EOSC Future

D7.5b

Augmented Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution

The EOSC Future project is co-funded by the European Union Horizon Programme call INFRAEOSC-03-2020, Grant Agreement number 101017536

Version 1.0
July 2023

D7.5b / Augmented Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution

Lead by **Nikhef (NWO-I) by way of EGI.eu**

Authored by David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Pau Cautrina (CERN), Sven Gabriel (Nikhef NWO-I), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich)

Reviewed by Paul Gondim van Dongen (SURF) and Athanasia Spiliotopoulou (JNP)

Dissemination Level of the Document

Public

Abstract

The continued evolution and development of trust, operational security policy and incident response of the EOSC-Core and EOSC-Exchange services are discussed compared to the baseline established in D7.5a [1], and how their constituent elements – information security management, baseline security policies and guidelines, risk assessment models, and incident response and resolution – have been defined. The information security model for the EOSC is based around subsidiarity of security maturity, monitoring, and incident response, but with a core incident response coordination team, which provides actionable support for the core services. The same team ensures a coordinated response for incidents in composed and distributed EOSC services and is linked to the global academic and research security community.

The evolution of operational security during the EOSC Future project is laid out by identifying the three primary challenges: increasing awareness and maturity of security posture within the providers connecting to the EOSC, specific topic guidance for critical elements for composite services (including attribute authority and AAI proxy operations) and supporting IT risk self-assessment and definition of controls by means of risk-management tooling.

The EOSC Security Incident Coordination, also supporting the incident response for the EOSC-Core services, remains a central part of the operational security activities.

Version History

Version	Date	Authors/Contributors	Description
V0.1	24/05/2023	David L. Groep (Nikhef NWO-I)	Structure and foundational text
V0.9	11/07/2023	David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Pau Cautrina (CERN), Sven Gabriel (Nikhef NWO-I), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich)	Completion of content and internal editorial review and writeup of sensitive content sections. Review of potential confidential data exposure.
V1.0	18/07/2023	David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Pau Cautrina (CERN), Sven Gabriel (Nikhef NWO-I), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich), Ron Dekker (TGB), Mike Chatzopoulos (ATHENA)	Final version submitted to EC

Copyright Notice

Table of Contents

Table of Figures

Glossary

EOSC Future project Glossary is incorporated by reference: https://wiki.eoscfuture.eu/x/JQCK

List of Abbreviations

Acronym	Definition
AAI	Authentication and Authorisation Infrastructure
AARC	Authentication and Authorisation for Research Collaboration
AAOPS	Attribute Authority Operations (AARC security guideline)
AUP	Acceptable Use Policy
CSIRT	Computer Security Incident Response Team (also known as a 'CERT', i.e., a Computer Emergency Response Team)
DoS/DDoS	Denial of Service / Distributed Denial of Service
eduGAIN	EDUcation Global Authentication INfrastructure (R&E interfederation service)
IAM	(Indigo) Identity and Access Management, AAI software product
IdP	Identity Provider (source of authentication and attributes in an AAI interaction)
I/F	EOSC Interoperability Framework
IoC	Indicator of Compromise
ISM	Information Security Management
MISP	Malware Information Sharing Platform
PDK	Policy Development Kit
R&E	Research and Education
RAW-WG	Risk Assessment WISE Working Group (see also: WISE)
SCI	Security for Collaborating Infrastructures (WISE working group)
Security Baseline	Set of minimum security controls defined for an information system that has been established through information security strategic planning activities (herein also 'baseline', see e.g. https://csrc.nist.gov/glossary)
SMS	Service Management System
SPM	Service Portfolio Management
WLCG	Worldwide LHC Computing Grid (research infrastructure)
WISE	WISE Information Security for E-infrastructures community

1 Executive Summary

The operational security of the EOSC ecosystem and the information security management process of its core services are centred on a risk-assessment methodology and an incremental mechanism of defining a baseline: the initially established set of minimum security controls. These can be either mandatory for EOSC-Core services, or as community good practice guidelines for the services listed in the EOSC-Exchange, complemented by an incident response and coordination scheme composed of operational security and forensics analysis experts.

Based on the work previously reported in the initial 'Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution' (D7.5a), we explore the implementation of the mechanisms proposed therein, how the EOSC Service Management System has evolved to address the operational requirements for the EOSC-Core, and how the security operational guidance may be applied to the services in the EOSC-Exchange for thematic, regional, and horizontal services.

We specifically review the implementation of guidance for secure operation of the (community) attribute source services that underpin the EOSC authentication and authorization infrastructure, the risk assessment framework and how this has been applied to three EOSC reference Core services (Portal, Core AAI, and the Observatory), the adoption of the Security Operational Baseline as part of the Interoperability Framework, and the incident response posture and experiences.

