Computers & Security 141 (2024) 103844

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A logging maturity and decision model for the selection of intrusion detection cyber security solutions

Manuel Kern [a,*], Max Landauer [a], Florian Skopik [a], Edgar Weippl [b]

[a] *Austrian Institute of Technology, Giefinggasse 4, Vienna, 1210, Austria*
[b] *University of Vienna, Universitaetsring 1, Vienna, 1010, Austria*

ARTICLE INFO

Keywords:
Intrusion detection
Logging and monitoring
Standards
Guidelines
Maturity level
Decision model
Survey
sme

ABSTRACT

Many modern cyber attack techniques cannot be prevented. Logging and monitoring, however, offer a means to at least detect these techniques early, and therefore become increasingly important for defense. Many companies are unfortunately reluctant to invest more in cyber security logging and monitoring or hire additional security staff to operate detective solutions. There is a need for a methodology to pick appropriate cyber security solutions from the vast pool of available products. Our model takes requirements mandated by common standards from ISO, NIST, BSI and the like into account. While standards and guidelines remain at a high abstraction level and are applicable to different organizations over a long period of time, guidance on implementation becomes outdated comparatively quickly. We propose a novel logging maturity and decision model for the selection of the best fitting cyber security solutions for an organization. The novelty is that this model accounts for constraints in the selection process, such as cost, complexity, compliance, and relevance to the organization's assets. We validate the model with MITRE ATT&CK framework data and apply it to illustrative use cases based on our survey.

1. Introduction

Recent reports show that the level of sophistication of cyber attacks has been steadily increasing in recent years, with attackers remaining undetected in organizations for long periods of time (IRBM Corp, 2022). Safety-critical systems are increasingly based on commodity IT equipment, making them vulnerable to cybersecurity attacks. Standards establish mandatory security requirements ensuring that processes, systems and applications are securely implemented and operated, while guidelines are recommended best practices and supplement standards where a margin of discretion is possible. Procedures on the other hand describe the steps required for a task or process to be operated in alignment with standards. Organizations may or must comply with standards because of internal (self-set requirements / market strategy) and external (contractual / regulatory) influences. For example, in the United States federal agencies and their contractors that operate or manage federal IT networks are required to implement NIST SP800-53 (NIST, 2020a). In 2015 NIST SP800-171 (Ross et al., 2021a) was released to provide requirements for protecting controlled unclassified information that applies to government contractors.

Following standards and best practices is an effective means to achieve a high level of security and to avoid blind spots (Skopik et al., 2022). However, standards and guidelines are often too generic in nature to provide actionable advice. While standards and guidelines address *what* is required to fulfill goals and objectives, procedures deal with the *how*. For example, an organization that wants to detect cyber threats in their systems to achieve their business goals (*why*), may or must use standards and guidelines that supply them with *what* is required. A common taxonomy for the technical and administrative safeguards within a standard are controls. Typically, a standard consists of multiple controls that are measured to verify the implementation state of a standard. Multiple controls are often consolidated to control families or control groups and specify an area of focus. The Center for Internet Security (CIS) Critical Security Controls (Center for Internet Security, 2021), used to achieve the goal of threat detection, are mainly found in the control group (i) Audit Log Management and (ii) Network Monitoring and Defense, but do not go into much detail of *how* to

* Corresponding author.
E-mail address: manuel.kern@ait.ac.at (M. Kern).

https://doi.org/10.1016/j.cose.2024.103844
Received 16 December 2023; Received in revised form 8 March 2024; Accepted 4 April 2024
Available online 9 April 2024

achieve this. Procedures fill this gap but must be very precisely adapted to the organization (including the underlying systems, applications and processes) in scope. Therefore, a procedure has the shortest lifetime and is the least universally applicable compared to standards and guidelines that have a higher abstraction level. This is simply because organizations, their processes, technology and threat landscape are continuously changing and evolving; and in their combination unique to each organization. Logging and monitoring solutions support addressing the *how* by automating and encapsulating the steps required for threat detection.

Cyber security standards, often referenced as frameworks, are very extensive as they cover multiple cyber security aspects, but do not go into great implementation detail. Organizations have to establish security processes and procedures which are supported and automated utilizing logging and monitoring solutions. Because of the increasing scales of cyber attacks and the paradigm shift towards a presumed compromise (an attacker operates already in the system for a long time), there is a vast amount of logging and monitoring solutions. This essentially leads to the following problems:

- Organizations are overwhelmed with security solutions and guidance but resources are limited. It is especially difficult for small and medium enterprises (SMEs) to adequately address security issues. There is no dedicated security personnel, there are many standards and guidelines available but it is challenging to obtain an overview of what is relevant for a specific context (company size, deployed technology stack, market situation, risk profile) and even more challenging to objectively assess and select a specific solution and guideline.
- Choosing the wrong logging and monitoring solution leads to security misinvestment and a dramatically increased risk of attackers operating undetected for long periods of time causing drastic damage.
- Compliance with standards may not lead to the expected result. It is necessary to further strengthen monitoring and detection capabilities. This is corroborated by the memorandum M-21-23 from 2021 to improve the Federal Government's investigative and remediation capabilities (Executive Office Of The President, 2021) as a response to recent events, including the SolarWinds incident.

We therefore propose a method to assess the current state of logging in organizations and, building on the identified assets and requirements, automatically recommend solutions as quick-wins. There is a need for a simple decision model that generates quick wins for organizations. In addition, we propose a maturity model to drive the implementation of logging and monitoring capabilities based on a collection and distillation of existing security frameworks, with three levels of succession, making it ideal for building logging and monitoring capabilities in the SME sector.

We summarize our contributions as follows:

1. An empirical study of the technologies/software used, how these solutions are operated, and the planned investments in personnel and monitoring solutions,
2. a logging and monitoring maturity model,
3. a novel decision model for the assessment and selection of logging and monitoring solutions, and
4. an evaluation of aforementioned models in an illustrative scenario.

The remainder of this paper structures as follows: Section 2 summarizes related work, while Sect. 3 describes the concept of the proposed model. Our survey that serves as a base for the illustrative use case is presented in Sect. 4. A logging and monitoring maturity model is presented in Sect. 5 which serves as an input for the decision model to assess and select logging and monitoring solutions presented in Sect. 6. The results are discussed in Sect. 7 and finally Sect. 8 concludes the paper and outlines future work.

