Deep Science Publishing, 2026
https://doi.org/10.70593/978-93-7185-896-0_7

Chapter 7: Security, Resilience, and Incident Response Strategies

7.1. Introduction

Although preventive security controls (e.g., malware protection, firewalls, strong authentication) attempt to ensure confidentiality, integrity, and availability of information systems, no system can be fully secured. Data breaches, denial of service, and malware infections will continue to occur. The expectation is not that organizations will be ever free from security incidents, but that they will be sufficiently resilient to withstand them without suffering unacceptable damage. Striking the correct balance between security and resilience is essential. Resilience by itself, however, is insufficient. Organizations, in particular, must also be able to detect incidents accurately and quickly so that timely and effective remedial actions can be taken. An effective incident response capability complements resilient systems by enabling organizations to recover quickly and reduce the damaging impact of security breaches.

An incident is an occurrence that is not part of the standard operation of an information system and that causes, or may cause, an interruption to the system's operation, or a violation of the system's security policy; for example, unauthorized access (and, hence, a violation of confidentiality or integrity), a denial of service, or a web site being defaced. The unauthorized use of the Internet and Wi-Fi by outsiders is normally considered unacceptable system use, but is not viewed as an incident.

7.1.1. Recovery Time Objectives and Recovery Point Objectives

Clear definitions of Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are needed to establish an incident response strategy. People sometimes confuse these concepts or think they can have different values for different systems and applications. An organization must determine the RTO and RPO for every deployed system and application, then classify them in terms of the overall organizational objectives based on those values.

RTO measures the amount of downtime that a business can tolerate. For instance, an organization with an RTO of ten hours can tolerate an outage of that duration. RPO measures the amount of data loss the business can tolerate, typically expressed in terms of hours; an organization with an RPO of two hours tolerates losing two hours of data. If a system or application has a very small RTO and RPO, such as five to ten minutes, then either redundancy or always-on capability is required when one system goes down, another system takes its place without any noticeable downtime. The more critical a system is for supporting a business process, the smaller its RTO and RPO must be. During a major incident response and recovery effort, the RTO and RPO values must be updated based on the temporary state of the systems and applications that the organization is bringing back online.

7.1.2. Chaos Engineering and Resilience Testing

Chaos engineering is the practice of deliberately introducing faults into a controlled production environment to test service resilience. Like penetration testing, chaos engineering tests real-world ability to withstand attacks. Resilience testing seeks deeper insights by exposing components at local and global levels while increasing the number and severity of introduced faults. For high-test service components, the scale of fault introduction exceeds the baseline for chaos engineering, effectively stressing the surrounding environment. The use of simulated faults particularly malleably extending, for example, the impact of a service component failure, load imbalance, or network partition allows resilience testing to probe the entire service ecosystem.

Although chaos and resilience testing deliver business benefits by minimizing incident costs, they can also incur direct and indirect losses through test failures. Direct losses include often-unique substitute costs, additional IT load during testing, and reduced recovery-speed advantages from successful testing. Indirect losses including customer attrition, reputation harm, and penetrating attacks must be clearly understood and minimized. Similarly, optimizing normal operations reduces redundancy costs with incident-risk implications. Designing services for true end-to-end resilience, rather than just for individual service-component resilience with additional padding between components, also requires compromise. Such testing may demonstrate that service operations testing points are better left untested than tested, with self-inflicted incidents causing greater operational consultancy harm than potential external attacks.

7.2. Foundations of Security and Resilience

Cybersecurity threats can incapacitate an organization or result in significant, sometimes catastrophic, damages. Although it is impossible to predict and prevent every possible

incident, with a proper understanding of the threat landscape and a suitable mix of security controls, one can minimize the likelihood and severity of incidents that will adversely affect the organization. Security planning is only one part of a broader strategy that prepares the organization to cope with the adverse effects of severe cybersecurity incidents. Regardless of how strong preventive controls are, organizations must expect that serious security incidents will occur. The strength of the organization depends on its degree of resilience: the faster and more completely a system can recover from an incident, the stronger its resilience.