2 Introduction

The trope 'security is only as strong as its weakest link' has been so frequently repeated that its urgency and relevance is nowadays often lost. Yet for the EOSC, with its aims to link together research portals, resources and services in a web of data and services, security and trust does not stop at the boundary of services, but necessarily extends between the services in the EOSC-Core, and between EOSC-Core and EOSC-Exchange, as well as involving research community services from which the trust in users ultimately flows.

In the baseline discussion on security evaluation (D7.5a, 'Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution' [1]) we described the trust and security landscape and identified the Hippocratic principle[1] of '*primum non nocere*' as the basis for the EOSC security operational methodology, differentiating between 'Core' services and 'Exchange' services.

In this supplementary review of the security posture of EOSC and EOSC Future, we address the Information Security Management elements of the EOSC Service Management System (SMS), the evolution of the items identified in D7.5a (specifically section 7 therein) and provide recommendations for their evolution beyond the termination of the current EOSC Future project.

3 Information Security Management in the EOSC SMS

The EOSC operational security model is anchored in the EOSC Service Management System (SMS) through the Information Security Management (ISM) system for the EOSC-Core Services. This targets the management of information security effectively through a series of activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant information assets are preserved. The ISM activities are based on the EOSC service portfolio abstraction of 'assets', and we consider the 'service' to be the smallest constituent element of the information security processes. Hence, the service provider is the entity that has primary responsibility for the protection of these assets.

The identification of assets is based on the EOSC-Core Service portfolio, and the ISM.2 'Information assets and threats' procedure leverages the SPM process to identify assets and collect the basic security contact information. The set of assets drives both the scope of the operational incident response (intervention-oriented for the services in the Core services in the service portfolio; coordinating for incidents that only involve Exchange services and collaborating partners, as described in the ISM.1 procedure), and the risk assessment process (where validation of the provider-supplied risk assessments in accordance with the ISM.3 'Security Risk Management' procedure is performed for core services).

The Information Security Management system[2] also provides procedures that Core service providers should follow to mitigate identified risks that their service exposes to other services in either Core or Exchange. In order to support providers in the assessment of the appropriate controls, the ISM system has supplementary information that provides general guidance and good practice recommendations (in https://wiki.eoscfuture.eu/display/EOSCSMS/ISM+Security+Controls+and+Risk, accessible to the SMS audience only). Although not itself part of the SMS, this guidance supports the providers to collaborate with the EOSC Security team in defining the controls as part of the ISM.4 Control procedure.

The five procedures in the ISM system support the EOSC Security Operational Baseline (discussed in more detail below), which is itself part of the ISM system as an ISM Policy. The joint 'Acceptable Use Policy and Terms and Conditions' framework for the EOSC-Core completes the ISM policy set. This framework is based on the WISE Security for Collaboration among Infrastructures (WISE SCI) work to which EOSC Future has been a contributor, and this augmentable WISE Baseline AUP framework both reduces the number of 'click-through' pages to which

[1] For background, see e.g. https://en.wikipedia.org/wiki/Primum_non_nocere

[2] The Information Security Management 'system' term as used here comprises all elements of ISM that are part of the SMS, including policies, procedures that implement processes, guidelines, and relevant indicators.

an end-user is exposed, and provides confidence for underpinning services that the user has seen both the appropriate AUP as well as any relevant privacy notices (a reference to which is part of the AUP template).

The Information Security Management system has been audited in December 2022 and June 2023. No deficiencies were found in either audit. The suggestions and hints provided in the December 2022 review of the ISM system have been incorporated in their entirety in the EOSC ISM system, and the June 2023 audit identified no issues in the EOSC ISM system.

4 Evolving the information security for EOSC

The EOSC ecosystem as a whole and the security activities evolve in tandem, and the updates to the EOSC Interoperability Framework, Rules of Participation, and the implementation of the EOSC-Core affects the way trust and operational security fits into that framework. At the same time, clearer security requirements (and the increasingly recognised need to secure critical infrastructure in society in general) also influence interoperability and co-determine the conditions under which service providers can connect to the EOSC.

4.1 Policy recommendations: WISE recommendations and the Attribute Authority Secure Operations Guidelines

The security and trust fabric of the EOSC is part of a global ecosystem of information security for e-infrastructures. This community includes participants not only from the EOSC Future project or the Core services, but also many of the horizontal infrastructure providers, ICT-intensive research infrastructures, multiple European member states, and partners such as Access-CI, Open Science Grid, and the Trusted CI collaboration (based in the US), as well as global collaborations. The WISE (WISE Information Security for e-infrastructures) community furthers these collaborations and stimulates alignment of ISM processes for the research infrastructures that – by their very nature – span multiple spheres of governance. The WISE Baseline Acceptable Use Policy and its use by very diverse services (in the EOSC-Core, but also many of the Exchange services, national services, and research infrastructures) is a result of this global collaboration. Highlighting the value of the WISE Baseline AUP, also through the EOSC Service Management System as ISM Policy ISM.1, has increased adoption. The AUP thus reduces the number of 'click-through' pages experienced by users.