2. Related work

Dube and Mohanty (2020) developed a cybersecurity maturity model including System Security Engineering Capability Maturity Model (SSE-CMM), NIST Cyber Security Framework (CSF), and others by comparing the strengths and limitations of current maturity models and conducting an empirical analysis with 200 industry experts. Kim et al. (2022) establish a framework for Internet of Things (IoT) data quality maturity compliant to ISO 8000-61/62 and review several software quality and data quality maturity models including Capability Maturity Model Integration (CMMI), data management maturity (DMM) and others. In contrast, our maturity model is specific to threat detection and aligns with already proven and well-known cyber security best practices. Therefore it is directly applicable by organizations. Ponsard and Grandclaudon (2018) survey standards and practical guidelines such as ENISA, ANSSI and the like with focus on applicability by Small Medium Businesses (SMEs). They find that ISO27001 (Int. Org. for Standardization, 2013) is too complex for SMEs to adapt. Antunes et al. (2021) conducted a case study which shows that the SMEs audited and surveyed reap significant benefits due to the robustness of their information security management and the cyber awareness of their employees. Kabanda et al. (2018) emphasize that SMEs in developing countries usually do not process logs due to budget, management support, and attitude; the lack of complex business processes is seen as an advantage. When compliance with standards was forced by external factors, SMEs adopted open-source and cloud computing solutions. A case study by Rawindaran et al. (2021) on the cost-benefit analysis of deploying Intrusion Detection Systems (IDS) in SMEs showed that open source solutions require a certain level of expertise compared to commercial products. They also note that while anomaly-based IDS solutions offer great benefits in detecting zero-day attacks, they come at a cost to the IT infrastructure and staff managing the technology. They conclude that SMEs need to strike a balance between technology and cost.

Llansó et al. propose a method for selecting cybersecurity measures based on an organization's priorities and constraints using a capability-based representation of measures, while also considering cost, impact, applicability, effectiveness, and other criteria. Although this solution sounds promising, we argue that applying their multicriteria decision making (MCDM) and multicriteria decision analysis (MCDA) approach in a real-world scenario in the cybersecurity detection systems domain is too complex and impractical for organizations. Our solution considers cost, complexity, and compliance requirements based on the latest cybersecurity frameworks and is focused on detection coverage of attack techniques. It builds on existing expert catalogs and is designed for detection and response, and also takes the likelihood that a vulnerability will be exploited and an organization's risk appetite into account. It is much more focused on logging and monitoring, and significantly improves all previous approaches by introducing a methodology that provides directly applicable solutions tailored to an organization's constraints.

In Sect. 5 we outline the state of the art of logging and monitoring standards and guidelines.

3. Concept

Many organizations, in particular, SMEs, often find it difficult to assess their security requirements and select adequate solutions that fit their needs. In this section we therefore outline a concept for the selection of logging and monitoring solutions. Fig. 1 depicts an overview of this workflow, where gray boxes are state-of-the-art solutions and empirical studies that mainly act as sources of information for our concept, orange boxes are models presented as the main contributions of this paper, green boxes are the outcomes of the workflow, and white boxes are normal activities that are carried out as part of the proposed workflow. As visible in the figure, the workflow consists of three phases. In the

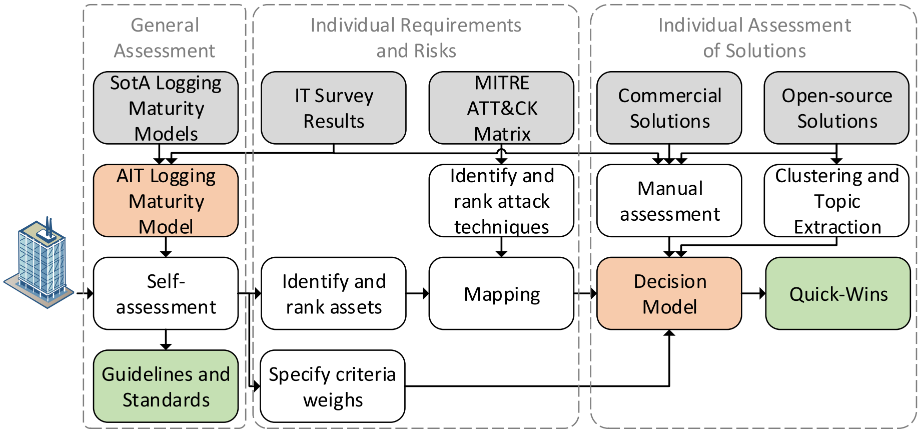


Fig. 1. Workflow to improve organizational logging maturity with two-fold output: First, self-assessment with the maturity model points to relevant guidelines and standards. Second, recommendations for logging solutions are provided based on available assets, organization-specific criteria, and pre-existing information on attack techniques and logging solutions. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

first phase, organizations assess their logging capabilities with the maturity model presented in Sect. 5. We construct this model to address gaps with existing maturity models and also incorporate findings from a survey among stakeholders that we discuss in detail in Sect. 4.

In the second phase, we map assets of organizations to applicable attack techniques provided by the well-known attack framework MITRE ATT&CK[1] to identify relevant attack cases. We thereby rely on a weighting scheme for ranking attack techniques that was proposed by Kern et al. (2022). The third phase of the workflow comprises the decision model that selects solutions based on their abilities to detect attack techniques identified in the previous phase as well as other criteria important for the organization, such as price and complexity of the solution. Thereby, we consider both commercial as well as open-source solutions that we assess to rate their feasibility for attack detection. This procedure is carried out either manually through surveys or semi-automatically using machine learning techniques and publicly available documentation. We provide a thorough description of the selection procedure in Sect. 6.

4. Stakeholder survey

To base our assessments and illustrative use-cases on real-world data we conducted a survey among several stakeholders. This section summarizes and interprets its results.

4.1. Setup of the survey

The purpose of the survey is to gain a general overview of the state of logging in organizations. We identified four main areas for questioning: (i) *Organizational characteristics* includes questions on industry sectors and size of the organization. (ii) *Technical environment* concerns the availability of software and security solutions for monitoring and logging. (iii) *Investments* helps to assess the willingness to increase financial spending on security, preferred cost models for security solutions, and planned changes of currently used technologies. (iv) *Personnel* concerns the number of employees or person hours assigned for security as well as the experience and training of these employees.

We prepared a form comprising single- and multiple-choice questions as well as text boxes to enter numbers. The form was hosted as an anonymous survey online and subsequently distributed to potential stakeholders via cyber security mailing lists and direct messages to customers or partners. In the following we present the obtained answers and interpretations of some of the aforementioned questions in detail.

4.2. Survey results

After hosting the survey for one month, we received answers from 29 organizations. Thereby, we aggregated all obtained answers by the specified number of employees to investigate whether there are any significant differences in the overall trends with respect to the size of the organization. In particular, we differentiate between micro (1-9 employees), small (10-49 employees), medium (50-249 employees), and large (>250 employees) organizations, which we mark with distinct colors in the following visualizations.

Fig. 2 shows an overview of responses to some of the questions that we selected as particularly interesting for the purpose of this paper. Note that each organization was able to mark several answers as applicable. The leftmost block shows the prevalence of common operating systems, where the vertical axis depicts the total number of organizations that stated that the respective operating system is used by their employees. It is not surprising to see Microsoft Windows on top of the list as their global market share for desktop operating systems is around 75% as of August 2022.[2] The comparatively high fraction of Linux/Unix operating systems can be explained by the fact that our surveyed organizations are primarily in the Information and Communications Technology sector, where these operating systems are more common.[3] These overall trends are similar across all organization sizes.