Resilience refers to the systems and capabilities that allow an organization to prepare for, respond to, and recover from severe incidents. Major components of resilience include detecting and monitoring events, planning for response and recovery, analyzing incidents and potential problems, performing rigorous testing of system resilience, building redundancy into systems and procedures, and improving security and resilience continuously from hardening systems, documentation, and security posture. Resilience includes the business continuity capabilities described in the BS25999 standard series, and it encompasses the user-centered principles of resilience authoring and publishing, archiving and preserving, and reducing the cost of failure described in the Digital Preservation Coalition's Technical Watch Report No. 9.

Fig 7.1: Foundations of security and resilience

7.2.1. Core Concepts of Cybersecurity

Various schools of thought have developed cyber concepts over the years, but commonalities between them help form a solid foundation. The concepts act as a

strategic compass to orient cyber efforts toward the overall mission of governments, companies, institutions, and peoples. When developing a concept governing a security activity regarded as inherently classified, it is useful to recall the adage that “no plan survives contact with the enemy.” Such observations highlight the importance of regular reassessment to identify outdated elements that could lead to complacent thinking. All organizations operating in a cyber space also referenced as “the fifth domain” need to analyze and provide resources to achieve:

1. Security: The objectives of information assurance ensuring that information and services are available data confidentiality and integrity are achieved. A combination of open and closed systems has the potential of achieving these individual and collective objectives.

2. Resilience: The organization’s cyber systems can absorb all attacks, including those that cause considerable pain before the service can be restored. Acceptance of a high-profile attack and extended outage should not lead to organizational panic. Resilience requires management of children’s expectation of the cybersecurity posture.

3. Privacy: Fundamental democratic freedoms are upheld. Security versus privacy debates should be avoided, and a posture for the cyber domain should be considered promotion instead of suppression of operations.

7.2.2. Definitions of Resilience in Information Systems

Finding a universally accepted definition of resilience is complicated; Zadeh, for example, holds that "the difficulty arises because the term appears to mean different things to different people." In the context of information systems, "system resilience is also inconsistent and evolutionary in nature," growing into a discipline with its associated terminology and concern resilience. Ouyang proposes that the field of resilience moves from being "a systematic concept applied to individual components and subprocesses" to one that emphasizes the system of systems perspective of resilience. Klein proposes associating political imperatives with resilience and highlights architecture that accommodates multiple and divergent mission requirements. Rinaldi follows an implicit systems-of-systems approach, although he outlines critical infrastructure resilience.

Woods considers resilience as an emergent property of the system of systems that encompass national security and emergency response and includes no definitions. But others are less ambiguous: resilience is the property of a dynamic system that enables it to withstand adverse conditions by avoiding and/or rapidly recovering from system failures. For Saleh, resilience integrates vulnerability, recovery time, and risk "the ability

of a system to prepare, respond, and recover from an external disturbance that changes its behavior by avoiding catastrophic failure circuits."

7.3. Threat Landscape and Risk Assessment

An organization faces numerous external and internal threats. A taxonomy of threats helps identify these threats and the attack vectors that can be exploited. Risk assessment is a process involving the identification of threats, their probability, and the potential impact. Two commonly used methodologies for risk assessment are the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach and the National Institute of Standards and Technology (NIST) risk-management framework.

Information-Security Threat Taxonomy

To protect the organization's information assets, the organization needs to identify the potential threats that might exploit the vulnerabilities present in its information systems. The identification of threats should be derived from a threat taxonomy that categorizes the key information-security threats arising from the internal and external business environment. Such a taxonomy organizes threats into various types and subtypes so that the threats affecting a specific area of operation are identified and considered in a structured manner. Threats can be divided into six major types:

1. Natural hazards such as earthquakes, floods, landslides, and so on.

2. Intruders who might access the information system physically or electronically to cause disruption, corruption, and modification of data and other resources.

3. Network-based attacks that exploit system/network/broadcasting procedures and protocols.

4. Application and system-software-related programming vulnerabilities that are susceptible to threats.

5. Hardware-related threat categories that are credibly exposed to significant loss of data.

6. Threats arising through information theft, degradation of information quality, increased information-processing time, and so on.