As the role of 'proxies' in the EOSC community AAIs increases in prominence, becoming more important as the source of almost all attributes that are used for making authorization decisions, their integrity and availability is now a critical element for the EOSC services. The importance of these AARC Blueprint Architecture proxies is now likely comparable to those of the AAI federations of identity providers - since they have a domain-wide scope across many countries and regions, and their integrity and role in incident response is crucial. The AARC-G071 guideline on 'Secure Operation of Attribute Authorities and other issuers of access statements' (AAOPS Guideline) has been completed in 2022 (https://aarc-community.org/guidelines/aarc-g071/), but its validation in real-world scenarios was still to be completed.

In order to validate the AAOPS Guideline comprehensively, we identified the three distinct types of AAI Proxies that are expected to be prevalent in the EOSC ecosystem, and selected one example from each type. These are the Core AAI infrastructure proxy (a necessary EOSC-Core element), one proxy at the national level (in this case the UKRI IRIS IAM proxy), and one research infrastructure 'community' proxy (the selected one being the WLCG RI proxy). These three proxies used two different technology stacks (eduTEAMS and IAM), and were operated by three different organisations. The validation mechanism used was one that is common in the federated R&E trust and identity ecosystem, based on peer-reviewed self-assessment using a transparent disclosure process. All infrastructures used a common assessment sheet (which provides a breakdown of the G071 guidance alongside fulfilment hints) that is available from https://edu.nl/88dwf.

While infrastructure-specific results are not presented here (since they are open to the peer reviewers and peer infrastructures, yet not entirely public), the process itself included plenary discussion sessions where all AA operators were present. This resulted in completed assessment for the selected infrastructures, as well as suggestions for improvement for the AAOPS guideline itself (available in the public assessment sheet referred to above). The AAOPS Guideline evolution will continue in the AARC policy community, so that other operators

of attribute authorities and proxies in the EOSC and its (national) infrastructure equivalents may benefit from the results obtained here.

4.2 Implementing risk assessment for EOSC-Core and Exchange services

Risk management should be the starting point in proactive security for protecting the assets by identifying and mitigating cyber and other risks. The subtask for risk management has a long background in the WISE risk management working group and in their respective organisations.

The risk management subtask for the current period had the objective to implement and facilitate risk assessments for the mission critical EOSC-Core and exchange services. Instead of traditional and tedious methods by using a large risk assessment template as the starting point, the risk assessment was now implemented by a modern and agile enterprise risk management platform called *Inclus*, originating from complex and sensitive peace mediation processes conducted by Nobel Peace Prize laureate and President Martti Ahtisaari's Crisis Management Initiative (CMI) [3]. Licences to utilise the platform were kindly provided by CSC - IT Center for Science Ltd.

The risk assessments were prepared by and based on previous assessments and work done in the WISE Risk management working group, a tailored risk register, which the respondents could assess, score and also add additional risks. The respondents received personal links to submit their contributions to the assessment.

Virtual risk assessment sessions were arranged by utilising the Inclus platform for the EOSC Catalogue & Marketplace team, for the EOSC-Core Infrastructure Proxy team and for the EOSC Support SP: EOSC Observatory. To compare the results with a control group a similar risk assessment session was arranged for the Information security manager of Finnish higher education information security managers.

The following diagram summarises the consensus results and the distribution of the results.

