

Cybersecurity as a Service

John Morris*

Stefan Tatschner*

Michael P. Heint

Patrizia Heint

Thomas Neue

Sven Plaga

February 22, 2024

*These authors contributed equally to this work.

Authors:

1. John Morris*; Department of Electronic and Computer Engineering, University of Limerick, Ireland; john.morris@ul.ie; ORCID: <https://orcid.org/0000-0003-2811-1055>
2. Stefan Tatschner* Fraunhofer AISEC, Department Product Protection and Industrial Security, Germany; Department of Electronic and Computer Engineering, University of Limerick, Ireland; Confirm, the SFI Centre for Smart Manufacturing, Ireland; stefan.tatschner@aisec.fraunhofer.de; ORCID: <https://orcid.org/0000-0002-2288-9010>
3. Michael P. Heint; Fraunhofer AISEC, Department Product Protection and Industrial Security, Germany; michael.heint@aisec.fraunhofer.de; ORCID: <https://orcid.org/0000-0002-1094-4828>
4. Patrizia Heint; Technische Hochschule Ingolstadt, Germany; patrizia.heint@thi.de; ORCID: <https://orcid.org/0009-0001-1594-2119>;
5. Thomas Newe; Department of Electronic and Computer Engineering, University of Limerick, Ireland; Confirm, the SFI Centre for Smart Manufacturing, Ireland; thomas.newe@ul.ie; ORCID: <https://orcid.org/0000-0002-3375-8200>
6. Sven Plaga; Center for Intelligence and Security Studies (CISS), Germany; sven.plaga@unibw.de; ORCID: <https://orcid.org/0000-0002-1658-1140>

*These authors contributed equally to this work.

With the increasing sophistication and sheer number of cyberattacks, more and more companies come to the conclusion that they have to strengthen their cybersecurity posture. At the same time, well-educated Information technology (IT) security personnel are scarce. Cybersecurity as a service (CSaaS) is one possible solution to tackle this problem by outsourcing security functions to managed security service providers (MSSP). This chapter gives an overview of common CSaaS functions and their providers. Moreover, it provides guidance especially for small- and medium-sized businesses, for asking the appropriate questions when it comes to the selection of a specific MSSP.

1 Introduction

Cybersecurity as a service (CSaaS), also sometimes referred to as Security as a Service (SE-CaaS) [1], is the outsourcing of key IT security functions to an external specialist company or third-party. The concept of CSaaS ultimately began back in 1987 with the availability of the first antivirus product called VirusScan from McAfee [2] where computer users paid to be protected from malware attacks. Roll on 30 years and as the malware has become more abundant and complex, the need for more protective services has increased in tandem. The initial uptake on this new breed of cybersecurity services with names like vulnerability assessment and Chief information security officer (CISO) as a service has been passive. One cause for this slow engagement is that many Chief executive officers (CEOs) believed investment in such services is an unnecessary expense. On the technical side, some IT Directors feel that their positions within the company structure is endangered and they are confident that they can do it better themselves, anyway. Particularly in the case where the outsourcing of key organisational security functions to outside contractors is concerned.

The recent increases in cyber-attacks of high-profile companies around the world [3] and better cybersecurity education has altered this mindset in a positive way. Additionally, it has been proven that most organisations are still reactive when it comes to cybersecurity. They still believe that a malware attack will not happen to them: so why pay for cybersecurity? It is deemed too high a price for embracing the concept of precaution. However, when such deniers are stroke by a sudden malware attack, suffering untold data losses or paying ransoms to the cybercrime-as-a-service industry, these entities suffer greatly for their negligence. That is, if they are still even in business after the attack as currently over half of all small businesses close within six months of a malware attack [4].

What is for certain though, is that the volume of malware attacks are set to increase and become more sophisticated, particularly with the advent of malware enhanced by artificial intelligence (AI) like DeepLocker [5], and few companies will have the expertise and resources to deal with this evolving cyber problem. Another point of note is that the malware attack surface is no longer confined to large networks of connected computers and servers, poorly written web interfaces, and email phishing attacks. The newer malware is targeting the entire Internet of Everything (IoE) landscape. From mobile phones to smart wearables, and resource-constrained Internet of Things (IoT) devices to cloud-based platforms. With such a large IT ecosystem to protect, it has become increasingly expensive for companies to train their IT staff to protect this attack surface or hire dedicated IT security staff. This is compounded by the fact that there is currently a worldwide shortage of IT security staff with current estimates at 3.4 million vacant positions [6].

CSaaS appears to be a step in the right direction to handling this growing threat landscape and allows companies to pick the IT security functions that they most need help with at a more affordable monthly rate. Simultaneously, not least due to the rising numbers of supply chain attacks, it is important that a provider is chosen who does not only offer an increase in security to its customers just from a technical viewpoint. To be able to protect sensitive customer data, a strong security ethos is also required on the provided services. Over the course of this chapter, a more in-depth review of the most common IT security functions being offered by CSaaS companies will be discussed. Also, a comparison of the main CSaaS companies will be conducted. Finally, a checklist will be created for companies looking to choose a CSaaS for

themselves.