Regarding the installation location of software used by employees, there is a slight tendency for installation on client computers over servers and cloud providers. Again, the distribution across organization sizes is similar for each alternative. The block on deployed security solutions shows that both commercial as well as open-source solutions are commonly used; few organizations outsource security and only a single one has no solution in place. Only micro organizations have a tendency to utilize open-source solutions over commercial solutions. Thereby, there is no clear preference between running costs that are mainly required to pay for subscriptions of commercial solutions and staff costs necessary for maintaining open-source solutions. However, few organizations prefer one-time investments.

Our question on security responsibilities shows that a vast majority of participants stated to have dedicated staff for maintaining security within the organizations. Only few organizations rely on external

[1] https://attack.mitre.org.

[2] https://gs.statcounter.com/os-market-share/desktop/worldwide/.

[3] https://truelist.co/blog/linux-statistics/.

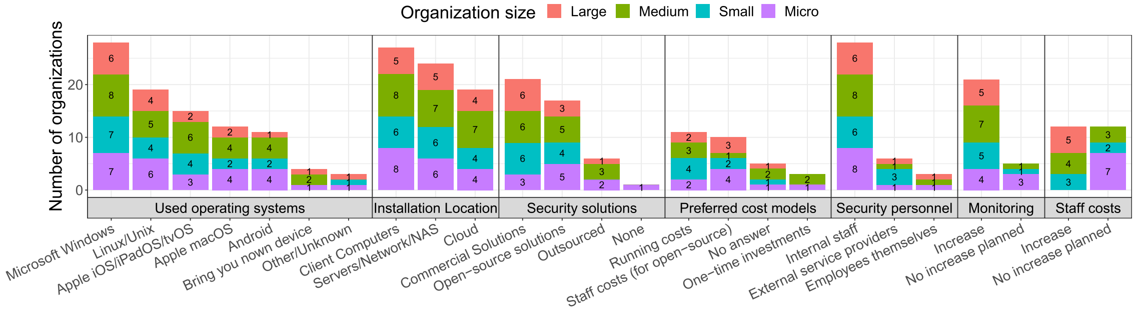


Fig. 2. Survey responses on technical and managerial states of organizations in the IT domain.

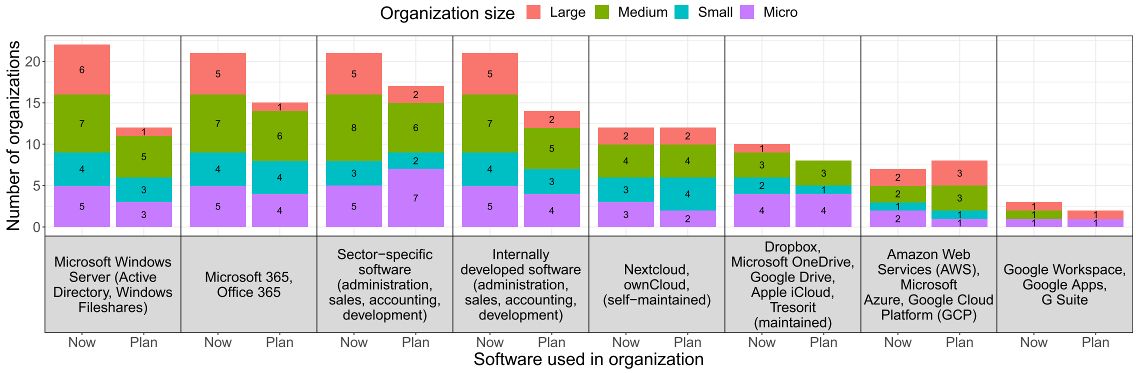


Fig. 3. Survey responses on applications currently used within organizations and projections on a 3-5 year horizon show no significant changes, except a decline of certain services in large organizations.

security providers, even fewer delegate security responsibilities to employees. Other than aforementioned results, there are clear differences between organization sizes when it comes to investment plans. The last two blocks show that the willingness to spend money on monitoring and logging as well as staff costs for security personnel increases with the organization size. In particular, none of the micro organizations plan to increase security staff while all of the large organizations do.

We also surveyed applications currently deployed in organizations and future plans of using them. Fig. 3 shows that Microsoft Windows Server and Microsoft 365 are currently the most wide-spread applications, on a par with sector-specific and internally developed software. Self-maintained cloud solutions (e.g., Nextcloud), managed cloud solutions (e.g., Dropbox), Amazon Web Services, and Google applications are less prevalent. Interestingly, the projections on a three to five year horizon show that primarily large organizations plan to decrease the deployment of Microsoft products as well as sector-specific and internally developed software.

The survey results allow us to derive some general profiles for organizations that we will use for our illustrative evaluation in Sect. 6. Large organizations run many commercial security solutions but some open-source solutions as well. They have full-time employees for security, plan to make significant investments in monitoring and security staff, and are willing to change large parts of their technology stack. SMEs on the other hand tend to be more conservative: They plan significantly fewer investments and largely retain their currently deployed technologies, in particular, Microsoft 365. They have a slight preference towards running costs, i.e., use software-as-a-service or managed by service providers.

5. Log maturity model

Based on a review of common standards and guidelines, we define a model to implement and operate logging and monitoring in organizations.

5.1. Background

Over the past decades, a wide range of cybersecurity standards and guidelines have been built on proven best practice approaches. While some standards like ISO27001 are rather general and suitable for different types of organizations, others like the Payment Card Industry (PCI) Data Security Standard (LLC PCI Security Standards Council, 2022) are specific to sectors. In Table 1 we list the most well established cybersecurity frameworks in the English and German speaking community, complemented with guidelines and maturity models with a focus on logging and monitoring.

Some standards and guidelines include a maturity level based on enterprise cybersecurity capabilities, ranging from basic “cyber hygiene” protections for SMEs to advanced capabilities to defend against sophisticated targeted cyberattacks. This helps an organization to prioritize controls based on their current progress and their risk appetite. The higher the risk appetite, the lower the maturity level that has to be achieved. The SP 800-53B (NIST, 2020b) Control Baselines on the other hand are three baselines for low-, moderate- and high-impact systems depending on the criticality and sensitivity of the information stored, processed or transmitted. Rather than suggesting controls for organizations, SP800-53B relies on determining information criticality and sensitivity of systems. Besides these general frameworks that focus on all kinds of cybersecurity aspects, there are others with a focus on logging and monitoring listed in Table 1. A more recent guidance, and also the most detailed in terms of technical implementation, is M-21-31 (Executive Office Of The President, 2021). Besides general logging and monitoring requirements, three tiers ranging from basic to advanced logging requirements, technical details of data sources, the data to be stored, the format and retention period are given.

5.2. Logging and monitoring maturity model

The Logging and Monitoring Maturity model (LMM) provides a uniform view of the controls and best practices listed in Table 1. We

Table 1
Cybersecurity / logging & monitoring controls and guidance.