7.3.1. Threat Taxonomy and Attack Vectors

Numerous taxonomies exist to classify cyber threats, none of which is definitive. A practical approach organizes cyber threats into four broad categories. Criminal Threats are normal criminal activities that no longer require physical trespassing due to physical

location and personal safety. These threats are mainstream. Cyberespionage Threats involve the act of spying, wherein one nation steals critical, valuable, and sensitive information from another over the internet. Cyberterrorism Threats change the nature of terrorism, targeting online infrastructures. Hacktivism Threats use the internet to create political unrest, unlike conventional methods of using violence and destruction.

Identifying possible attack vectors is similarly vital when planning or deploying defenses to protect systems, networks, and organizations. A modern attacker has many potential entry points: PCs, Internet of Things (IoT) devices, point of sale (PoS) systems, smartphones, and eBook readers. They may be unsuspecting users or enabled by other malicious users launching attacks through social engineering tactics. Attackers may also use wireless technologies such as Bluetooth or Wi-Fi to compromise and gain access to wireless devices. Once an attacker gains control over a vulnerable system, getting or deploying malware is straightforward, as there are multiple remaining vulnerabilities. Organizations must be cognizant of these attack vectors when designing defenses.

7.3.2. Risk Assessment Methodologies

Risk is commonly defined as representing both the potential for gain and the potential for loss, which suggests that taking risks can sometimes be beneficial. Accordingly, organizations often employ risk management to identify possible risks to their operations and to employ the right types and levels of security to meet their governing risk tolerance. But without additional context, this basic premise becomes largely meaningless, as risk can be minimized almost completely, through constraining operations, while risk that is managed improperly can lead to excessive security costs or collapse of business objectives.

An exhaustive threat assessment would include the full taxonomy of threat agents available in the literature. In general threat assessment, however, the focus typically falls on the threat actors and their motivations, capabilities, and methods. Organizations typically conceptualize risk relative to specified assets or missions using one of many available methodologies (SANS, 2004; Tolk et al, 2008). A number of different risk assessment methods can be captured in a common framework consisting of three steps: (1) identifying the possible impact on the organization, (2) trying to define the likelihood that a situation will arise, and (3) establishing an organization's attitude toward the risk, indicating a willingness to accept, mitigate, transfer, or avoid. Risk determination is aligned with probability assessment and an event's probability units must match the level of detail being modeled.

7.4. Preventive Security Controls

Preventive controls aim to reduce the probability of disruptive events or security incidents and, therefore, the implementation of such controls has an inherently prevention focus. Depending on the existence of a prevention focus, preventive security controls are divided into two categories: technical controls and administrative as well as policy controls. The former are technologies or systems that are aimed explicitly at reducing the risk of certain threats actually being able to compromise the information system. The latter represent a wide array of policies that govern the development and operation of the information system.

Technical controls (prevention focused) are security-relevant components that have been implemented specifically to defend against known vulnerabilities within the system or to protect against a defined set of threats. Firewalls are a fundamental security control that prevent unauthorized access by closing known attack vectors. Many other device controls have very similar objectives. Antivirus solutions are designed to protect against the presence of known malware by looking for and removing known patterns of malicious code. In similar fashion, Intrusion Prevention Systems are also designed to operate proactively by blocking attacks, by closing or filtering off points of entry identified as likely attack paths.

7.4.1. Technical Controls (Prevention Focused)

Preventive security architectural measures and functionality should be implemented as layers of protection and fall into four major categories: technical controls, administrative controls, access protection, and use and support protection.

Technical preventive controls operate at the technology layer and ensure that security functions execute to create a protected and monitored platform. Their effectiveness requires proper usage at all other interaction layers. Technical preventive controls include but are not limited to the following: data integrity, logging and monitoring, auditing, access control, directory services management, intrusion preventive technology, e-mail security filtering (SPF, DKIM, DMARC), source address spoof detection, account management, change detection, and vulnerability identification. These controls should in principle be deployed at all critical components including servers, communication devices, and end-user workstations.

Control surrounding configuration management has long been recognized as a crucial component of network and security architectures but is often insufficiently segregated from normal operational activities. Configuration management scanning tools exist, as do change management input and output verification processes. Ensuring the implementation of appropriate separation of duties and delegated responsibility between

users, managers, and auditors will enhance the reliability of these technical controls. A lack of coherent control will invariably weaken the configuration integrity management process and increase risk exposure now and in the future.