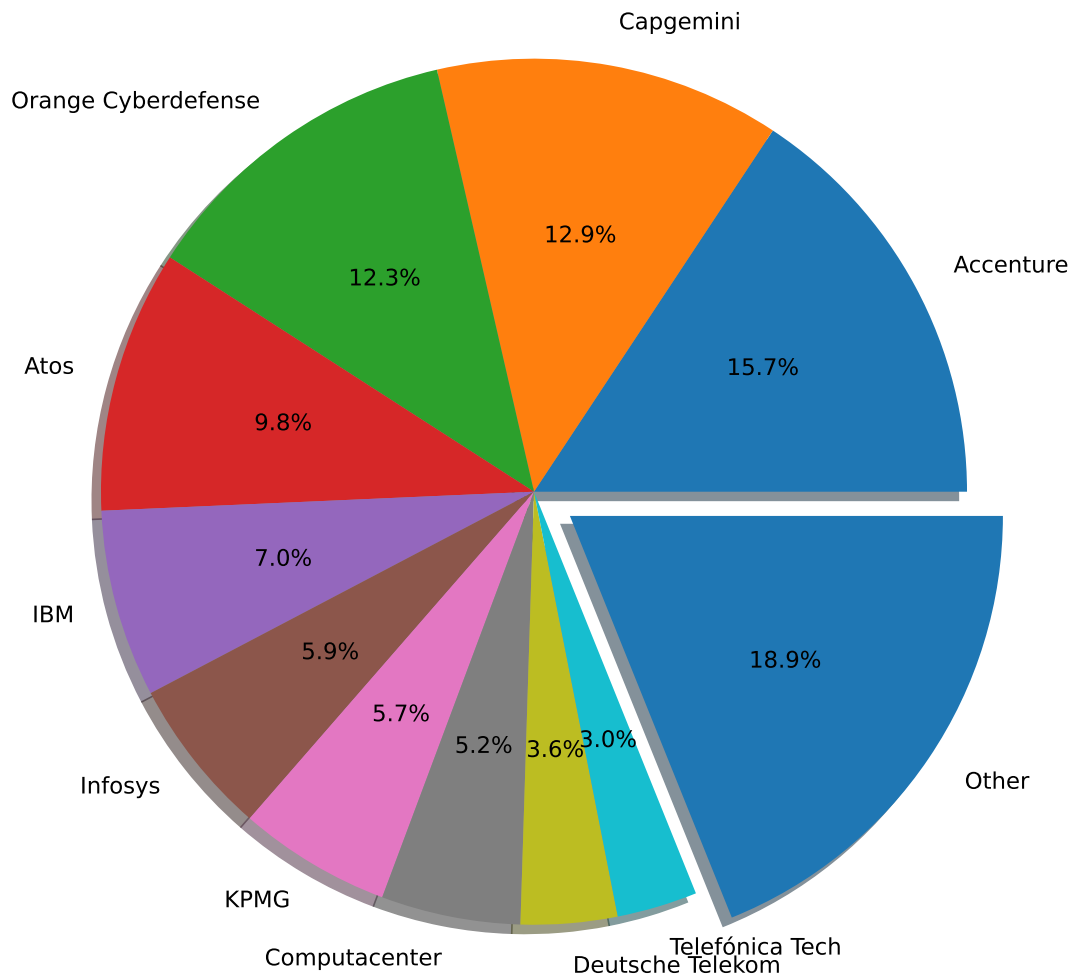


Figure 1: Managed & Professional Security Services Market: Revenue Share of Top Participants, Europe, 2022; conducted by Frost & Sullivan [7]

The cybersecurity market has developed into one of the most profitable IT markets over the last decade [8]. Consequently, a lot of new IT companies specialised in cybersecurity were only founded in recent years or where existing IT companies launched dedicated cybersecurity divisions. According to the revenue study shown in Figure 1, the top ten companies in the managed and professional security services market in Europe are:

- **Accenture** (<https://www.accenture.com>),
- **Capgemini** (<https://www.capgemini.com>),
- **Orange** (<https://orange.com>),
- **Cyberdefense** (<https://www.cyberdefensecompany.com>),

- **Atos** (<https://atos.net>),
- **IBM** (<https://www.ibm.com>),
- **Infosys** (<https://www.infosys.com>),
- **KPMG** (<https://www.kpmg.us>),
- **Computacenter** (<https://www.computacenter.com>),
- **Deutsche Telekom** (<https://www.telekom.com>), and
- **Telefónica Tech** (<https://www.telefonica.com>).

CSaaS companies typically offer services in several forms, for instance subscription or payment for utilised services. In contrast, there are also variants where basic usage is free to use, but additions (e.g., 24/7 customer support, higher rate limits, or additional premium features) are charged.

Outsourcing key IT security functions comes with benefits like cost cutting, a consistent and unified architecture, or better security expertise (by the CSaaS company). On the other hand, implementing CSaaS relies on sensible data being sent to the service provider which introduces multiple challenges requiring a well-designed architecture to avoid insecure applications. Consequently, companies offering CSaaS *must* maintain a good reputation in the marketplace and be trusted to stay relevant. The importance of a good reputation for companies offering CSaaS begs the question of decent selection. When looking to choose a CSaaS company to engage with, what are the ten most common traits to look for?

1. How long is the entity in business?

The reputation is easier to spot when the entity is in business for a long time. In this case there may be online reviews, news articles, or similar material from third parties available.

2. What companies is the entity working with already?

Collaborating with big players in the same area of work can be a hint for a good and trusted reputation. Particularly, if these are long term customers.

3. What range of services does the entity offer?

Offering few services could be a hint for a highly specialised entity offering high quality services. Are the specific services that are being sought, being offered by the entity?

4. What kind of service delivery model is employed? On-premise, remote, or both?

This trait is very specific to the relevant use case and the current security posture of the client company. On-premise means that dedicated resources and staff need to be provided, but a certain level of control is still ensured.

5. Is it a fully managed service or do internal IT resources have to be dedicated to delivering the services?

This depends on whether the client company has internal staff with the requisite skills and time to manage the security requirements of the company. Fully managed is designed for client companies with little or no internal security personnel or systems.

6. What type of pricing model is offered? Fixed monthly, annually, per employee or device?

This will depend on the type of security service being offered. Security training is typically charged by employee whereas penetration testing and cyber insurance can be charged monthly or annually.

7. What is the skillset and qualifications of the staff?

Are the staff certified or doing public speeches at conferences in their area of work? Is their training relevant and kept up to date? Where are the gaps in the security staff skills that need to be filled by an external security company?

8. Has the entity published any articles or does the entity take part in any blogs or forums in the areas of cybersecurity?

This is a big indication of a security company that is highly skilled and extremely competent. It also means that they are keeping up to date with the latest security threats and trends.