Figure 4.1: Results of risk assessments, Table A

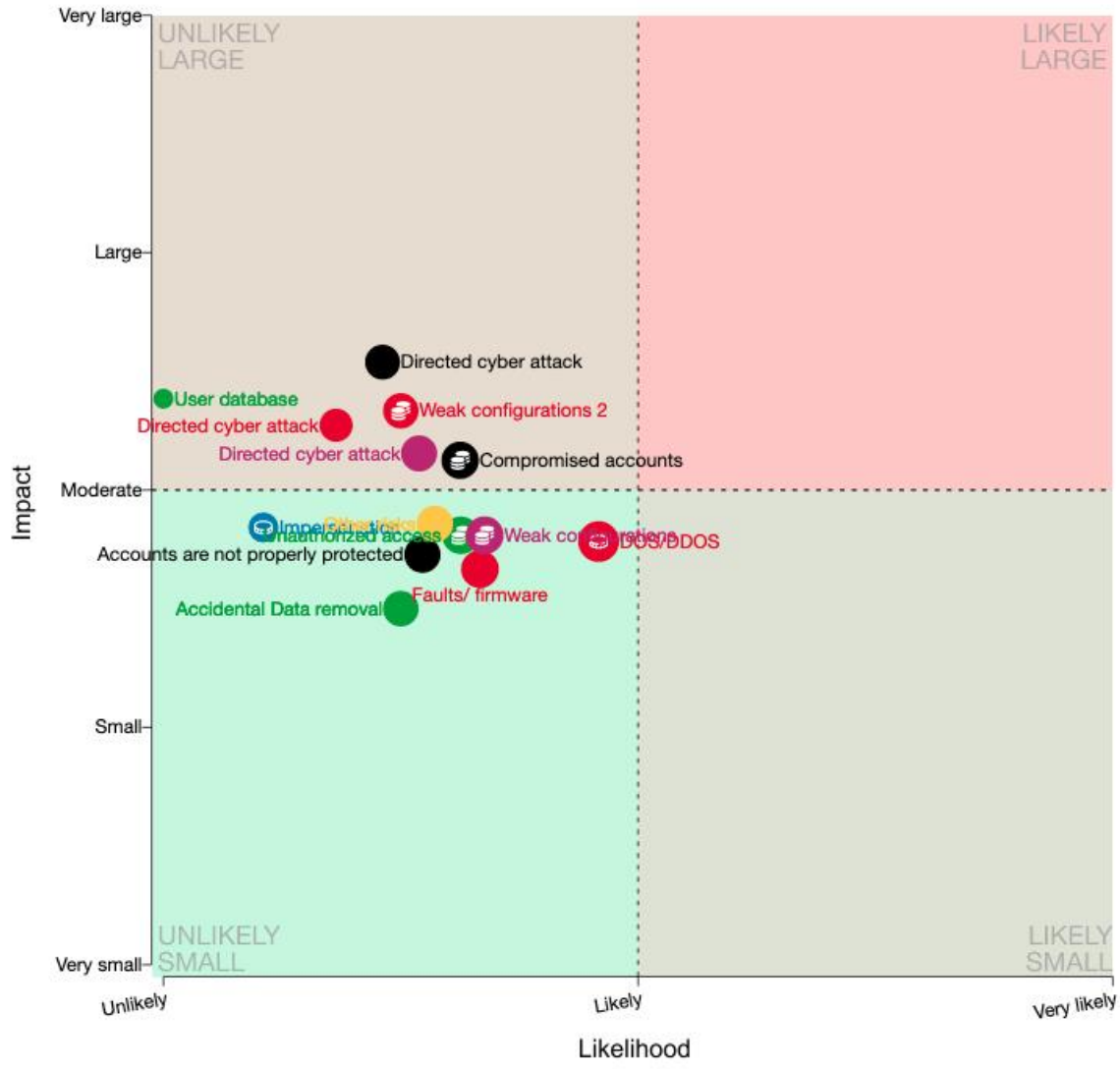

Figure 4.2: Results of risk assessments for all surveyed services

The results show that both the impacts and likelihoods of the risks identified in the risk register were identified to have a moderate impact and be somewhat or moderately likely to happen. Individual assessment showed great variations.

Directed cyber-attack received not surprisingly the highest score, due to the current global polarisation and increased information warfare activity. The well-known standing risks related to compromised accounts and DoS/DDoS attacks were also well identified. Ensuring fundamental best information security practices is a prerequisite to mitigate all identified risks but coping with advanced cyber-attacks can require additional investments in situational awareness and developing CSIRT and SOC (Security Operations Center) activities.