Name	Type	First / latest release	Levels	Incl. LMM
Security Logging Capability Maturity Model (Bromberger and Maraschino, 2012)	Logging Datasource Guideline	2012 / 2012	5	
Security Monitoring Capability Maturity Model (Bromberger and Maraschino, 2012)	Monitoring Guideline	2012 / 2012	5	
SP 800-53 Security and Privacy Controls for Information Systems and Organizations SP 800-53B Control Baselines (NIST, 2020a)	Cybersecurity Controls	2005 / 2020	3	x
Cybersecurity Maturity Model Certification (Carnegie Mellon University and The Johns Hopkins University, 2021)	Cybersecurity Certification	2019 / 2021	3	x
SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Ross et al., 2021a)	Cybersecurity Controls	2015 / 2021	-	x
SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information (Ross et al., 2021b)	Cybersecurity Controls	2021 / 2021	-	x
Application Security Verification Standard (ASVS) 4.0.3 (OWASP, 2021)	Application Security Controls	2009 / 2021	3	x
IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik, 2022)	Cybersecurity Controls	1994 / 2022	-	x
Minimum Cyber Security Standard (UK Gov., 2018)	Cybersecurity Controls	2018 / 2022	-	
SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) (Scarfone and Mell, 2012)	Monitoring Guideline	2007 / 2012	-	
SP 800-92 Guide to Computer Security Log Management (Kent and Souppaya, 2006)	Logging Guideline	2006 / 2006	-	
ISO/IEC 27002:2022 (Int. Org. for Standardization, 2022)	Cybersecurity Controls Guideline	2005 / 2022	-	x
Effective Daily Log Monitoring Guidance (PCI Security Standards Council, 2016)	Logging Monitoring Guideline	2016 / 2016	-	
Data Security Standard v4 (LLC PCI Security Standards Council, 2022)	Cybersecurity Controls	2004 / 2022	-	
CIS Controls v8 (Center for Internet Security, 2021)	Cybersecurity Controls	2008 / 2021	3	x
Cyber Security Guidance Technical User Edition (Ministry of Justice, 2022)	Cybersecurity Guideline	2017 / 2022	3	x
Improving the Federal Government's Investigate and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31) (Executive Office Of The President, 2021)	Logging Monitoring Controls	2021 / 2021	3	x

summarize cybersecurity and logging & monitoring controls and guidelines from materials that were recently updated (latest publication after 2020) and do not focus on sector-specific guidance. The frameworks are concerned with multiple cybersecurity domains and therefore information relevant to logging and monitoring has to be extracted. We do this by searching for the following keywords “log, record, monitor, collect, retention, retain, analyze, analysis”. We collect, group and unify the controls by manually reading through the relevant parts, as the taxonomy and structure differ. Our research has shown that three maturity levels are common in the cyber security domain. In version 2.0 of the Cybersecurity Maturity Model Certification (CMMC) (Carnegie Mellon University and The Johns Hopkins University, 2021), the five levels of CMMC version 1.0, were reduced to three levels. For LMM we propose three levels: basic, intermediate and advanced. As a baseline we follow the Center for Internet Security Controls (a well-known cybersecurity non-profit organization) which also propose three organization types. Compared to the CIS controls, the LMM recommendations are more detailed in the area of logging and monitoring, as we include information from a variety of sources and go deeper into implementation than the CIS controls, which contain general requirements at a higher level of abstraction. The assigned maturity value of each LMM is derived as follows: If there is already a CIS Top 18 (Center for Internet Security, 2021) or a M-21-31 (Executive Office Of The President, 2021) control that recommends a similar measure, categorization is applied to the derived LMM. If there is no similar control, it is verified if NIST SP800-53B (NIST, 2020b) categorizes the control, followed by the CMMC (Carnegie Mellon University and The Johns Hopkins University, 2021) and by the application-specific Application Security Verification Standard (OWASP, 2021) categorization in that order. The standards and guidelines marked “Include” (see Table 1) are carefully read, relevant controls are extracted, clustered and then summarized. This is a very time-consuming, manual process which is difficult to automate and requires domain knowledge since different names are used for similar activities. The result is a summarized catalog with more than 80 controls that cannot be published due to copyright restrictions of ISO 27001 / ISO 27002. To attain similar results without constructing the entire catalog as detailed earlier, readers are encouraged to consult (Executive Office Of The President, 2021). This guideline concentrates on logging and monitoring, and it introduces three distinct levels. In contrast to our LMM, the primary difference lies in the extent of detail provided in the control descriptions. For reference, an example of an LMM, which is subsequently utilized, is illustrated in Table 2.

6. Selection of security solutions

This section describes our decision model for the selection of security solutions.

Table 2
LMM 21 - illustrative sample.

Level	Name	Description
Interm.	Identify anomalies via a baseline	To identify system anomalies a system baseline has to be established. When establishing the baseline consider normal and peak conditions; usual access times, access locations, frequency of each user and group (Int. Org. for Standardization, 2022; NIST, 2020a; Center for Internet Security, 2021; Bundesamt für Sicherheit in der Informationstechnik, 2022; Executive Office Of The President, 2021; Ministry of Justice, 2022).

Table 3
Used symbols and their definitions.

Sym.	Definition	Sym.	Definition
S	Monitoring or logging solution, e.g., $S1$.	S_p	Price of solution S, e.g., $S_p = 10\$/\text{user/m}$.
S_c	Compl. of solution S, e.g., $S_c = 1$ (low).	S_l	Fulfillment of level req. of solution S.
C	Comb. of solutions, e.g., $C = \{S1, S2\}$.	C_p	Price of combination C.
C_c	Compl. of combination C.	C_l	Fulfillment of level requirement of comb. C.
T	Attack technique, e.g., $T1566$.	T_w	Weight of attack technique, e.g., $T_w = 51$.
T_r	Rel. of technique, e.g., $T_r = 2$.	$\mathcal{T}_S$	Set of techniques covered by comb. C.
O	Specific organization.	O_p	Desired solution price of org. O.
O_c	Desired solution compl. of org. O.	O_w	Weight vector for price, compl., and level.

Table 4
Sample organizations.

ID	Employees	GB / Employee	Desired Price O_p	Price weight O_{w_p}	Complex. O_c	Complex. weight O_{w_c}	LMM 21 O_{w_l}
A	5	10	3	0.8	1 (low)	0.8	0
B	50	7	30	0.1	2 (medium)	0.3	1
C	10	10	15	1	1 (low)	1	0

6.1. *Individual requirements and risks*

The maturity model outlined in the previous section allows organizations to assess their logging and monitoring capabilities and - based on the selected maturity level - identify relevant assets and criteria to improve their security and advance to higher levels. While our referenced guidelines provide immediate advice on how to fulfill requirements of each level, they are usually tool-agnostic, i.e., it is necessary to manually identify and select cyber security solutions that are suitable to accomplish the needs. In the following we describe a model that enables security personnel to make informed decisions and identify fitting solutions as quick-wins following our workflow depicted in Fig. 1. We state and explain all variables used in the following sections in Table 3.