9. Does the entity provide a trial period or proof of concept?

This can be helpful in deciding if a particular security company or tools is compatible with the needs of a client company. A proof of concept can provide a try before you buy type scenario to help key decision makers in the approval process.

10. Is the entity certified?

Certifications help ensuring that at least a minimum level of security. It also gives the client company a comfort in knowing that the entity has the requisite security qualifications to complete the security services being offered.

This book chapter contributes a list of ten most common traits to look for when choosing a CSaaS company. In addition to these traits, common CSaaS functions are researched and are related with high revenue companies. Furthermore, an overview over the current market share of professional CSaaS providers with a comparison about the offered services is given.

2 CSaaS Functions

The number of different cybersecurity services offered by these companies are substantial, especially when specialised use cases are included. However, the Cloud Security Alliance has published an overview [1] where a categorisation of cybersecurity services was carried out. The provided categorisation was enhanced by additional services based on our practical knowledge and logical reasoning. The identified key services are described in the following sections.

2.1 Security Personnel as a Service

CISO as a Service or Virtual CISO is the outsourcing of the Chief Information Security Officer role within an organisation. This resource can work onsite within a particular organisation or work remotely; reporting directly to the C-Level Group which is key for decision making. They

can work independently or as the head of a security team, work for a fixed contract period or month-to-month. Their duties include:

- Full review of an organisation's security position.
- Recommend best practise hardware, software and security changes. This can also include purchases.
- Interview, vet and hire new security staff
- Train internal security team.
- Generate penetration testing report.
- File NIST 800 security reports where required.

This role is more suited to mid to large sized companies where the budget for a permanent CISO role is currently not available or as a try before you buy type scenario. A main constraint of this approach is the often steep learning curve for the contractor in terms of corporate knowledge, cultural norms and company politics. However, this last point can also be an advantage as the contract CISO is not affected by internal conflicts or job security.

Additional security roles that can be outsourced include a data protection officer, compliance and risk officer, forensic analyst, security trainer, penetration tester and security helpdesk personnel.

2.2 Cyberawareness Training

Cyberawareness or malware threat detection training involves the systematic education of company employees in how to correctly identify malware threats, since 95% [9] of current company malware breaches are caused by human error. The format of the training is usually a step-by-step guide containing videos and a series of items to identify afterwards, to reinforce the training. The training usually finishes with a quiz of all the topics discussed in the session with a completion certificate produced for a passing grade. The most popular cyberawareness training programmes concentrates on email phishing and social engineering attacks. In other words, training employees to think before clicking on that web link and entering their login credentials into a fake website like in figure 2.

The training normally lasts around 30 to 40 minutes with some like the Kevin Mitnick inspired KnowBe4 email phishing offering lasting 50 minutes. The cyberawareness training is then reinforced further with weekly mock phishing attacks being sent out to all employees. Training should be retaken by employees at least once a year to keep abreast of new types of malware attacks. The training is offered as a managed service that typically reports to the Human resources (HR) department rather than IT. The main types of cyberawareness training sessions include:

- Phishing, Smishing and vishing attacks.
- Remote work training.

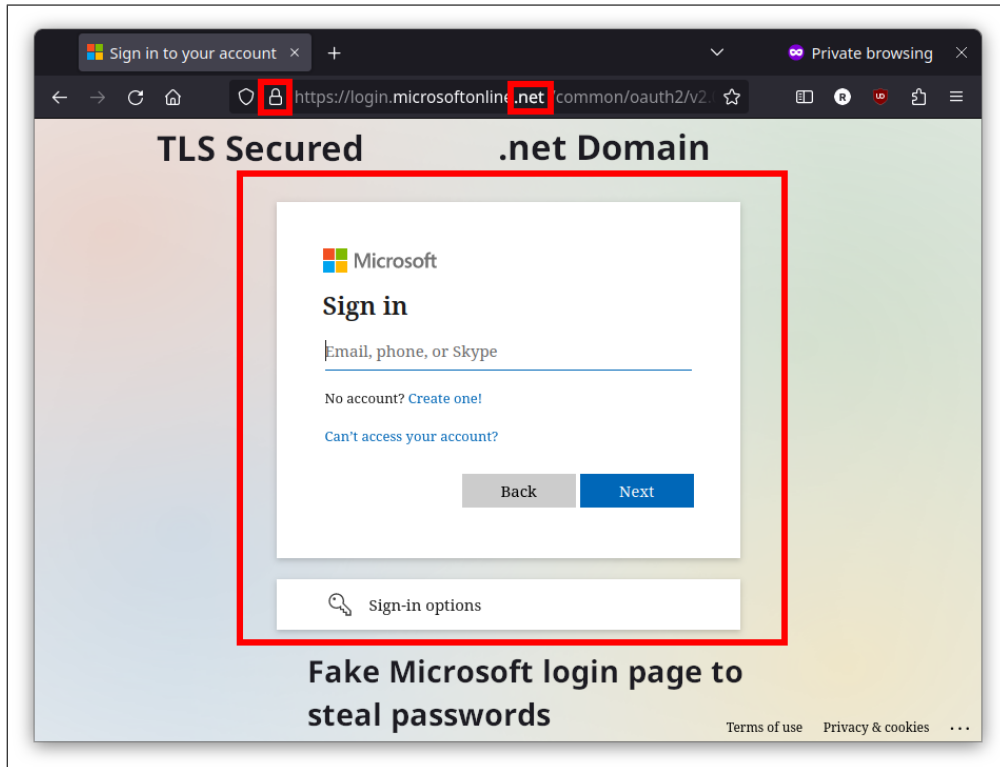


Figure 2: Screenshot of a phishing website for a Microsoft login [10].

- General Data Protection Regulation (GDPR) training.
- Foreign travel dos and don'ts.
- Intellectual or physical company property training.