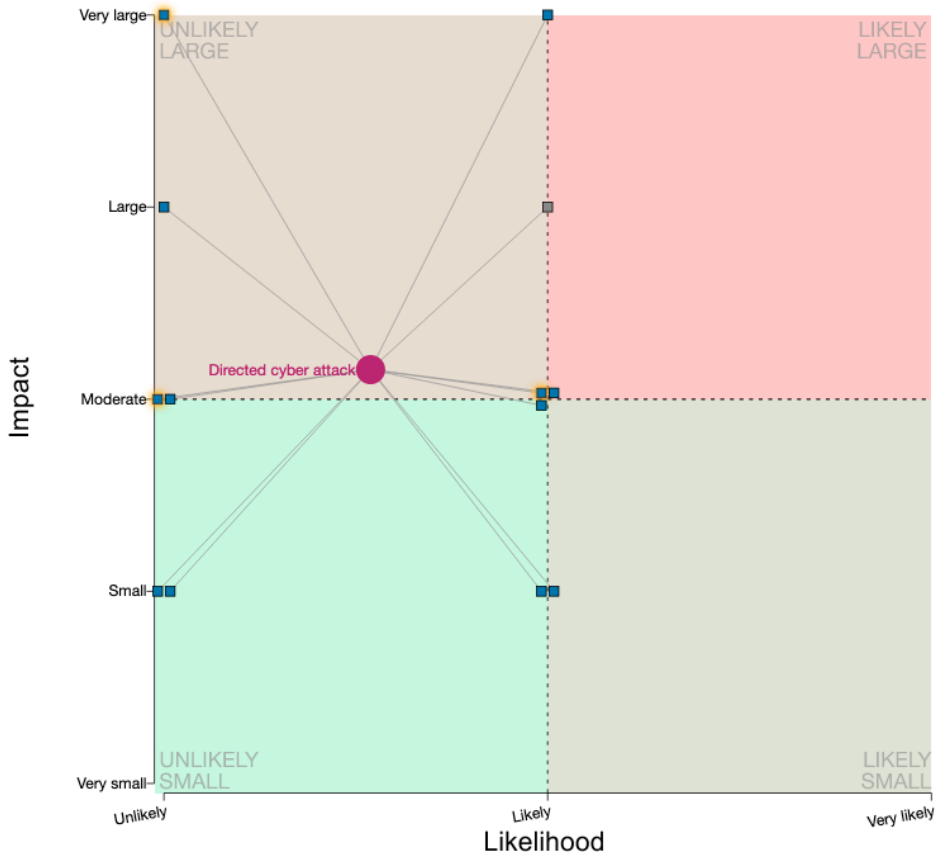

Figure 4.3: Directed cyberattacks are identified as having the highest risk score in the survey. The figure indicates how the individual responses (for all participating service providers) contribute to the impact-likelihood figure and (in this specific case for example) how the impact of directed cyberattacks is identified

4.3 Communications challenges and mock incident response

'Nothing but the Real Thing'. Incident response processes for EOSC have been based on good practices from the Research & Education ecosystems. Despite being based on proven good practices the processes still need to be implemented in a new team and everyone needs to agree on roles, responsibilities, definitions and (interpretation of) procedures. In order to test the initial process implementation several exercises have been set up, exercises that can and will be repeated on a regular basis in order to identify in an early stage any miscommunication within and between teams and any omissions. The exercises that have been run fall into two categories: validation of the internal incident response process, and testing the response capabilities of system owners.

4.3.1 Validation of the incident response process

In the reporting period, 2 tabletop exercises have been held with the core incident response team. The main purpose of these exercises was to verify completeness of the incident response procedures. The exercises have resulted in minor modifications to the procedures (Procedure ISM.1) and the exercises emphasised the need for maintaining an accurate and complete directory of security contacts. In this tabletop exercise, we verified the completeness of all steps in the ISM.1 incident response procedure, to ensure all affected parties are involved and are provided with the correct information. We also verified the assignment of responsibilities between the Incident Response Coordinator, the service provider, and the incident reporter. Mock incidents were used to verify the procedure for completeness.

To assess the capabilities in containment and forensics, more complex scenarios need to be developed which can be done either using the 'tabletop' approach to exercises, or even more advanced in a red-blue team approach. However, the feasibility of the larger-scale exercises including red-blue teaming and full crisis exercises (with even more parties) depends critically on the resources available - and at this time are beyond the

scope of the EOSC SMS or the EOSC Future project. Participation of EOSC services and service providers in existing cyber-crisis exercises (e.g. as organised in the research and academic security community) may be both more cost effective and useful, given the broader interdependency of services in the research and education ecosystem also outside of the EOSC.

4.3.2 Communications challenges and service provider interaction

The EOSC-Core Provider Agreement and the Interoperability Framework set a minimum security operational baseline (described in more detail below) that provides the basis for incident response and operational security. In particular, it engaged the service providers to 'participate in drills or simulation exercises to test Infrastructure resilience as a whole'. Given this minimum security baseline, the technical ingredients for Incident Response (IR) need to be put in place. These can be categorised as communications, containment and forensics.

Coordination of the security activities, in particular in distributed environments, starts with *communications* between the coordinating team and the security contacts of the affected participating resources. The standard communication tool is e-mail. To efficiently organise these communications a maintained directory of security contacts is needed. To structure the security related communications a ticket system is used which respects the requirements on confidentiality and integrity.

