organization prefers a centralized CDC organizational model due to the lack of a legacy structure.

Federated CDC

A large-scale organization with distributed infrastructure across different geographical regions would prefer this model where each region has its own small CDC unit. This CDC has at least two entities: the central control CDC and the regional control CDC. In practice, there will be multiple regional CDCs that perform region-specific local tasks related to monitoring and local incident handling. The central CDC deals with global high-priority events, analyzing incident and behavior patterns, researching cyber security issues, and performing threat intelligence and forensic analysis. This model can be adopted along with centralized IT/OT CDC or a decentralized model.

Resourcing models

Our research has identified at least three organizational types based on the resourcing model:

1. In-house CDC

An in-house CDC is a fully self-managed CDC model where organizations own and manage their infrastructure, tools, processes and resources. In this model, the headcount of the CDC is the internal headcount of the organization, and the organization also manages the competence of its resources. Large organizations with a higher budget and infrastructure with adequate security may adopt this model.

2. Outsourced CDC

In this model, organizations outsource their CDC to a managed security service provider organization. The organization does vendor management and governance of service providers and is reliant on their services. Organizations with less expertise in the security domain are adopting this model. It is also possible to outsource CDC services as a cloud-based service with predefined SLAs, monitoring and analytics services.

3. Hybrid CDC

This model does not follow any strict principle of insourcing and outsourcing resources, infrastructure and tooling, and its implementation may vary based on organization-specific requirements. Typically, organizations keep governance and strategy management of the overall CDC within their walls and may keep Level 3 experts with niche skills for threat hunting and advanced analytics, but outsource monitoring and incident response to a service provider. Organizations can build a two-level structure where they leverage service provider tools and capabilities for threat hunting, incident response and advanced analytics while also leveraging in-house security experts to supervise and ensure the right level of execution.

Typical resource sizing

CDCs must have enough resources to detect potential risks. The size of the team depends on a variety of factors, such as the size and complexity of the company's network and infrastructure, the types of security threats it faces, and the resources available for the team.

Our research indicates that SOC staff are highly occupied with handling operational issues, leaving no time for researching new cyber risks. A modernized approach would be to have a mix of automation tools such as SIEM, XDR, and SOAR with strong analytics capabilities using AI and ML, along with a fair distribution of human cyber defense experts. A cyber defense organization must implement security principles such as separation of duties and rotation of duties during the formation of the CDC. An organization may not necessarily need to hire security resources for its CDC; it may opt for a "CDC as a service" model from an expert service organization. Each organization has different security requirements based on their industry type, regulations, risk profile and business objectives. One model may not fit all. An organization must choose and map the right model based on an investigation of its business objectives and strategy.

In general, the size of the security operations team should be sufficient to effectively monitor and protect the company's systems and data against potential security threats. The following factors impact the resource requirements of a CDC:

- Complexity and volume of the threats faced by an organization
- Company size, type, complexity and industry sector
- Complexity and number of security tools
- Sensitivity, criticality and number of assets
- Specific security and regulatory compliance requirements (e.g., PCI-DSS, HIPAA).

Having the right resources also depends on the organization's maturity across different security dimensions. Bell Labs Consulting has created a sizing model that considers quantitative and qualitative aspects of an organization. Quantitative factors consider the size of the network, while qualitative factors consider the organization's security maturity, including security tools, processes and automation.

Quantitative factors

- The number of devices, servers, applications in scope
- The number of users (employees for an enterprise and IT)
- A count of subscribers
- EPS (events per second) and data volume based on the number of devices and device types.