7.4.2. Administrative and Policy Controls

Administrative and policy controls complement technical control elements. Technical controls primarily focus on reducing the likelihood of information security incidents through prevention. However, technical controls cannot provide complete mitigation for all risks. They also require appropriate policies and administrative controls, for example:

- Policies and procedures that require users to use antivirus software, explicitly deny the use of personal thumb drives, and enforce secure configurations on all servers.
- Policies and procedures requiring staff background checks prior to hiring and security awareness training for all employees.
- Management oversight of systems with highly sensitive or personal data by review of access logs.
- The most common types of administrative controls include the following:
- Procedures: Detailed descriptions of the steps that personnel follow to carry out a process. For example, the procedure for user account creation for a cloud application specifies the steps an authorized member of the cloud service administration team must perform to create a user account.

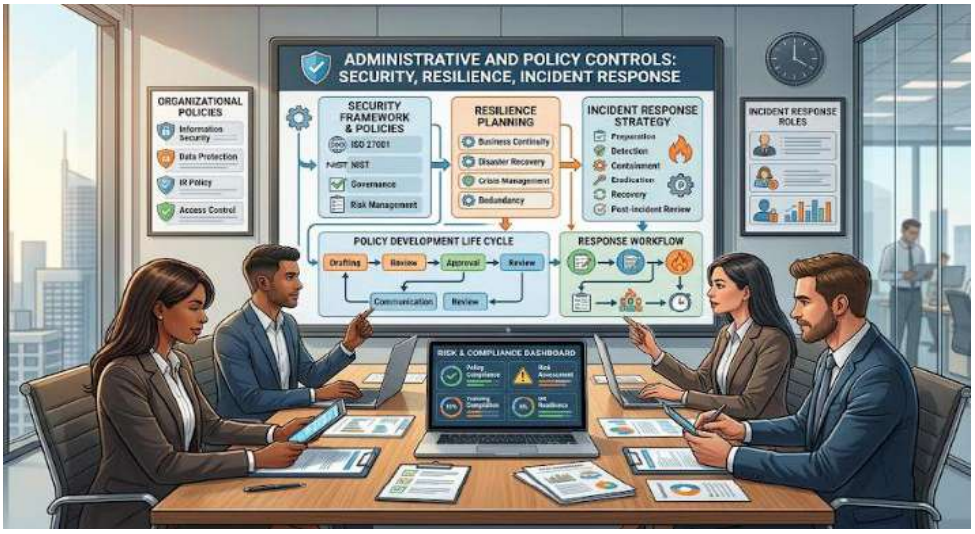

Fig 7.2: Security governance and resilience strategies

- Guidelines: General recommended actions or behaviors, but it is not mandatory to perform them. For example, clearing the cache at the end of every browser session is a guideline of a web application security policy, and it helps mitigate some risks by catering for users using shared workstations.
- Standards: Rules that personnel must follow. Compliance with standards can be measured.

7.5. Detection, Monitoring, and Anomaly Management

A detection and anomaly management strategy monitors IT systems for behavioral anomalies that are symptomatic of security incidents. The concept of detection is tied to identifying unusual behavior on IT systems, networks, and applications (NIST 2018). Continuous Monitoring Architectures support the Principle of Principle of Defense-in-Depth. Rather than rely on a single detection mechanism, threat detection is supported by various overlapping detection mechanisms host-based analysis, endpoint detection, intrusion detection/prevention systems, and user and entity behavioral analysis.

Continuous Detection and Monitoring Architectures use techniques such as honeypots and network simulation testing, automated penetration testing, and red teaming to identify vulnerabilities at the same rate that new vulnerabilities are discovered and publicized by hackers on forums. Honeypots are decoy assets deployed by organizations to allow monitoring of attackers' techniques when they target unprotected assets or become distracted from their attacks. They combine human hackers and scripted or automated response techniques. OpSec and external attack resurfacing are performed continuously. During OpSec, new public information about the organization and new vectors of attack are examined to monitor their success. External attack resurfacing continually detects all the organization's externally visible services and applications, whether controllable or not. They help detect "broken windows" that, if visible to wannabe hackers, could tempt an attack.