In the first step an organization needs to identify and assess some characteristics of their organizational structure, relevant assets to be protected against cyber threats, and their requirements on a security solution. In the following, we select three parameters for a security solution: (i) The desired price, (ii) the desired implementation and maintenance complexity, and (iii) the fulfillment of an exemplary criteria of the maturity model, in particular, LMM 21. For the purpose of our illustrative scenario we create three sample organizations with varying sizes and demands based on our organization profiles from Sect. 4.2. Organization A is a micro organization with a small budget and interest in finding an easy-to-deploy solution. Organization B is a medium-sized organization with little constraints regarding cost and complexity of solutions that wants to fulfill LMM 21. On the other hand, organization C has clear preferences regarding cost and complexity. Table 4 depicts all characteristics of the sample organizations, where weights are in the range $[0, 1]$.

For simplicity and based on our survey (see Sect. 4.2), we assume that each of our sample organizations utilize Office 365. In order to map relevant attack cases to assets of our organizations we first obtain a list of all known attack techniques on Office 365 from the MITRE ATT&CK Matrix[4] and subsequently weigh them using the method proposed in Kern et al. (2022) to take the likelihood of an attack being used into account. In brief, techniques receive a higher weight T_w when they are known to have been used by a higher number of discovered adversaries and when they are more often implemented by hacking tools or malware. In addition, we assign each technique a relevance score T_r based on manual assessments of (i) the impact of a successful execution of the respective technique, which is usually directly linked to the caused damage, and (ii) the required resources for carrying out such an attack. The columns of Table 5 also contain solutions, which we cover in the following section.

6.2. *Individual assessment of solutions*

Our survey in Sect. 4.2 shows that most organizations either employ commercial solutions from security vendors or open-source solutions that are openly accessible on the Internet. For our illustrative use-case, we select five commercial solutions: (i) *MDO* is a low-cost Microsoft product specifically designed to protect Office 365 against phishing, malware, spam, etc, (ii) *MEMS* is a Microsoft 365 product for endpoint management and protection, (iii) *ME* is a more advanced version of MEMS offering additional security applications, (iv) *AS* is yet another Microsoft product for Log Analytics, and (v) *ESS* is a cloud-based storage and analysis engine leveraging pre-defined rules for threat detection. We manually assess the properties of our selected solutions, in particular, regarding price (pricing information was taken directly from the website of the respective vendor), complexity of integration and maintenance categorized in three levels (low, medium, high), and their ability to fulfill LMM 21, where 1 indicates fulfillment, 0 indicates that the requirement is not fulfilled but still achievable, and $-\infty$ indicates that the solution prevents achievement of the requirement. Table 5 provides an overview of the solutions and the attributes required for matching them to the needs of organizations.

In addition to assessing properties of solutions, we need to determine whether a solution is able to detect a specific attack technique or not. We achieve this through a simple Internet search using the name of the security solution and the attack technique as keywords. Whenever we find a website (usually a page of the documentation of the security

[4] https://attack.mitre.org/.

Table 5
Exemplary selection of solutions.

ID	Solution	Pricing S_p	Complexity S_c	S_l
MDO	Microsoft Defender for Office 365 (Plan 1)	2.00$ per user/month	1 (low)	0
MEMS	Microsoft 365 Enterprise Mobility + Security E5	16.40$ per user/month	1 (low)	1
ME	Microsoft 365 E5	57.00$ per user/month	1 (low)	1
AS	Azure Sentinel	2.46$ per GB	1 (low)	1
ESS	Elastic Security Solution	109$ per month	3 (high)	1

Table 6
Attack techniques for Office 365 and assessment of detection capabilities.

ID	Technique	T_w	T_r	Solutions
T1518	Software Discovery	102	1	
T1566	Phishing	51	2	MDO
T1110	Brute Force	38	1	MEMS, ME, AS, ESS
T1078	Valid Accounts	38	2	AS, ESS
T1114	Email Collection	16	2	AS, ESS
T1087	Account Discovery	12	1	MEMS, ME
T1098	Account Manipulation	10	2	MEMS, ME, ESS
T1080	Taint Shared Content	10	2	ESS
T1137	Office Application Startup	9	0	
T1069	Permission Groups Discovery	9	1	MEMS, ME, ESS
T1539	Steal Web Session Cookie	9	2	
T1213	Data from Info. Repositories	8	2	AS
T1499	Endpoint Denial of Service	4	1	AS
T1564	Hide Artifacts	3	2	ESS
T1136	Create Account	2	2	AS, ESS
T1534	Internal Spearphishing	2	2	AS
T1498	Network Denial of Service	2	0	
T1550	Use Alternate Auth. Material	2	1	MEMS, ME, ESS
T1606	Forge Web Credentials	1	2	
T1562	Impair Defenses	1	2	ESS
T1528	Steal Appl. Access Token	1	2	
T1552	Unsecured Credentials	1	2	AS
T1538	Cloud Service Dashboard	0	2	
T1526	Cloud Service Discovery	0	1	

product) we note the solution in the respective attack technique row in Table 6. As visible in the table, some techniques are detected by multiple solutions (e.g., *T1110 Brute Force* is detected by four out of five solutions) while others are only covered by a single one (e.g., *T1566 Phishing*) or none (e.g., *T1498 Network Denial of Service*).

6.3. Decision model

The main idea of the decision model is to combine requirements derived from organizations (cf. Table 4) with properties of security solutions (cf. Table 5) and rank them by their abilities to detect relevant attack techniques (cf. Table 6) to identify the most suitable solutions for each organization. However, comprehensive protection often requires relying on more than one solution at the same time, in particular, when different solutions have disjoint sets of detected attack techniques, such as MDO and AS. On the other hand, some solutions may already cover most or all attack techniques detected by another solution, which means that deploying both of them simultaneously increases cost and maintenance effort while having only little benefit for threat detection. We therefore first identify reasonable combinations of solutions before assessing and ranking them. Notice that we omit detailed investigations on the quality of detection because this would require a demo-lab environment and benchmarking. This would clearly exceed the scope of this paper.