Once the communication channels between the relevant parties are established, the coordination of the incident response activities, like forensics support to resolve an incident, can take place. Inter-service *containment* is based on timely exchange of indicators of compromise (IoCs) that are shared both by email (as above), and - where the target service has been appropriately connected - through automated intelligence sharing platforms such as MISP (the Malware Information Sharing Platform). However, given the diverse operational environment of the EOSC-Core service providers, email remains the primary means of sharing information for containment. The procedures rely on the individual service providers to perform intra-service containment of incidents.

During the incident response process, collecting *forensics* is critical to prevent the same actor from repeatedly compromising the system and to identify any (software) vulnerabilities that were abused during the incident. For the EOSC-Core services, the EOSC Security Coordinator provides forensics expertise as needed to the affected providers. By providing security *forensics training*, the expertise level within the service providers can also increase (this activity is undertaken by the same forensics experts through other means within the EOSC Future project).

The above described basic capabilities are frequently tested in communication challenges. Here we use a framework which records the response times of the challenged parties. The communications challenges are run twice-yearly and target the Core service providers. As part of their agreement, they register a security contact in their service portfolio entry, and the security communications challenge re-uses those entries to target the Core services. Service providers may receive multiple challenges, one for each of their registered Core services. By mid-2023, 21 Core services were classified as 'production' services in the service catalogue, and these contacts (converted from SMS name handles to email addresses where necessary) were used to reach out to the service security contacts.

In the challenge, we consider a response within one business day to constitute 'in a timely fashion' as expected by the Security Operational Baseline - which corresponds to, or is longer than, the maximum response delay allowed for high-priority incidents for all recognised service levels in the Core Provider Agreement. In an incident response situation, a response time of 4 office hours is required to efficiently coordinate the security activities in the distributed infrastructure - this corresponds to the maximum response delay for Advanced services in the Core Provider Agreement.

In the challenge run in August 2022, close to 50% of the service providers responded 'in time' to the communications challenge. The main barriers to response identified were lack of role-based contact details (messages going to individuals, who may be on leave), and (one) outdated security contact details in the (then-sheet-based) Core service provider catalogue.

The current results of the communications challenge form a baseline; here we had 35 security contacts participating, the shortest response time was 2 minutes, the longest 19h 40min. 17 service components (some of them under the same security contact) did not reply at all. Only a single run (i.e., without any reminder) was sent. The baseline is constant, however, with a much enlarged service catalogue. This points to the need for more frequent challenges, and better training for onboarded service providers.

4.4 Baseline implementation mechanisms

Based on the federated and distributed nature of the EOSC services, the responsibility for their compliant operation and service management has been devolved to the service owners. With regard to the security aspect of the services, this implies we consider the 'service as a whole' to be the asset in the EOSC security model. This applies to both Core services as well as those services and assets in the Exchange, although the level of involvement with each of them is slightly different (as described previously, e.g. in D7.5a, the level of control is much higher with respect to Core services where forensics, intervention, and monitoring is concerned). To ensure all parties in the EOSC ecosystem collaborate in security operations and collectively address their risks and challenges, we established a Security Operational Baseline that sets minimum requirements on the security posture of the services and their providers. Derived from the AARC Policy Development Kit and incorporating elements from various national frameworks based thereon (such as the UKRI 'IRIS' infrastructure), it aims to be a compact and simple representation ('just' 12 points) of the mutual security expectations that services in the EOSC can rely on.

Initially, the scope of the EOSC Security Operational Baseline (the 'Baseline') was set as mandatory for Core services, and strongly recommended for the Exchange services to which it is applicable (it is geared towards services rather than data sets or publications). As such, the Baseline was introduced as a mandatory part of the Core Participation Agreement, and made a prerequisite for joining the EOSC AAI Federation.

With the more prominent positioning of the EOSC Interoperability Framework (I/F), we have worked with the relevant I/F boards to bring the Baseline into the Interoperability Framework as a guideline, with the lead partner for the work here identified as the 'provider' thereof. This has resulted in the Security Operational Baseline (2022 edition) to be incorporated as the first operating guideline in the framework in June 2023 (as https://search.marketplace.eosc-portal.eu/guidelines/eosc.df8f717f77566b7adde87ede8f55b31d):