The cyberawareness training can also be customised with corporate branding and content to make it more realistic to the employees (e.g., actual company emails) and assist in the process of turning them into human firewalls.

2.3 Vulnerability Assessment

A vulnerability assessment involves the systematic identification, measurement and categorisation of weaknesses within an organisation's systems. These weaknesses can take the following forms:

- Unpatched and unencrypted servers and/or computers.
- Poorly setup firewall with open rules and port access.
- Remote access vulnerabilities.

- Software and application unauthorised access.
- Lack of document lock storage cabinets or shredding facilities.
- Poor website design with limited security and/or no TLS encryption.
- Faulty door locks or doors left open
- Weak or no password policies.
- No document or data audit process.
- Weak or no Wireless Access Point security.
- Employees susceptible to social engineering attacks.

Typically, an off-the-shelf vulnerability scanner is used to identify weaknesses within an organisation. Current scanners can identify over 100K separate system vulnerabilities in as little as an hour; depending on the system size and complexity [11]. In the absence of in-house security personnel to conduct the assessment, it can be conducted using external security personnel. However, to complete the assessment properly, all systems will need to be scanned from inside the organisation as well as from the outside. Once the assessment is complete, a detailed vulnerability report is created based on the weaknesses listed above. The vulnerabilities are classified by severity and frequency. A separate executive report is normally produced for the key decision makers with less detail and more emphasis on the risks and financial impact to the organisation.

2.4 Periodic Penetration Testing

Periodic Penetration Test is an authorised simulated cyberattack on a computer system, performed on a regular basis to evaluate the security of the system. Its objective is to identify vulnerabilities that could otherwise be used by malicious actors to abuse the computer system. A Penetration Test needs to be performed by a technical domain expert who can use similar techniques as those used by attackers.

Penetration Testing is a demanding task, and the following challenges apply:

1. **Staying up to date** with the current state of the art from a technical standpoint. The IT sector is developing at a very fast pace and a penetration tester must be capable of all the current and relevant technologies when conducting an effective test.
2. **Scope:** Defining the scope of testing is a challenging task. On the one hand, a scope that is too narrow might not yield useful results. On the other hand, too broad a scope could be unfeasible from a management perspective.
3. **Realistic Attack Scenarios** are considerable for a penetration test, since a highly academic attack scenario could indeed yield results. However, these results are at risk of not being relevant for the desired use case of the product.

4. **Limited Access:** The integration of cybersecurity in the development process (i.e. security by design) is desired, since technical design decisions often have an impact on the security of a system. However, penetration testing during development can be restricted, since parts of the system might not be implemented yet.
5. **Reproducing Issues:** Reproducing findings needs the careful documentation of all involved working steps and parameters of the test environment. Monitoring every relevant parameter in a penetration test is a difficult task, since all included parameters might not be known by the penetration tester at the offset.
6. **Time Constraints:** Penetration testing is a complex task including creative components where good findings do not strongly correlate to the amount of time being spent on a test. However, budgeting in the first place can limit the effectiveness of penetration testing, since it limits the creativity of the tester.
7. **Collaboration and Integration** with the development team is required for the feedback loop to integrate any findings improving the actual product.
8. **Skills:** Finally, the skillset of the penetration tester must be accurate for the relevant architecture and used technology.

Security by Design is becoming more and more important in the design process of software products. Companies are beginning to integrate Secure Software Engineering into the relevant value chains [12]. Periodic Penetration Testing is a good option for evaluating that the designed software architecture is secure and that included security measures serve their purpose. However, in order to be effective, it requires careful planning and implementation.

2.5 Email Security

E-mail security is a critical component of an organisation's communication. Due to its legacy, e-mail suffers from many design issues related to security. For instance the *content* of an e-mail is usually only secured from the e-mail client to the e-mail server rather than being end-to-end secure. E-mail was designed at a time when the internet was mainly an academic tool and thus end-end-security was not relevant. However, the success of e-mail especially in a corporate context might be a result of this simplicity.

There are several key technologies available which are implemented by default by the common big e-mail service providers. Since e-mail does not provide any of these technologies by default, they were added on top, for example, adding metadata via e-mail headers.

1. **Encryption:** A procedure of converting plain text into a so-called cipher text, which can only be decrypted with a specific key. Encryption implements the protective goal of confidentiality both at transit and at rest. Most commonly used state of the art technologies are Secure/Multipurpose Internet Mail Extensions (SMIME) or Pretty Good Privacy (PGP).
2. **Digital Signatures:** Digital Signatures are used to verify the authenticity and integrity of messages by using special metadata which is attached to a message. In other words,

these signatures can be used to verify that the message has not been tampered with during transit and that it was sent by the claimed sender. Most commonly used state of the art technologies are Secure/Multipurpose Internet Mail Extensions (SMIME) or Pretty Good Privacy (PGP).

3. **Spam Filters:** Filters which use sophisticated techniques to block unwanted messages.
4. **Anti Malware Solutions:** Use signature-based detection, heuristics, or machine learning to identify and block messages that contain malware, such as viruses, Trojans, or spyware.
5. **Sender Policy Framework (SPF):** A protocol that allows organisations to specify which mail servers are authorised to send e-mails on their behalf.
6. **DomainKeys Identified Mail (DKIM):** A protocol that allows organisations to digitally sign e-mail messages on the server side to verify the authenticity and integrity of the message.
7. **Domain-based Message Authentication, Reporting and Conformance (DMARC)** A protocol that allows organisations to protect their domains from unauthorised use, such as phishing and e-mail spoofing. DMARC allows organisations to publish policies that specify how recipient mail servers should handle e-mails that fail SPF and DKIM authentication.
8. **Authenticated Received Chain (ARC):** A protocol that provides a chain of authentication results for an e-mail message, starting from the original sending mail server to the recipient's mail server.
9. **Transport Layer Security (TLS):** A protocol that is used to provide communications security over a computer network. Due to its current widespread use in instant messaging, file transfers and web traffic, TLS has become a basic technology for secure internet today.