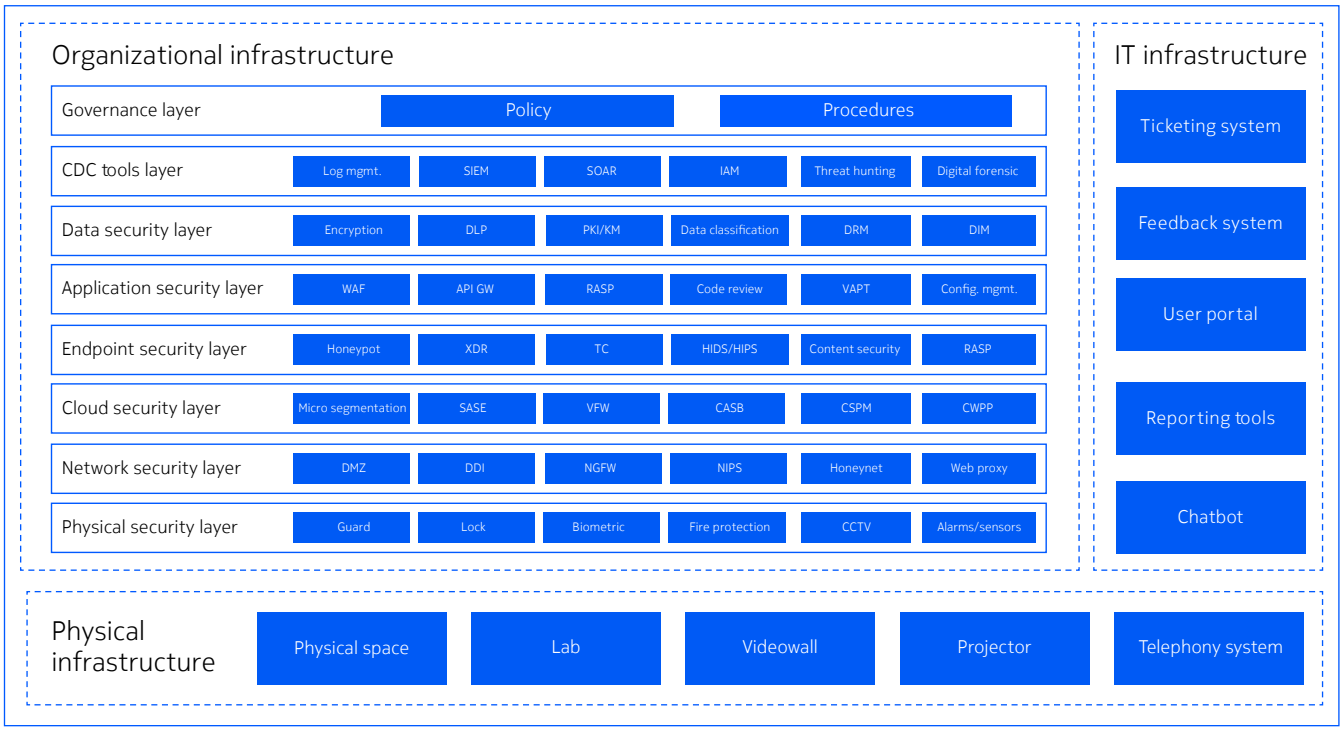
Qualitative factors

- The existence of a SIEM system and its automation maturity within the organization
- The existence of a SOAR and its automation maturity within the organization
- Threat hunting capabilities and maturity level within the organization
- The organization's digital forensic capabilities
- Overall security maturity level and security posture of the organization.

Typical CDC technology and tooling

A typical CDC organization has three major components: organizational infrastructure, physical infrastructure and supporting IT infrastructure. The following figure depicts different components of the CDC infrastructure.

Figure 2. CDC Infrastructure



A modern CDC utilizes technology efficiently. Here are a few examples of some critical tools:

- Firewalls
- Network intrusion prevention system or network intrusion detection systems
- Host intrusion prevention system or host intrusion detection system
- Security incident and event management (SIEM)
- Threat intelligence and hunting tools
- Security analytics
- Forensic analysis
- Security orchestration, automation and response (SOAR)
- Public key infrastructure (PKI) and key management system
- Vulnerability scanning tools
- Endpoint security tools such as extended detection and response (XDR), managed detection and response (MDR), and endpoint detection and response (EDR)
- Identity and access management system
- Network access control (NAC)
- Data loss prevention (DLP)
- Reporting tools
- Anti-DDoS
- Configuration audit system.