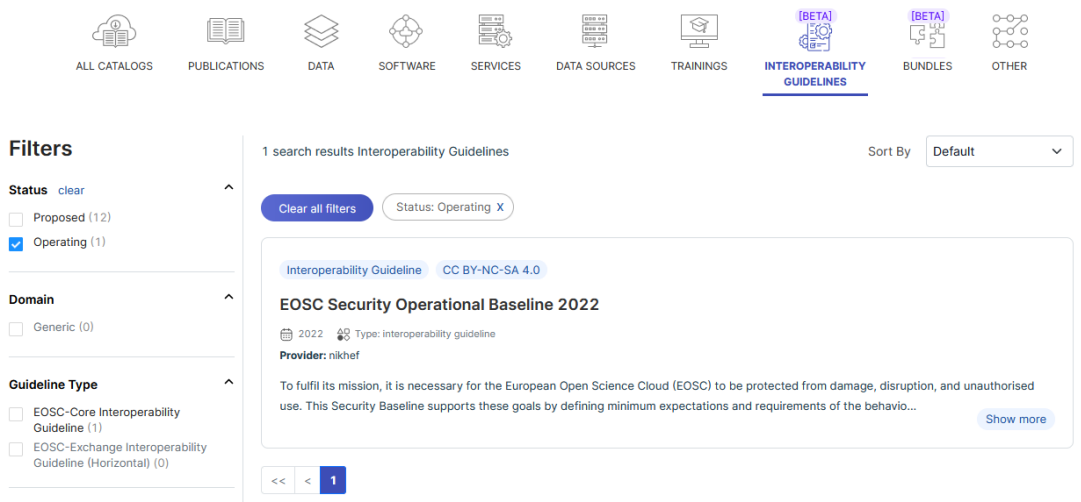

Figure 4.4: The EOSC Security Operational Baseline as seen in the EOSC Portal under Interoperability Guidelines (visited June 28th, 2023).

With the inclusion of the Baseline in the I/F, its visibility is increased beyond what it would have had through only the EOSC AAI Federation component (through the cross-work-package working group on AAI).

Adoption of the Baseline brings concrete value to the overall security coordination in the EOSC, since it allows EOSC-wide security drills and map-table exercises that improve the response posture in case of real incidents. It also facilitates sharing of 'threat intelligence' during actual response, as it mandates collaboration with the

EOSC-Core Security Incident Coordinator and the Information Security Management processes (in particular procedure ISM.1 on incident response).

4.5 Incident mitigation and resolution

The capabilities to handle security incidents are provided by the EOSC Security Team that was established during the first phase of the project. The main constituency of the team is the EOSC-Core services for which the team is the primary coordinator of operational security aspects related to them. For the rest of the EOSC ecosystem the team provides the point of contact and coordination, and can offer additional services if they are required and resources are available in the team.

Following its establishment, the team continued to work on operational security aspects. A regular shift rota schema was kept, and internal procedures to handle issues were reviewed and updated several times to address issues that were tackled. The need for a clear procedure and internal steps was emphasised by the personal changes in the task leadership in autumn of 2022, which posed another opportunity to review and improve internal documentation for incident response.

The EOSC security team is primarily designed as a coordinating body that communicates with many parties involved in a security incident. As such, the team is heavily dependent on functional communication flows and channels, and timely and comprehensive sharing of information is important to prevent spreading of ongoing incidents. This requires that a view of actions taken during an investigation can be established, and that such a report provides a full audit record and thus helps identify weaknesses and lessons for improvements. Another important requirement is the security of information exchanged during the investigation, especially maintaining the proper level of confidentiality.

Over the reported period technical tools and organisational measures were evaluated to achieve communication means that cover the needs of the security team. A list of requirements on ticketing systems was produced and thoroughly discussed with the EOSC-Core help desk representatives. Also, after a downtime of the EOSC Confluence Wiki (due to patching for a critical vulnerability) it was decided to keep a copy of crucial materials outside the Wiki space to make sure the main response capabilities are not hindered by an outage of the primary document storage. The communication platform used internally by the team (Keybase) was used to keep the secondary copies of the materials.

In addition to developing and strengthening the internal response capabilities, the team focused on maintaining the communication channels towards the constituency. As a joint effort with the other tasks, a list of security contacts was established and reviewed several times. The current version is maintained at a central place, as part of the EOSC-Core Service Portfolio, providing the security teams with a view at relevant information.

The EOSC Security Coordination team had to handle two EOSC-specific incidents in the first half of 2023 (the team was involved with and notified of other incidents as a collateral party, which will not be discussed here). The EOSC Security Coordinator also gets notified of security events and vulnerabilities in core services. We distinguish between 'security events' (indicating a *possible* breach of information security) and 'security incidents' (*security events* with a significant probability of having a negative impact on the delivery of *services* and business operations).

Security incidents require immediate and comprehensive investigation and mitigation. Usually, these incidents also spread both laterally within the service and between services where accounts are shared. Acting in a federated context, we also observe incidents where a single (compromised or abused) credential from one identity-providing organisation within a federation is used against multiple services. In the R&E multilateral federation context. Such incidents are tackled by propagating IoCs and credential indicators between affected parties, based on for example the *Sirtfi* (Security Incident Response Framework for Federated Identity) and inter-federation cooperation mechanisms. In the presence of AARC Blueprint Architecture proxies, which are prevalent in the research world, these proxies take on responsibility to propagate such indicators between their source identity providers and downstream services.