The following Listing 1 shows the added header fields and the structure change of an e-mail with ARC, DMARC, DKIM, SMIME, and SPF in place. Items in **bold** face are added by these extensions.

```
From: sender_email_address
To: recipient_email_address
Subject: email_subject
MIME-Version: 1.0
ARC-Seal: arc_seal_value
ARC-Message-Signature: arc_signature_value
DKIM-Signature: dkim_signature_value
DMARC-Record: dmarc_record_value
Received-SPF: pass (sender_ip_addr: domain_of_sender designated_server_ip_addr permitted)
Authentication-Results: domain_name;
    spf=pass smtp.mailfrom=sender_email_address;
    dkim=pass header.i=@domain_name;
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
Content-Transfer-Encoding: base64

base64_encoded_SMIME_message_body
```

Listing 1: Structure of an e-mail with ARC, DMARC, DKIM, SMIME, and SPF

Due to this added complexity on top of the basic e-mail design, running a secure e-mail service is relatively cumbersome. Especially as a violated or missing protocol could impair successful delivery of e-mails. Consequently, there are several companies that are specialised in providing secure e-mail services. Well known free e-mail providers utilising most of the mentioned key technologies are Google with its GMail¹ service and Microsoft with Exchange².

2.6 Identity and Access Management

Identity and Access Management (IAM) is a basic requirement of every effective security program in order to protect data, applications, and other assets. To be able to technically enforce it, i.e., only authorise legitimate requests, users must be reliably authenticated. This is usually done leveraging digital identities, e.g., usernames, which are linked to a person's actual identity. Typical standards used in this context are OAuth [13], OpenID [14], and Security Assertion Markup Language (SAML) [15]. Establishing and managing these digital identities seems to be a straightforward task but can become very complex once the number of employees and other stakeholders of an organisation increases.

Therefore, IAM providers do not only offer the corresponding technologies but also best practices in the form of pre-defined processes and concepts. Typical functionalities offered by IAM providers include but are not limited to:

- Initial registration of users.
- Assignment of roles and privileges.
- Creation, provision, and management of credentials.
- Centralised management of identities, roles, and privileges.
- Centralised authentication and authorisation of users
- Provision of means for Multi-factor Authentication (MFA)
- Support of interfaces for Single sign-on (SSO) services

Accounts with a very high level of privileges, e.g., administrators or superusers, are a popular target of threat actors and prone to insider risk. They should therefore be additionally protected leveraging Privileged Access Management (PAM).

2.7 Cyber Insurance

In the last few years, the frequency and impact of cyber incidents against companies worldwide continued to increase steadily [16]. While some industry segments were hit less frequently than others [17], there is no guarantee for anyone to be spared to move into the focus of threat actors. Hence, no matter how much money a firm spends on its security program, or which technical

¹<https://gmail.com>

²<https://outlook.live.com>

prevention controls it implements, there is a residual risk of being hit by a cyber-attack that might lead to reputational and/or financial loss for the victim.

The purpose of Cyber Insurance is to step in if an insured victim experiences such a reputational or financial loss arising out of a covered cyber incident. Coverages that are generally offered by insurance companies include:

- First party damages (i.e., losses directly occurred to the policyholder) covering own costs (e.g., business interruption costs, incident response and forensics expenses, the launch of public relation campaigns, installation of call centres to inform customers).
- Third party liability (e.g., claims made against the policyholder by a third party) covering costs to indemnify the claimants for a loss and the expenses of defending lawsuits associated with it. In many cases, these losses arise from the failure of an organisation to appropriately protect third parties' data from being breached or compromised through a cyber incident.

Additionally, many insurance carriers offer further services to their customers such as establishing connections to forensic and incident response firms as well as consultancy services. This is beneficial for both, the insurance carriers and the insureds, as both are interested in quick recovery after an incident to reduce costs.

While the process for a company getting cyber insurance certainly can differ, there are some steps each carrier performs before offering a binding quote for cyber coverage:

1. Assessment of cyber exposure based on industry, company size, and business model.
2. Evaluation of security protection level by on-site visits, conversations, questionnaires, and/or cyber risk scanning and analytics tools.
3. Legal wording of cover elements and exclusions.
4. Actuarial calculation of potential losses, maximum capacity, and corresponding premium.

With the recent surge of cyber incidents, insurance companies started to be more selective on offering cyber insurance. Companies need to fulfil minimum security standards defined by each carrier. In addition to that, insurers need to protect themselves from large scale events which can hit multiple clients at once, so-called accumulation risks. Scenarios which are under discussion and currently excluded by most carriers are cyber incidents which arise out of any kind of cyber war (whether declared or not) and the outage of external networks, such as the internet or electricity supply.

2.8 Incident Response

There is a saying that companies should not ask themselves if they are vulnerable to a security incident but only when and to which extent this incident may occur. Keeping that in mind, it is important to be prepared for the moment in which such an incident happens. Therefore, Incident Response (IR) services should not only provide support during an incident. According

to the National Institute of Standards and Technology (NIST), the incident response life cycle encompasses a total of four phases as shown in Figure 3:

1. Preparation.
2. Detection and Analysis.
3. Containment, Eradication, and Recovery.
4. Post-Incident Activity.

Ideally, an IR service covers all of these phases. This makes rapid response much more likely, as information from all phases is directly available during the actual IR and does not have to be shared cross-organisationally among different service providers, which would cost valuable time.