The architecture implements an integrated, multi-layered approach to manage, detect, and respond to previously unknown attacks. The layered approach detects different types of attack paths, such as web application attacks against business-critical web applications and sensitive data, and advanced persistent threats related to command/control remote access, backdoor installation, and lateral movement. Technologies used for detection include file integrity monitoring, SIEM, Security Orchestration and Automated Response, intrusion detection/prevention, argumenting honeypot, endpoint detection and response, and user and entity behavior analytics (NIST 2018; Lacey et al. 2017; Chen & Hsu 2017).

7.5.1. Continuous Monitoring Architectures

Rapid digitalization initiatives have considerably expanded the threat surface. Modern attack foes can strike all verticals, from gov-ernments to health care, finance, and energy. Conglomerates with extensive resources for preventive efforts are often viewed as more desirable targets, due to rich data sets and computing power. Cybercrime-as-a-service is emerging, with ready-made exploits for sale to script kiddies and nations daring attribution-free attacks. Even smaller enterprises today are extensively monitored by dedicated external spoofing groups, sometimes for years. Briskly executed attacks, such as exploitation of prominent selection vulnerabilities, can dent not only a victim's reputation but also customer trust. Continuous monitoring enabled by an advanced anomaly management framework is a key condition for deterioration-proof systems.

Continuous monitoring applies to operations across different lines of business. In information technology, it is a vital necessity for securing perimeters. Preventions, detection, and mitigation related to machine learning and artificial intelligence algorithms are becomingly progressively more in demand. New kinds of preventive and active malicious software are also emerging. Firstly, malware has turned into a concept rather than into a technology. New stateful technologies are constantly on offer, although new threats are still based on the same old files and exploits. New kinds of file-less malware that run only in random memory and get removed once the operating system reboots are now popping up. These file-less malware make prevention and detection harder to build for standard Windows antivirus. Typical antivirus detection rates have often dropped below 30 percent on the public Internet. Ransomware and advanced persistent threats focusing on exploiting attackers' capabilities and money are pushing organizations into data loss. Normally, within a hundred days, busy administrators discover in their information systems that data of a billion users have been sold.

7.5.2. Incident Detection Technologies

Failure to detect abnormal behaviours and incidents in a timely and efficient manner creates opportunities for attackers to compromise systems and information resources. Attacks are therefore more likely to be detected by external observers than by those responsible for protecting and monitoring the systems themselves. The threat landscape is not static. Attack vectors become more sophisticated and automated, and the number of attackers increases to include not only outsiders but also insiders. Detection must therefore be continuous, bounding the time of detection. Detection is further complicated by advance planning and a heightened level of realism of the attack.

Traditional methods are based on searching for known malware using signature-based methods. The availability of reliable signatures requires knowledge of the malware used

and sufficient information on the attack characteristics to draw additional signatures. Newer malware might use the previously mapped commands, ip address/ranges, and infected host names of major C&C infrastructures to hide their activities.

Anomaly detection is an activity that forms a major part of computer security monitoring. Schemes typically include analysis of user behaviour (one or more actions whose usage deviates from the normal usage of the user), network data flow analysis (deviation from the standard communication pattern), and kernel-level monitoring (protection against rootkits). Network behaviour analysis is particularly useful since it does not require host access. Network anomalies that can be detected include traffic flow patterns deviating from expected behaviour, unusual types of connections, unequal partner behaviour (between client/server pair), higher-than-normal volume of broadcast or multicast traffic, and excessive number of resets or ICMP messages.

7.6. Response and Recovery Planning

Preparing for incidents means identifying the most effective way to contain, eradicate, and recover from the consequences. A well-defined plan focuses on deciding who will do what and how. The importance of maintaining the integrity of forensic evidence is often neglected in response planning, even though this is essential for both operational control and legal evidence. Operators locating an event may also have to preserve evidence for legal purposes.

An organization needs to select and implement an incident response framework. Popular frameworks include the National Institute of Standards and Technology Computer Security Incident Handling Guide (NIST SP 800-61), the Open Source Security Incident Management Framework (OSSIM), the SANS Institute Incident Handling Process, and the Forum of Incident Response and Security Teams (FIRST) Incident Management Framework. These frameworks all define steps, responsibilities, and procedures for allocating resources and information across containment, eradication, and recovery. The details of each step depend on the organization and its resources and structure.