6.3.1. Solution combination identification

The main problem is that the number of combinations to consider increases exponentially with the number of solutions, in particular, it is a power set of size 2^n, where n is the number of solutions. We represent these cases in a decision tree so that the leaves of the tree comprise all possible combinations of solutions. Consider solutions $S1, S2, S3, S4$ which detect techniques $\mathcal{T}_{S1} = \{T1, T2\}$, $\mathcal{T}_{S2} = \{T1, T3\}$, $\mathcal{T}_{S3} = \{T2, T3\}$, $\mathcal{T}_{S4} = \{T1, T4\}$ respectively as an example. Fig. 4 shows a tree where each node shows the currently considered set of solutions (first line) and the techniques covered by their combination (second line), and each layer either adds (branches labeled “yes”) a specific solution to the set of solutions considered by the respective node, or leaves the set unchanged (branches labeled “no”). The complexity of the tree is reduced by pruning nodes that do not add any new techniques, e.g., the node on the left side of the figure representing combination $\{S1, S2\}$ does not branch into a node where $S3$ is added as $S3$ does not add any new techniques rendering all combinations containing $\{S1, S2, S3\}$ redundant. To further reduce the computational overhead of finding combinations, we leverage dynamic programming and memoization (Michie, 1968) by constructing the tree in a recursive manner and storing results for each node (i.e., combinations of solutions occurring in leaves of the sub-tree originating from that node) in a dictionary, where the set of covered techniques by that node is the key to that dictionary. Whenever the same set of techniques occurs for a node on the same level of the tree, it is then easy to obtain all combinations by replacing the solutions of the memoized node with the solutions of the new node and leaving the techniques unchanged. We indicate the influence of memoization with horizontal arrows, for example, the bottom left part of Fig. 4 shows that $\{S1, S2\}$ is replaced with $\{S1, S3\}$ in the memoized combinations $\{S1, S2, S4\}$ and $\{S1, S2\}$ to obtain the new results $\{S1, S3, S4\}$ and $\{S1, S3\}$ without the need to consider branching.

Note that this setup requires that techniques of solutions added on lower levels of the tree are not supersets of techniques covered by combinations in higher levels, because this would render solutions on higher levels redundant. This issue can be resolved by sorting solutions by the number of covered techniques, starting with the solution covering the most techniques in the top of the tree.

6.3.2. Solution combination ranking

Once the set of relevant combinations is known we aim to compute a quantitative score to enable ranking. For this we first assign numeric factors to combinations based on the properties of the individual solutions they consist of. This is simple for the price as all solutions need to be paid for, assuming that there are no combined offers available and that no solutions subsume each other. Accordingly we add up all prices of the individual solutions as shown in Eq. (1) to estimate the price of their combination. Note that we normalize S_p for each organization using the number of employees and estimated data usage per employee from Table 4.

$$C_p = \sum_{S \in C} S_p \tag{1}$$

The complexity of a combined solution is less trivial to determine, because it may take more effort to deploy and maintain multiple solutions with low or medium complexity in comparison to a single high-complexity solution. We address this issue by using the highest complexity of any solution involved in a combination as a base complexity and adding a term normalized to $[0, 1]$ that is higher for combinations comprising more solutions as depicted in Eq. (2).

$$C_c = \max_{S \in C} S_c + \frac{|C|}{|\{S1, \ldots, Sn\}|} \tag{2}$$

We compute a factor that is 0 when one of the solutions in a combination prevents fulfillment (i.e., $\{\exists S \in C : S_l = -\infty\}$) or none of them

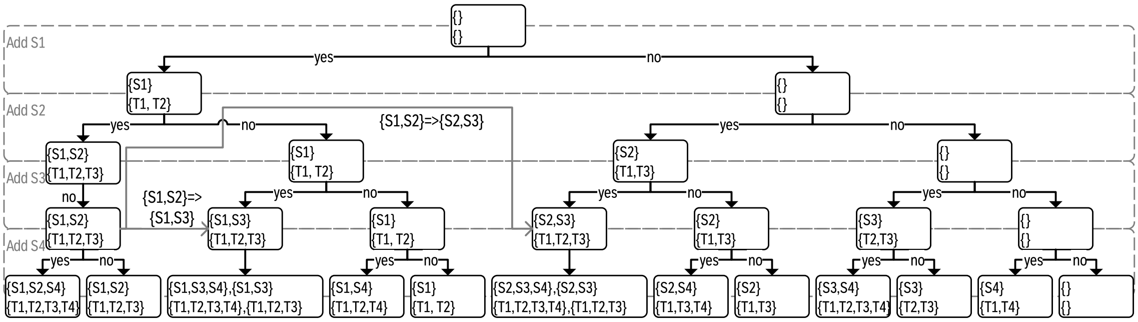


Fig. 4. Sample decision tree for identifying relevant combinations of solutions.

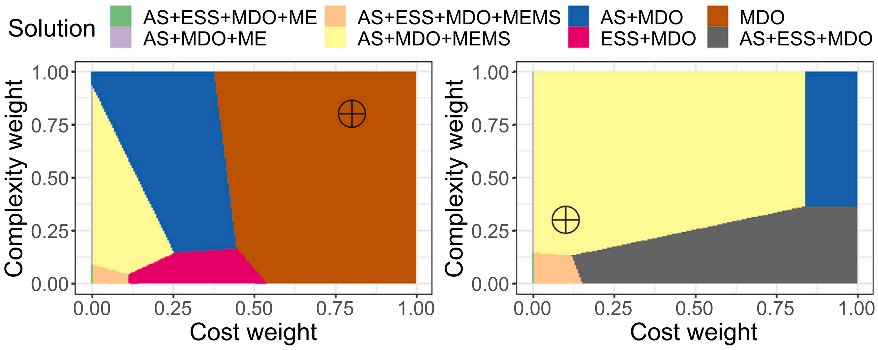


Fig. 5. Recommended solutions for organizations A (left) and B (right) when cost and complexity weights are varied.

fulfills the requirement (i.e., $\{\forall S \in C : S_l = 0\}$), and 1 otherwise. We state the corresponding equation in Eq. (3).

$$C_l = \max\left(0, \min\left(1, \sum_{S \in C} S_l\right)\right) \tag{3}$$

We further define a function to compare levels. In particular, solutions always yield best scores when their cost or complexity is lower than desired by the organization, and yield lower scores the farther away they are from the specified criteria. We state the function for a generic attribute i in Eq. (4).

$$a(O_i, C_i) = \begin{cases} 1 & \text{if } O_i \geq C_i, \\ \frac{O_i}{C_i} & \text{otherwise.} \end{cases} \tag{4}$$

To compute the overall score s of a combination we multiply all aforementioned factors with weights and relevance of detected techniques as stated in Eq. (5). In particular, the latter term is higher when more techniques with higher weights and relevance are detected by any of the involved solutions. Note that we scale factors for level fulfillment, price, and complexity by their respective weights as specified by the organizations. Thereby, a weight of 0 means that the respective factor does not affect the overall score and larger weights up to the maximum value of 1 increase the influence of the factor by reducing the overall score accordingly. Moreover, the term in the denominator normalizes the score to $[0, 1]$.

$$s_{O,C} = \frac{C_l^{O_{w_l}} \cdot a(O_p, C_p)^{O_{w_p}} \cdot a(O_c, C_c)^{O_{w_c}} \sum_{T \in \bigcup_{S \in C} \mathcal{T}_S} T_w \cdot T_r}{\sum_{T \in \bigcup_{S_1, \dots, S_n} \mathcal{T}_S} T_w \cdot T_r} \tag{5}$$

6.4. Evaluation results

We execute the selection procedure for each sample organization from Table 4. The source code can be found on Github.[5] First, we apply the decision tree model to identify 23 viable combinations of solutions that do not involve any redundant sets of solutions with respect to covered attack techniques as described in Sect. 6.3.1. Next, we assess and rank each of these combinations for each organization using the equations from Sect. 6.3.2. The top 3 recommended combinations and their scores for organization A are MDO (0.22), AS+MDO (0.09), and MDO+MEMS (0.08). This result is reasonable as organization A looks for cheap solutions with low complexities, which is best fulfilled by MDO. For organization B which accepts higher costs and complexities we obtain AS+MDO+MEMS (0.67), AS+MDO+ME (0.62), and AS+ESS+MDO (0.61). Clearly, MDO is part of every combination due to its ability to detect a high weighted technique paired with its low cost, and AS is a good candidate as it detects many other high weighted techniques but is less complex than ESS. The recommendations for organization C, AS+MDO (0.28), MDO+MEMS (0.26), and AS (0.23), confirm this trend.