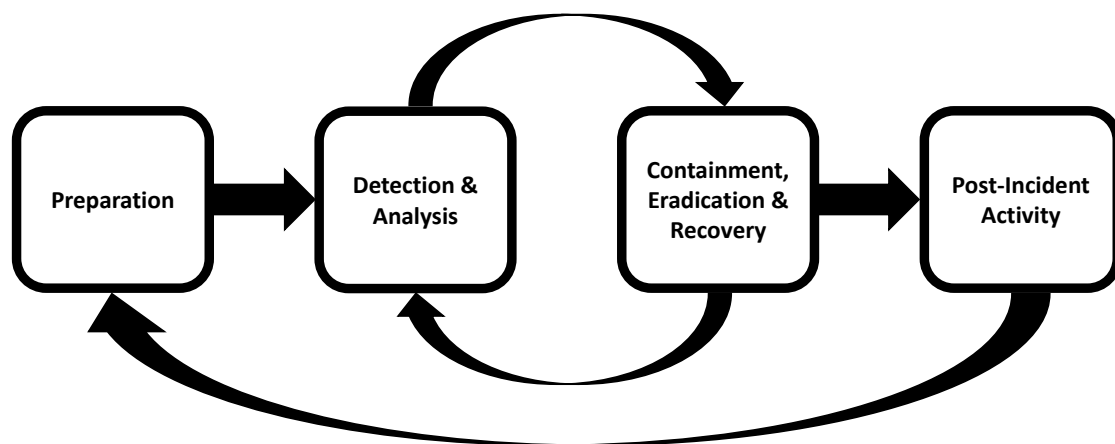


Figure 3: Incident response life cycle according to NIST SP 800-61 Rev. 2 [18].

Before the actual incident, incident response services encompass consultation on technology enabling the customer to detect and contain incidents, e.g., solutions for Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR). Furthermore, one of their technological focuses is on configuring the customers' infrastructure not only securely but in a way that retains and protects information which is valuable for incident handling and investigation, e.g., read-only backups and audit logs. Apart from these technological measures, IR also encompasses preparation on an organisational and human level, including the preparation of customised response plans and playbooks as well as regularly putting their content into practice through tabletop exercises. Ideally, these tabletop exercises are as inclusive as possible, involving not only representatives from IT (security) but also from operations, legal, human resources, public relations etc.

For the case where a potential incident has been detected, IR services ideally offer an emergency hotline which can be consulted 24/7 in order to provide support during the process of triage and first response. Once it is confirmed that the initial alarm has not been a false positive, IR services begin with evidence collection and root cause analysis. In order to be prepared for potential court

cases and to support law enforcement, it is paramount to document the analysis as thoroughly as possible and maintain the chain of custody during forensics.

When affected parts of systems and networks are identified, an appropriate containment strategy, such as powering them off or disconnecting them from other parts of the network, has to be chosen. The choice heavily depends on the pursued, sometimes conflicting objectives besides the actual containment, e.g., preserving evidence even in non-persistent memory or stopping a ransomware attack from continuing to encrypt data. Once the threat is contained, it has to be eradicated, e.g., by wiping malware, mitigating vulnerabilities, and disabling compromised accounts. After that, recovery can take place, e.g., by resetting passwords and restoring systems.

As indicated in Figure 3, the described phases are not strictly linear but rather part of an iterative, recurring process. Depending on the organisational and technological environment of the individual incident, IR engagements can happen on premise, remotely, or in a mixed mode, depending on the phase.

2.9 Business Continuity / Disaster Recovery Planning

The planning of IR and Business Continuity / Disaster Recovery (BCDR) are closely related. However, the scope of BCDR goes beyond potential business interruptions caused by security incidents and does primarily focus on the continuity and recovery of the core business, i.e., keeping critical processes running independently from the environment or restore them as quick as possible, respectively. Since these core processes change over time, BCDR also must dynamically adapt and is therefore not a task to do once but a continuous process which can be managed systematically according to ISO 22301. Just as IR, BCDR is a highly interdisciplinary process involving various stakeholder groups to discuss and define a desirable yet realistic Recovery Time Objective (RTO), Recovery Point Objective (RPO), as well as the corresponding measures. BCDR as a Service can include the organizational part of moderation, consolidation, and documentation of these stakeholders' requirements in the form of a BCDR plan but also what is called Recovery as a Service, meaning backup and restore solutions hosted in the cloud.

2.10 Security Information and Event Management

As previously mentioned, SIEM can be very helpful when it comes to the detection and investigation of security incidents. Besides the pure aggregation of potentially security-related information, e.g., log files or real-time network data, from a variety of sources, it can also offer continuous monitoring and correlation to automatically (e.g., by anomaly detection) or semi-automatically (e.g., by pre-configured use cases) detect suspicious activities. Additional factors to be considered are intuitive user interfaces and flexible support of formats and protocols to include data from as many nodes as possible, as well as the scalability to be able to serve the dynamic landscape of a growing business. Apart from the option to deploy and use it on premise, it can also be deployed in the cloud and observed by well-trained analysts of the provider, ideally working in shifts to provide 24/7 coverage. This comes with the advantage that security alerts can be analysed directly when they happen, i.e., without long delays after business hours or on weekends.

2.11 System Patching and Updates

With the disclosure of software vulnerabilities, vendors are required to correct them as fast as possible, since they might be discovered and exploited by attackers to gain access to a computer system. Reacting as fast as possible to disclosed vulnerabilities is commonly called patching, since it is critical to preempt attackers. Good historical examples where software updates were mission critical are Heartbleed³, Triple-Seven⁴, Shellshock⁵, and EternalBlue⁶. What these vulnerabilities have in common is a large and possibly fatal impact on the attacked IT infrastructure:

- They can be easily discovered by an attacker.
- They are easily exploitable (usually few lines of e.g. Python code).
- They have a fatal impact, for instance Remote Code Execution (RCE) or sensitive information leaks.

Fortunately, software updates for such kinds of critical vulnerabilities usually are available very quickly. For instance, patches for the famous Heartbleed vulnerability were available even before it was privately disclosed to the development team. Seven days after the disclosure an official release of the affected software was available⁷. At the time of disclosure there were a round 300k vulnerable servers online. It is surprising that six years later there were still 200k vulnerable servers online⁸.