The EOSC portal was targeted by such an identity-based attack against many of its Core services as well as against horizontal and thematic services in the Exchange. Since actual negative impact on service operations

was identified, this was treated as a security incident and action taken to contain, mitigate, and analyse the incident. Originally identified during a community-AAI enrolment process as a potentially unwanted user, the EOSC Security Coordination Team identified the parties involved, assessed the incident and blocked it from spreading. Potentially affected service providers were informed to prevent the attacker from using non-EOSC mechanisms to achieve their from the service-provider view unwanted) objectives. Through collaboration with the identity provider, federation, and proxies involved, no technical resources (EOSC or otherwise) were abused.

Security *events* often concern vulnerabilities and configurations in web sites, and the notification thereof in a (responsible) disclosure. The EOSC Security Coordination receives such notices, either directly at the abuse@eosc-security.eu address, or through notifications forwarded to it by service owner or (helpdesk) operators. Examples include web-site vulnerabilities such as cross-site scripting or user-ingestible content that can be used for reflection attacks. The EOSC Security Coordination team was notified of one such event and, following the ISM.5 procedure, involved the affected service provider for resolution. Follow-up of such events is devolved to the service provider, who is responsible for its resolution and any subsequent communication with the reporter. In this case, the report was acted upon forthwith and the vulnerability resolved.

5 Conclusions and outlook

Using the community white paper '*Trust Coordination for Research Collaboration in the EOSC era*' [2] as a basis, security operations and policy coordination have been embedded in the EOSC Service Management System based on a subsidiarity approach. The services that constitute the EOSC, both Core and Exchange services, are identified as the fundamental 'assets' on which security coordination is based. This allows service providers to protect their own information security assets in a way that is in line with their risk profile (so that for example data services hosting sensitive personal data implement more controls and put in additional safeguards), and allows for a scalable way to address security incidents that will happen in the EOSC ecosystem.

Emphasis has been placed on the Core services, since their unavailability (or loss of integrity and confidentiality) have the broadest impact on the EOSC. The (central) incident response coordinator has dealt with several security events in the EOSC, although the number of actual incidents was limited (indicative: twice per half-yearly period, picking up pace in the last year of the EOSC Future project). To ensure appropriate readiness for 'real' incidents, a mechanism for security communications challenges was set up and is now exercised periodically (twice yearly) for all Core services. When actual incidents occur, the central team has provided forensics and resolution support.

For the Exchange services, including horizontal services, the central incident response team provides support for coordination and for the exchange of threat intelligence and incident mitigation information. Collaboration was established between the EOSC-Core security team and those providers in the EOSC Exchange (horizontal and thematic services) that avail over an operational security team. Similar links were established with the eduGAIN Security Team, which is supported under the GEANT framework.

The model of 'do no harm' for the services in the EOSC is founded on the understanding of risk by each service, and the ability to identify risks that occur due to composition of multiple services. For this, the WISE Risk Assessment Framework was used to have providers self-assess their exposure based on a standard questionnaire. Rather than requesting an *ab-initio* assessment of their risks based on the ISO 27005 standard, the WISE framework uses a pre-selected list of key security risks for research infrastructures and then have service providers self-assess their service against these risks. In practice, this yields more timely and more comparable results, which is both necessary and (at this stage) sufficient for assessing the cross-service risks in the EOSC (as opposed to service-specific risks, which may of course differ significantly depending on the service involved). The risk self-assessment performed by the chosen reference Core services put the preliminary risk for the EOSC-Core services as 'moderate and somewhat likely' to occur.

To improve the security posture of all services, both Core and Exchange, the Security Operational Baseline has been adopted. This is an intentionally concise set of requirements that all service providers must adhere to. It was incorporated into the EOSC Interoperability Framework in May 2023, and thus applies to all service providers in the ecosystem. While we expect the baseline to slowly evolve over time (as the external threat landscape changes), the principal improvements here should be in the practical guidance that accompanies the Baseline. This FAQ, provided through EOSC Future and linked to the Service Management System, should be kept up-to-date as a standing basis for EOSC Services operation.

References

[1] David L. Groep *et al.* (EOSC Future Consortium), 'D7.5a Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution,' 2022. [Online]. https://wiki.eoscfuture.eu/display/EOSCF/D7.5a+Evaluation+of+EOSC+Security+Baseline (under review).

[2] David L. Groep *et al.*, 'Trust Coordination for Research Collaboration in the EOSC era' 2019, doi:10.5281/zenodo.3674677

[3] The Martii Ahtisaari Peace Foundation CMI, https://cmi.fi, visited July 2023