Role of automation and analytics in a CDC

Automation and analytics play a vital role in a CDC. Here are some of the significant benefits that automation can provide to security:

- Automate routine, repetitive tasks, which allows security professionals to focus on more complex, high value tasks
- Improve the accuracy of security processes by reducing the risk of human error
- Enhance visibility into environments by enabling them to identify potential security issues more quickly and effectively
- Improve cyber resilience to security threats by automating backup and recovery processes, as well as enabling rapid incident response
- Enables security teams to scale their operations more effectively, allowing them to keep pace with the increasing volume and complexity of security threats.

SOAR is a platform that enables organizations to automate and orchestrate their security operations. It can help security teams streamline their workflows and respond to security incidents more quickly and effectively.

SOAR provides a contextual view of security posture across the infrastructure and delivers reporting capabilities and real-time monitoring. These enable security operation teams to be more effective and keep track of the dynamic digitalized environment. Here are some of the key roles that SOAR plays in security automation:

- Ability to interact (collect/trigger) with multiple, vendor-independent technologies
- Ability to automate routine, tedious tasks
- Analytics and machine learning offer complex correlations and detection capabilities
- Orchestration of security tools
- Customizable dashboards guarantee an effective presentation of key information
- Integration with threat intelligence feeds
- Incident response automation
- Automated workflows that allow the acceleration of the investigation and mitigation processes.

Success criteria for a CDC

It is important for the CDC program to measure the program's success using metrics. Business stakeholders or customers must be able to visualize improvements in the organization's overall cyber security posture. The CDC program must have documented and agreed-upon key metrics, as well as tools to report them.

Table 1. Example CDC metrics

S. No	Metric	Metric description
1	Mean time to detect (MTTD)	How fast an organization identifies an attack
2	Mean time to respond (MTTR)	The mean time to respond to a discovered incident
3	Mean time to contain (MTTC)	The average time taken by security teams to shut down all attack vectors across all end-points and reduce the potential for further impact
4	The actual vs. attempted incident ratio	Measures the effectiveness of the CDC and the number of attacks defended by it
5	Average time from ticket creation to ticket closure	Identifies total time spent on a ticket or ticket type
6	Total business Impact	Measures the impact on business due to un-defended security attacks
7	Number of successful hunts	Measures successful threats hunted by CDC program
8	Number of assets protected	Shows CDC coverage in volume of assets
9	False-positive rate	The percentage of alerts diagnosed as invalid threats post-triage of the incident compared to total alerts
10	Detection to decision time	Time taken for anomaly detection and processing through SIEM before it reaches an analyst or automated incident response system to determine the need for an action
11	Patch management compliance	The percentage of actual updated information system devices versus the latest agreed-upon software patching target
12	Industry peers and benchmark metrics	CDC program's performance measured against industry peers or benchmark (optional)
13	The phishing test success scope	Measures employee's awareness of social engineering attacks

Conclusion

In conclusion, a CDC is an emerging requirement for critical businesses and industries as it focuses on proactive cyber defense against adversaries. A dedicated unit and a robust defense strategy are more important than ever due to the increasing frequency and complexity of cyberattacks. A CDC plays a significant role in shielding an organization's information assets and data from increasing cyber threats. To detect, prevent and respond to cyber threats, a CDC typically employs a range of technologies and tools, including firewalls, intrusion detection systems, SOAR, SIEM, XDR, forensic analysis tools, advanced analytics, and threat intelligence.

Enterprises must continuously enhance and review their security posture against new threats, enhance automation, and strengthen the proactive side of security. Bell Labs Consulting envisions growing demand for CDCs over traditional SOCs due to increased security risks. Enterprises will adapt their existing reactive SOC to a modern proactive CDC with strategy management, enhanced automation, analytics, threat intelligence, and automated response methodologies.

Enterprises will also require a strong culture of cybersecurity awareness and training for employees, partners and suppliers to ensure that all interested parties are well informed of the risks and can help play their role in maintaining a secure environment. Overall, a CDC is a crucial component of any enterprise's cybersecurity strategy, and enterprises will increase their attention and investment to safeguard against adversaries.