These examples show the necessity of keeping up with evolving threats. Therefore cyber security systems need to track the current state of the art of available countermeasures. For instance, software modules that process untrusted data are one of the most critical parts to protect, as they are directly accessible by attackers. Operating systems provide mechanisms offering basic protection which in general limit the attack surface. In order to benefit from such cautionary measures regular security updates and reviews are desired.

Software updates in production are rolled out via well-established update mechanisms. In Free and open-source software (FOSS) environments packet management systems, such as `apt`, `dnf`, or `pacman` are common. Usually, there are different update tracks including stable updates (i.e., stability and security updates) or bleeding edge (i.e., new features are deployed as fast as possible). In non-FOSS environments there might be proprietary solutions with similar semantics. Careful reviews of the used software repositories are required when building products or infrastructures relying on these updates. CSaaS companies ensure that maintained components or services stay up-to-date and are not affected by known vulnerabilities.

³<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>

⁴<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777>

⁵<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271>

⁶<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>

⁷<https://www.smh.com.au/technology/heartbleed-disclosure-timeline-who-knew-what-and-when-20140414-zqurk.html>

⁸<https://isc.sans.edu/diary/26798>

2.12 Security Standards Compliance

With the rising number of networked devices and digitisation of most parts of our lives in the context of the Internet of Everything, the number of security-related regulations and industry-specific standards which need to be considered continuously increases. Examples include:

- General Data Protection Regulation (GDPR),
- ISO/IEC 27001 Information Security,
- ISA/IEC 62443 Cybersecurity for Operational Technology,
- ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering,
- NIST 800-171 Security controls and processes for data protection,
- Cybersecurity Maturity Model Certification (CMMC) program,
- the European Cyber Resilience Act, and more to come.

Auditing the compliance with the requirements defined in these documents requires subject matter expertise and can be time-consuming. Therefore, it is often outsourced. With more and more services in the cloud, there are also approaches to check the compliance with specific requirements fully automated [19].

3 Future of CSaaS

Future CSaaS offerings will potentially have to consider different currently ongoing trends in the security landscape. For example, there is the already mentioned threat of AI-enhanced malware. However, AI also poses other security threats to companies and public organisations, e.g., in the form of deep fakes or ChatGPT-generated spear-phishing campaigns. Considering the ease of use of tools like ChatGPT, tailored spear-phishing could have the potential to supersede normal Spam not only in terms of quality but also in numbers. Another trend is the increasing number of supply chain attacks [20]. This may lead to an increased demand for zero trust architectures (ZTAs), especially towards previously trusted third parties, which can be potential starting points for the mentioned supply chain attacks, as well as for enhanced protection of customer data needed to deliver specific managed security services, e.g., SIEM. Moreover, existing trust relationships, for example, towards critical information infrastructures such as certificate authorities (CAs), have to be reconsidered and enhanced control mechanisms need to be established [21]. Eventually, the rise of quantum computers may not directly lead to new types of services. However, it will definitely have an impact on existing services. They will have to timely adapt to the new post-quantum algorithms once they are finally standardised by NIST to ensure future-proof security is also protecting against *store now, decrypt later* type of threat scenarios.

4 Findings and Suggestions

The fact that 95% of all company malware breaches are caused by human error [9], has precipitated in the volume of companies currently adopting cyberawareness training programs to increase by 15% year on year to date and the cyber awareness training market to reach a predicted \$10 billion annually by 2027 [22]. Additionally, the number of companies opting to pay for cyber insurance has risen steadily over the last three years partly due to a large number of high profile attacks during this time frame and the war in Ukraine. However, the uptake has now started to level off mainly due to the estimated 83% hike in cyber insurance premiums over the last 12 months and the purchasing of better IT security equipment (e.g. next-gen firewalls and business continuity solutions) [23]. As working from home, either partly or totally, has become more mainstream for employees around the world, companies have had to look at new ways to protect their employees and intellectual property from malware attacks. As company IT staff cannot effectively protect all of these new remote working location, decision makers are opting for CSaaS companies to assist with this large threat canvas. This new working model bodes well for the future growth of the IT security services industry. Finally, the new elephant in the room, from a security threat perspective, is the mobile phone. These ultra portable computers can now handle most of the day-to-day employee tasks like answering email, attending meetings, workflow approvals to reading and writing company documents. Most companies still overlook the security threat that mobile phones pose. They are finally taking action by installing anti-malware protection on these devices, allowing them access to guest wireless networks only and banning them from company meetings.

5 Conclusion

It is important to mention that the protection demand of a specific organisation can be highly individual depending on factors, such as the sectors they are doing business in and the type of data they manage. The list of security services therefore only covers a selection of services which are most likely to be relevant for the majority of companies. When deciding which protection needs are applicable for an individual organisation, it is recommended to include representatives of the organisation's stakeholders and utilise independent advice from external specialists, where needed. Companies employing connected manufacturing processes in the context of Industry 4.0, for example, might have an increased demand for monitoring focusing particularly on Industrial Control System (ICS) or Operational Technology (OT) which implies factors like safety and therefore another kind of security goal prioritisation. Explaining such sector-specific demands is not within the scope of this chapter.

In Table 1, the different services described throughout this chapter are mapped to the initially mentioned top ten companies in the managed and professional security services market in Europe according to Frost & Sullivan. It shows that almost all services are delivered by most of the discussed companies with just a few exceptions. One outstanding exception is cyber insurance. That is because cyber insurance is traditionally provided by traditional insurance companies rather than by tech companies specialising in cyber security services. However, representatives of both sectors do closely collaborate, e.g., regarding consulting and incident response services,

Table 1: Mapping CSaaS to top ten professional security providers according to Frost & Sullivan [7].