Containment, eradication, and recovery (CER) procedures ensure that steps to contain, eradicate, and recover from an incident are made when required and are effective. When an operator determines that an incident needs to be contained, staff should execute these procedures immediately. CER procedures identify containment measures appropriate for the organization and establish specific measures for the most critical incidents, with implementation responsibilities assigned. Successful containment should focus on limiting damage and preventing further incidents.

7.6.1. Incident Response Frameworks

Preparedness to respond to security incidents is essential. Incidents may result in an outage, including various mission-critical functions. During such an outage, it may not be possible to protect information from destruction, disclosure, or alteration. Incidents may also lead to violations of laws or regulations, such as criminal activity, and other forms of unacceptable behaviour, and they may require the involvement of outside authorities.

One commonly used framework for incident response is the Computer Security Incident Handling Guide. This is the second edition of the guide published by the National Institute of Standards and Technology (NIST). The guide has been prepared by the Computer Security Resource Center (CSRC), a part of NIST's Information Technology Laboratory. The guide describes the process of incident response and identifies the key issues that should be considered throughout the various phases of incident handling. It is intended to be beneficial to IT security managers, information systems security officers (ISSOs), incident handlers, and others with similar responsibilities. The guide can serve as an overview of incident handling, as a reference point for security policies, or as a source of helpful information for management decision-making. Although it does not provide a comprehensive approach to all facets of incident handling that are of interest to a particular organization, it can assist an organization in developing those aspects that its managers conclude are especially important to the organization.

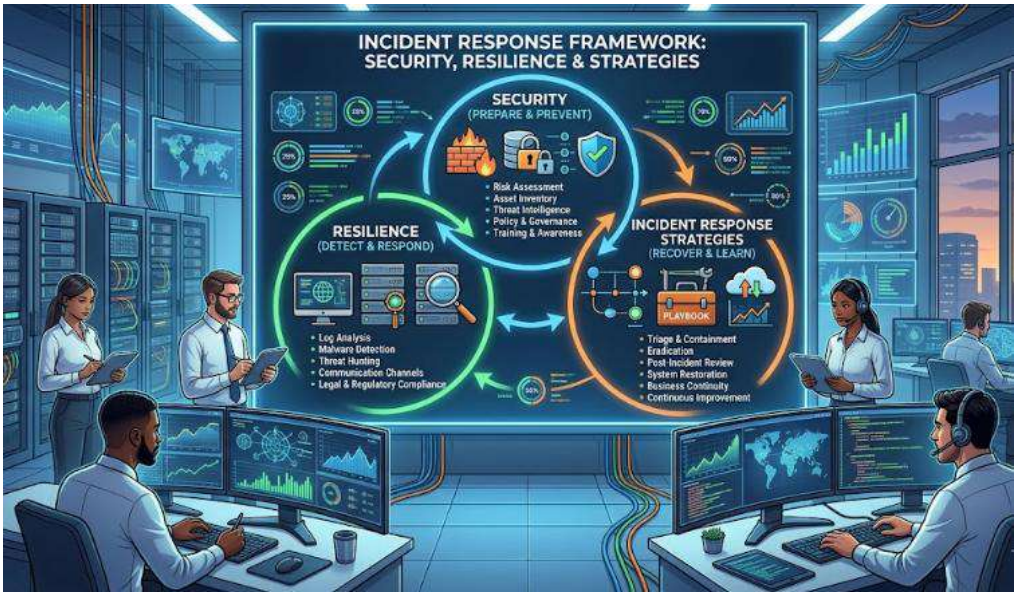

Fig 7.3: Cybersecurity incident response framework overview

7.6.2. Containment, Eradication, and Recovery Procedures

Containment, eradication, and recovery procedures describe a working layered approach that addresses both the immediate and long-term effects of a security incident. Containment actions are taken to minimize or limit damage and to allow critical business operations to continue, albeit at a degraded level. During this phase, steps may be taken to mitigate a vulnerability discovered during the incident or to shut down additional attack vectors. The eradication phase aims to remove any and all sign of the incident, including unauthorized access methods, and to correct underlying vulnerabilities. The final recovery phase addresses the need to restart operations and return systems to normal production levels.