Abbreviations

AI	Artificial intelligence
CAGR	Compound annual growth rate
CDC	Cyber defense centers
CERT	Computer incident report team
CIS	Center for internet security
CSC	Critical security controls
CSF	Cybersecurity framework
CSIRT	Computer security incident response team
CSP	Communications service provider
DDOS	Distributed denial of service
DLP	Data loss prevention
EDR	Endpoint detection and response
FIRST	The Forum of Incident Response and Security Teams
HIPAA	Health Insurance Portability and Accountability Act of 1996
IEC	International Electrotechnical Commission
IoT	Internet of things
IPS/IDS	Intrusion protection and detection systems
IT	Information technology
ISO	International Standards Organization (NGO)
MDR	Managed detection and response
ML	Machine learning
MTTC	Mean time to contain
MTTD	Mean time to detect
MTTR	Mean time to respond
NAC	Network access control
NIST	National Institute of Standards and Technology (US)
OT	Operational technology
PKI	Public key infrastructure
PCI-DSS	Payment Card Industry Data Security Standard
SIEM	Security incident and event management
SME	Small to medium enterprise
SANS	SysAdmin, Audit, Network, and Security Institute
SOAR	Security orchestration and automated response
SOC	Security operations centers
XDR	Extended detection and response

References

1. Petrosyan, A., “Annual cost of cybercrime worldwide 2017-2028,” Statista Technology Market Insights, Sep 2023. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
2. World Economic Forum, “These will be the main cybersecurity trends in 2020,” Jan 2020. https://www.weforum.org/agenda/2020/01/these-will-be-the-main-cybersecurity-trends-in-2020/
3. Koichiro, K., “SOC, CSIRT and then ‘Cyber Defense Center’, Africa First CERT and FIRST Regional Symposium, Speaker Slides, Feb-Mar 2023. https://www.first.org/resources/papers/africa-arab-regions2023/FIRSTAA23-Speaker-Slides-Koichiro-Komiyama.pdf
4. ITU-T, “X.1060 : Framework for the creation and operation of a cyber defence centre,” Jun 2021. https://www.itu.int/rec/T-REC-X.1060-202106-I
5. Kerner, S. M., “34 cybersecurity statistics to lose sleep over in 2023,” TechTarget, WhatIs.com? Jan 2023. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020
6. Verizon, “2023 Data Breach Investigations Report,” online. https://www.verizon.com/business/resources/reports/dbir/
7. Nokia, “Threat Intelligence Report,” 2023. https://pf.content.nokia.com/t007z0-trust-cybersecurity/report-nokia-threat-intelligence-report-2023?lb-mode=overlay&_ga=2.241118531.1762459471.1686805789-1341264514.1639661699&&lb-width=100&lb-height=100
8. IBM, “Cost of a Data Breach Report 2023,” online. https://www.ibm.com/reports/data-breach
9. WEF and Accenture, “Global Cybersecurity Outlook 2022,”Jan 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
10. Fortune Business Insights, “Cyber Security Market Size, Share & COVID-19 Impact Analysis by Security Type, By Enterprise Size, By Industry, and Region Forecast, 2023-2030,” Report ID: FBI101165, Apr 2023. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165#summary
11. U.S. General Services Administration, “Cybersecurity Framework: Supporting your agency’s CSF,” NIST Cybersecurity Framework, viewed online Nov 2023. https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/cybersecurity-framework#:~:text=The%20National%20Institute%20of%20Standards,Protect

Acknowledgements

Thank you to Mr. Alan McBride and Mr. Sampath Rangarajan from Nokia Bell labs Consulting and Mr. Ben Aveling and Mr. Kuldeep Bahadur from Nokia Cloud and Network Services group for kindly reviewing the document and providing their valuable feedback, which greatly improved the manuscript. I would also like to thank my manager, Mr. Furquan Ansari, for providing the opportunity and guidance to work on this topic.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID213646 (November)