Fig. 5 visualizes the influences of cost and complexity weights on the recommended combinations. In particular, areas with the same colors refer to the same combinations for organization A (left) and B (right). The crosshairs indicate the desired weights and correspond to the aforementioned top 3 solutions. This visualization allows to better understand how alternative combinations are affected by preferences, e.g., if organization B would put more weight on cost, then MEMS would be replaced by ESS in their optimal combination. We omit the plot for organization C for brevity; the visualization is similar to that

[5] https://github.com/d3tect/d3tect-solutions.

of organization A, except that the area of MDO is entirely covered by AS+MDO and ESS+MDO.

7. Discussion

The methodology presented in this work, along with the accompanying source code and datasets, provides a framework for organizations seeking to select cybersecurity solutions tailored to their specific needs and constraints. Despite its benefits, we recognize certain limitations when it comes to practically applying the model, ranging from the data-driven nature of the model to challenges in real-world implementation.

First, the effectiveness of the model is significantly influenced by the quality and precision of the underlying dataset used to evaluate security solutions. Ideally, the dataset would be generated through comprehensive validation of a security solution's detection capabilities, utilizing emulation of a realistic environment within a sandbox or testbed. Unfortunately, such a hands-on assessment procedure can be time-consuming, complex, and prone to errors. While it is possible to reduce the overall effort by relying on information about security solutions that is provided directly from their vendors (as we do for our study), such a strategy can be problematic due to the potential bias in marketing materials.

Another problem arises from the fact that identifying the ideal set of solutions with our proposed methodology involves a comprehensive examination of available detection solutions, which are often numerous, proprietary, and complex to test. As new security solutions appear over time, gathering and analyzing potential tools is not a one-time task but an ongoing process. Moreover, detection technologies continuously evolve, with some becoming better at detecting specific attacks or even implementations of attacks than others; pricing changes, but so do features, which may reduce complexity in implementation and operation. Even more challenging is the fact that attackers continuously adapt their methods, making it non-trivial for vendors to guarantee detection of all possible variations. These issues are not new, and the ongoing development of realistic and continuously updated adversary emulation platforms remains a problem for the cybersecurity industry that is not yet solved.

MITRE's ATT&CK Evaluations[6] offer a commercial framework for benchmarking different security solutions from various vendors against specific attack scenarios based on known threat actor procedures from past events. For this purpose, cyber security specialists need to re-implement attacks and then inject them into a test network, which is a tedious and costly task. Vendors then register their security solutions for certain scenarios to demonstrate their capabilities of detecting the attacks, serving as a significant selling point for expensive solutions. However, achieving true objectivity through these tests is challenging, because it is debatable whether the solutions have been pre-optimized for the test scenarios by the manufacturers who already knew about the attack techniques that they signed up for. Other possibilities for benchmarking such solutions in the real-world would be the operation of honey-pots and honey-networks. However, there is usually no way to obtain information on the types of adversaries and launched attacks, which prevents accurate benchmarking due to a lack of reliable ground truth.

Despite these challenges, our research offers significant contributions. To our knowledge, it provides the first methodology, source code, and structured dataset (based on MITRE ATT&CK and prior works Kern et al., 2022) aimed specifically at the detection domain while considering constraints like cost, complexity, and compliance with standards. The adaptability of the model, anchored in the regularly updated MITRE ATT&CK framework, ensures it can evolve alongside the threat landscape. This work significantly aids organizations, especially those with limited resources or expertise, in navigating the complex process of cybersecurity solution selection. We argue that even with an imperfect dataset, a set of software products aligned with organizational constraints and capable of detecting all MITRE ATT&CK defined techniques can significantly aid security specialists in selecting solutions for their companies.

The implementation of our methodology (Sect. 6) is based on the MITRE ATT&CK dataset, the most advanced and widely recognized best practice in the attack detection domain. Thus, it can be assumed that applying the methodology comprehensively achieves the best possible coverage. Extending the dataset to encompass all systems and solutions would be beyond the scope of this work, but is a critical area for future research. We provide the dataset generated from MITRE ATT&CK and the implementation of our methodology on GitHub,[7] serving as a foundation for further enhancements and addressing the lack of publicly available data sets that we encountered in our research.

8. Conclusion and future work

During our study we identified that many small companies are resistant to monitoring and logging cyber security investments. We proposed a methodology to pick appropriate cyber security solutions taking an organizations constraints regarding cost, complexity and compliance to standards and guidelines into account. Based on our study, we identified Office 365 as a common asset and applied our proposed methodology to three sample companies. We found out that a combination of three products (AS+MDO+MEMS) is the best solution combination when higher security investments are acceptable, while MDO as a standalone solution is the best solution for organizations with lower security investments.

Our method relies on a correct and complete assessment of security solutions which cannot be guaranteed in practice (yet). A method to reduce manual effort for assessing selected solutions is to automatically crawl and analyze publicly available repositories of open-source security solutions with natural language processing techniques. In particular, the descriptions and tags of repositories allow to cluster solutions by topics and extract keywords so that a large number of different solutions can be categorized and assessed in a more targeted manner. We omit this method as it would largely exceed the scope of this paper and leave an extensive evaluation for future work. It remains questionable whether the use of these techniques provides sufficiently good results for the selection of logging and monitoring solutions. Much better results could be achieved by creating a testbed over which detection solutions are uniformly benchmarked. These results could be fed back into our presented model to further increase the accuracy of detection.

Further enhancements could also incorporate other constraints, such as an organization's risk appetite, the cost of a successfully executed attack that remains undetected, or the specific impact on affected assets. Our model is not limited to current constraints, although if extended the complexity is increased, making it less likely to be applied by organizations.

CRediT authorship contribution statement

Manuel Kern: Visualization, Validation, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization, Writing – original draft, Writing – review & editing. **Max Landauer:** Methodology, Writing – review & editing. **Florian Skopik:** Writing – review & editing, Supervision. **Edgar Weippl:** Supervision.

[6] https://attackevals.mitre-engenuity.org/enterprise/.