Containment, eradication, and recovery procedures should be developed in advance of an incident and bolstered by planning with appropriate levels of data backup. External partners should also be engaged in review and testing of these procedures.

7.7. Conclusion

Fulfilling the preventive paradox requires a security strategy incorporating effective detection, response, and recovery capabilities. Incident detection is affected by network visibility, situational awareness, and the analysis of anomalies. Continuous monitoring architectures draw upon advanced technologies, including data analytics. Once an incident has been detected, it should be contained by limiting its spread. The containment, eradication, and restoration stages of the incident recovery life cycle are used to address each incident's unique characteristics, which are often informed by a broad threat taxonomy. To overcome the consequences of a data breach, cyber-resilient organisations take a risk-based approach to the defensive strategy.

The Security, Resilience, and Incident Response Strategies guide established preventive doctrines are evolving beyond their prevention-focused boundaries. The notions of cyber-resilience, resilience-testing, preparation for detection, and response planning are foundational to the strategies. These concepts inform and guide strategic investments, resources, and capabilities for the entire incident life cycle within resilient information systems one that extends beyond the internal perimeter and reduces reliance on de facto Zero Trust Security principles.

7.7.1. Future Trends

While the security field is, to a certain extent, reactive, the cyber threat landscape encourages the development of innovative solutions. These developments can take place around tools and practices or how SOC decision-makers manage, design, and leverage

these solutions. Some of the trends organizations can explore to enhance their security posture include the following.

Security in the Cloud

Cloud services also help avoid blind spots. Deploying an endpoint security service or an agent on a virtual machine in an infrastructure-as-a-service environment can be extremely difficult as the VM is decoupled from the application. Cloud-based service applications usually manage and control the hosts. These host applications generally allow security detection and monitoring services to be integrated, providing better visibility and identification for any deviant behavior occurring in the cloud environment.

Security and Operational Technology

Traditionally, security technology was completely separated from organizations' operational technology (OT). This part of the enterprise was usually separated from IT, and access was restricted. The communication technologies within OT usually provided limited detection capabilities. However, a few enterprise vendors and specialized detection companies are starting to focus on deployment models that make it possible to also monitor OT safely.

Endpoint Detection and Response

Enterprise detection and response solutions (called endpoint detection and response or EDR solutions) make it possible to monitor and act on endpoints continuously. Unlike SIEMs, these solutions leverage local computational resources and collect security-relevant data from endpoints in real time. The primary advantage of EDR solutions is the collection time window. These solutions can identify anomalous behaviors across data sources with wide-ranging time series, enhancing detection capabilities. Anomalies can also be anticipated based on modeling, patterns, or statistical and machine-learning forecasting. EDR offers visibility beyond the enterprise perimeter, following roaming users throughout the globe..

References

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). NIST.

Recharla, M. (2024). Advances in Therapeutic Strategies for Alzheimer's Disease: Bridging Basic Research and Clinical Applications. American Online Journal of Science and Engineering (AOJSE)(ISSN: 3067-1140), 2(1).

National Institute of Standards and Technology. (2012). Computer security incident handling guide (SP 800-61 Rev. 2). NIST.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems. ISO.

International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience Business continuity management systems. ISO.

ENISA (European Union Agency for Cybersecurity). (2021). Cybersecurity incident response: Guidelines for national and governmental CERTs. ENISA.

Botlagunta Preethish Nandan, "Data Analytics-Driven Approaches to Yield Prediction in Semiconductor Manufacturing," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2021.91217

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (SP 800-94). NIST.

Adusupalli, B., Malempati, M., Paleti, S., Mashetty, S., & Singireddy, J. (2025). Integrated Financial Ecosystems: AI-Driven Innovations in Taxation, Insurance, Mortgage Analytics, and Community Investment Through Cloud, Big Data, and Advanced Data Engineering. Journal of Information Systems Engineering and Management, 10, 1103-1117.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). Organizational models for computer security incident response teams (CSIRTs). Carnegie Mellon University, Software Engineering Institute.

Linkov, I., & Kott, A. (Eds.). (2019). Cyber resilience of systems and networks. Springer.

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for computer security incident response teams (CSIRTs) (2nd ed.). Carnegie Mellon University.