	Accenture	Capgemini	Orange Cyber Defense	Atos	IBM	Infosys	KPMG	Computa- center	Deutsche Telekom	Telefonica Tech
Security Personnel as a Ser- vice	○	○	●	●	●	○	●	○	●	○
Cyberawareness Training	○	●	●	○	●	●	●	○	●	○
Vulnerability Assessment	●	○	●	●	●	●	●	●	●	●
Periodic Penetration Testing	●	●	●	●	●	●	●	●	●	●
Email Security	○	○	●	●	●	●	○	●	●	●
IAM	●	●	●	●	●	●	●	●	●	●
Cyber Insurance	○	○	○	○	○	○	○	○	○	○
Incident Response	●	●	●	●	●	●	●	●	●	●
BCDR	●	●	●	●	●	●	●	●	●	○
SIEM	●	●	●	●	●	●	●	●	●	●
System Patching and Updates	●	●	○	○	○	○	○	●	○	●
Security Standards Compli- ance	●	●	●	●	●	●	●	●	○	●

as already described in the corresponding section of this chapter. There are even product bundles such as Deutsche Telekom’s “Magenta Security Shield” which includes technical monitoring and response services as well as cyber insurance. Although a bundled offer, the latter is, however, backed by the Allianz insurance company.

Table 1 is based on open-source intelligence, leveraging marketing channels such as the vendor’s web sites, service brochures, and white papers which are publicly available via the Internet. If vendors are not mapped to a specific service, it does not necessarily mean that they are not offering this service. Rather, it means that no information regarding this service from the specific vendor could be found at the point in time our investigation took place. Ultimately, what this all means is that the demand for CSaaS and additional security services, will increase in tandem with the expanding threat landscape that has created a real sense of fear across the entire Internet of Everything landscape.

References

- [1] Cloud Security Alliance - Security as a Service Working Group. *Defined Categories of Security as a Service*. 2016. URL: <https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf>.
- [2] Manish Sahay. *Who Invented the Antivirus? A History of Antivirus Software*. Tech. rep. thePCinsider, 2023.
- [3] Statista. *Annual number of data compromises and individuals impacted in the United States from 2005 to first half 2022*. 2023. URL: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>.
- [4] Robert Johnson. *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked*. Jan. 2019. URL: <https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/>.
- [5] D. Kirat, J. Jang, and M. P. Stoecklin. *DeepLocker - Concealing Targeted Attacks with AI Locksmithing*. 2018. URL: <https://i.blackhat.com/us-18/Thu-August-9/us-18-Kirat-DeepLocker-Concealing-Targeted-Attacks-with-AI-Locksmithing.pdf>.
- [6] International Information System Security Certification Consortium (ISC)². *Cybersecurity Workforce Study*. 2022. URL: <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>.
- [7] Frost & Sullivan. *European Managed and Professional Security Services Market*. Aug. 2022. URL: <https://store.frost.com/european-managed-and-professional-security-services-market.html>.
- [8] Statista. *Size of the Security as a Service (SECaaS) market worldwide from 2022 to 2033*. Jan. 2023. URL: <https://www.statista.com/statistics/595164/worldwide-security-as-a-service-market-size/>.
- [9] IBM Security. *X-Force Threat Intelligence Index 2022*. Page 16, Sum of top infection vectors linked to human error. June 2022. URL: <https://www.ibm.com/downloads/cas/ADLMYLAZ>.
- [10] Holm Security. *New Office 365 phishing tactics are difficult to spot but easy to prevent*. June 2020. URL: <https://www.rmtechteam.com/blog/new-office-365-phishing-tactics-are-difficult-to-spot-but-easy-to-prevent>.
- [11] Holm Security. *Next-Gen Vulnerability Management*. Mar. 2023. URL: <https://www.holmsecurty.com/>.
- [12] Rafiq Ahmad Khan et al. "Systematic Mapping Study on Security Approaches in Secure Software Engineering". In: *IEEE Access* 9 (2021), pp. 19139–19160. doi: 10.1109/ACCESS.2021.3052311.

- [13] Dick Hardt. *The OAuth 2.0 Authorization Framework*. RFC 6749. Oct. 2012. DOI: 10.17487/RFC6749. URL: <https://www.rfc-editor.org/info/rfc6749>.
- [14] N. Sakimura et al. *OpenID Connect Core 1.0*. Nov. 2014. URL: http://openid.net/specs/openid-connect-core-1%5C_0.html.
- [15] Brian Campbell, Chuck Mortimore, and Michael Jones. *Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants*. RFC 7522. May 2015. DOI: 10.17487/RFC7522. URL: <https://www.rfc-editor.org/info/rfc7522>.
- [16] Mike Mclean. *2023 Must-Know Cyber Attack Statistics and Trends*. 2023. URL: <https://www.embroker.com/blog/cyber-attack-statistics/>.
- [17] Troy Beamer. *What Industries Are Most Vulnerable to Cyber Attacks In 2022?* 2023. URL: <https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/>.
- [18] Paul Cichonski et al. *Computer Security Incident Handling Guide*. en. 2012-08-06 2012. DOI: <https://doi.org/10.6028/NIST.SP.800-61r2>.
- [19] Philipp Stephanow and Christian Banse. *Clouditor-continuous cloud assurance*. Tech. rep. Fraunhofer AISEC, 2017.
- [20] European Union Agency for Network and Information Security (ENISA). *ENISA Threat Landscape for Supply Chain Attacks*. 2021. URL: <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks/@download/fullReport>.
- [21] Michael P. Heintz et al. "MERCAT: A Metric for the Evaluation and Reconsideration of Certificate Authority Trustworthiness". In: *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, CCSW'19*. London, United Kingdom: Association for Computing Machinery, 2019, pp. 1–15. ISBN: 9781450368261. DOI: 10.1145/3338466.3358917.
- [22] Steve Morgan. *Security Awareness Training Market To Hit \$10 Billion Annually By 2027*. Apr. 2023. URL: <https://cybersecurityventures.com/security-awareness-training-market-to-hit-10-billion-annually-by-2027/>.
- [23] Ankura. *The Cybersecurity Insurance Market: What to Expect in 2023*. Mar. 2023. URL: <https://www.jdsupra.com/legalnews/the-cybersecurity-insurance-market-what-2446460/>.