[7] https://github.com/d3tect/d3tect-solutions.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Manuel Kern reports financial support, administrative support, and article publishing charges were provided by Austrian Research Promotion Agency. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

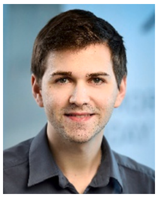
Acknowledgements

This work was partly founded by the Austrian Research Promotion Agency (FFG) project SPOTTED: FO999887725 (4148328) and KIRAS project CyberMonoLog: FO999886330.

References

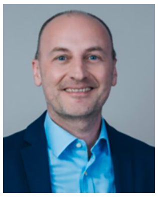
Antunes, M., Maximiano, M., Gomes, R., Pinto, D., 2021. Information security and cybersecurity management: a case study with smes in Portugal. J. Cybersecur. Privacy 1 (2), 219–238.
Bromberger, S., Maraschino, C., 2012. Security Logging in the Utility Sector: Roadmap to Improved Maturity. National Electric Sector Cybersecurity Organization. http://www.nerc.com/files/CIP-007-1.pdf.
Bundesamt für Sicherheit in der Informationstechnik, 2022. It-grundschutz-kompendium edition 2022. http://dnb.d-nb.de.
Carnegie Mellon University, The Johns Hopkins University, 2021. Cybersecurity Maturity Model Certification - Model Overview | version 2.0.
Center for Internet Security, 2021. Cis controls version 8. www.cisecurity.org/controls/.
Dube, D.P., Mohanty, R., 2020. Towards development of a cyber security capability maturity model. Int. J. Bus. Inf. Syst. 34 (1), 104–127.
Executive Office Of The President, 2021. Improving the federal government's investigative and remediation capabilities related to cybersecurity incidents. https://www.federalregister.gov/d/2021-10460.
Int. Org. for Standardization, 2013. ISO/IEC 27001:2013 Information Technology — Security Techniques — Information Security Management Systems — Requirements, 3rd edition. ISO/IEC.
Int. Org. for Standardization, 2022. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Controls, 3rd edition. ISO/IEC.
IRBM Corp., 2022. Cost of a data breach report 2022. report.
Kabanda, S., Tanner, M., Kent, C., 2018. Exploring sme cybersecurity practices in developing countries. J. Organ. Comput. Electron. Commer. 28 (3), 269–282.
Kent, K., Souppaya, M., 2006. Special Publication 800-92 Guide to Computer Security log Management Recommendations.
Kern, M., Skopik, F., Landauer, M., Weippl, E., 2022. Strategic selection of data sources for cyber attack detection in enterprise networks: a survey and approach. In: Proceedings of the 37th ACM/SIGAPP SAC, pp. 1656–1665.
Kim, S., Pérez-Castillo, R., Caballero, I., Lee, D., 2022. Organizational process maturity model for iot data quality management. J. Ind. Inf. Integr. 26, 100256.
Llansó, T., McNeil, M., Noteboom, C. Multi-criteria selection of capability-based cybersecurity solutions. In: Bui, T. (Ed.), 52nd Hawaii International Conference on System Sciences, HICSS 2019, Grand Wailea, Maui, Hawaii, USA, January 8-11, 2019. ScholarSpace, pp. 1–9. https://hdl.handle.net/10125/60169.
LLC PCI Security Standards Council, 2022. Pci-dss: Requirements and Testing Procedures, v4.0.
Michie, D., 1968. "memo" functions and machine learning. Nature 218 (5136), 19–22.
Ministry of Justice, 2022. Cyber Security Guidance Technical User Edition.
NIST, 2020a. Nist special publication 800-53 revision 5 security and privacy controls for information systems and organizations. https://doi.org/10.6028/NIST.SP.800-53r5.
NIST, 2020b. Nist special publication 800-53b control baselines for information systems and organizations joint task force. https://doi.org/10.6028/NIST.SP.800-53B.
OWASP, 2021. Application Security Verification Standard 4.0.3 Final.
PCI Security Standards Council, 2016. Information Supplement: Effective Daily Log Monitoring.
Ponsard, C., Grandclaudon, J., 2018. Survey and guidelines for the design and deployment of a cyber security label for smes. In: Int. Conf. on Information Systems Security and Privacy. Springer, pp. 240–260.
Rawindaran, N., Jayal, A., Prakash, E., Hewage, C., 2021. Cost benefits of using machine learning features in nids for cyber security in uk small medium enterprises (sme). Future Internet 13 (8).
Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., Guissanie, G., 2021a. Protecting controlled unclassified information in nonfederal systems and organizations. J. Res. Natl. Inst. Stand. Technol. 1. https://doi.org/10.6028/NIST.SP.800-171R2. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.
Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R., Bodeau, D., 2021b. Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to Nist Special Publication 800-171. National Institute of Standards and Technology.
Scarfone, K., Mell, P., 2012. Draft sp 800-94 rev. 1, Guide to Intrusion Detection and Prevention Systems (idps).
Skopik, F., Landauer, M., Wurzenberger, M., 2022. Blind spots of security monitoring in enterprise infrastructures: a survey. IEEE Secur. Priv. 01, 2–10.
UK Gov., 2018. Minimum Cyber Security Standard.

Manuel Kern is head of the penetration testing focus at the Austrian Institute of Technology (AIT). His research interests lie in the area of attack and defense of information systems. He holds a Master of Science in Information Management & Computer Security, as well as numerous industry-relevant IT security certifications. He has more than 15 years of experience in IT and IT security driven projects as well as positions as Senior Consultant, Head of IT and Chief Technology Officer. Furthermore, he is an ISO27001 Lead Auditor and an appointed auditor for operators of essential services (NISG §17(3)).



Dr. Max Landauer joined the Austrian Institute of Technology in 2017 and is currently employed as a Scientist in the Cyber Security Research Group. His main research interests are anomaly detection, cyber threat intelligence, log data analysis, and cyber security testbeds. Max obtained his master's degree in Computer Science in 2018 and finished his PhD studies in 2022 at the Vienna University of Technology.

Dr. Dr. Florian Skopik is Head of the Cyber Security Research Program at the Austrian Institute of Technology (AIT) with a team comprising around 30 people. He spent 10+ years in cyber security research, before, and partly in parallel, another 15 years in software development. Nowadays, he coordinates national and large-scale international research projects, as well as the overall research direction of the team. His main interests are centered on critical infrastructure protection, smart grid security, and national cyber security and defense.



Edgar Weippl is research director of SBA Research and full professor at the University of Vienna. Edgar's research focuses on fundamental and applied research on blockchain and distributed ledger technologies and security of production systems engineering. Edgar (CISSP, CISA, CISM, CRISC, CSSLP, CMC) is member of the editorial board of Computers & Security (COSE) and associate editor of IEE Transactions on Information Forensics and Security (IEEE TIFS). He is Austria's representative at IFIP TC 11: Security and Privacy Protection in Information Processing Systems. Edgar is steering committee chair person and involved in the organization of the ARES conference. He was General Chair of SACMAT 2015, PC Chair of Esorics 2015, General Chair of ACM CCS 2016, PC Chair of ACM SACMAT 2017, General Chair Euro S&P 2021 and 2024.