EOSC-hub week, 19 May 2020

Session Name **Security coordination & policy** *Slides available at:* *https://www.eosc-hub.eu/eosc-hub-week-2020/agenda/security-coordination-policy*	
Main take-aways	*The federated aspects of open scientific communities, our infrastructures, and distributed network makes the EOSC, and EOSChub today, especially challenging. This applies across confidentiality, integrity, and availability. The session addresses the entire spectrum of these challenges, from reactive security incident response, to proactive risk planning, handling vulnerabilities, and establishing and maintaining trust across many administrative domains.* *Attendance was varied, with the 54 participants at the beginning distributed across researchers (5), service developers (10), operators (11), security teams (15), management (6), (and 3 others).* *The sharing of information between service providers, communities, centrally is essential to contain incidents across a multi-domain infrastructure. The central collection and coordination of incidents, as demonstrated again by some recent incidents, protects both the service providers and data, as well as the research being conducted. Stealing of user credentials remains a common attack vector, after which both zero-day vulnerabilities and unpatched systems are used to gain more privileges and subsequently steal even more. And the attacks often spread beyond just the academic community, but collaboration and established reputation still allows to keep tracking the source of incidents. Timeliness is of the essence.* *Many more providers will be coming, and we are in this together - overcome the sharing barriers!* *Complicated networks of infrastructures and communities make for a higher-level picture that brings confidentiality, availability, and integrity into a collective framework. And risks and controls need to be balanced and without losing the 'big picture' when many are involved, and everyone will need to speak the same language. Planning in advance, across all*

	participants, is key, and communication - especially outside your own organisation and site - at least 50% of the task, if not more. *There will be a new study carried out by AON Hewitt on risk management for EOSC. We'd be interested in hearing about your work in this area. here is a link to a news piece on this. The study will contribute to the EOSC governance and is funded by the EOSCsecretariat's co-creation funding* *https://www.eoscsecretariat.eu/eosc-liaison-platform/post/aon-hewitt-support-strengthening-eosc-risk-governance-through [Nick Ferguson, n.ferguson@trust-itservices.com]* *Significant risk, as is almost continuously demonstrated, is incurrent because of vulnerabilities that are exploited by miscreants. And with the increased heterogeneity as more services join the EOSC and the Infrastructures, it becomes more complex to identify, address, and assess the severity of vulnerabilities. Yet like services can help each other and thus - together - improve their posture. At the very least, ensuring known vulnerabilities are addressed and updates applied to operational services, needs close attention. Most incidents are caused by, or aggravated by, unpatched services.* *The challenge related to having end-user provided software, especially in the form of containers, needs both isolation-controls by the service provider running the container, and may benefit from having pre-reviewed containers - that are at the same time attractive to the users - that are engineered to baseline good security practices.* *One of the complementary controls are policy - out of band - controls. The EOSChub efforts have taken the AARC Policy Development Kit as the starting point, adapting them to fit the specific EOSChub environment. The AUP for example is based on the WISE Baseline AUP template, with a common baseline AUP making it simpler for the end-users as well when moving across service providers and infrastructures. They will have agreed to the common AUP, so service providers can feel confident the user had signed a compatible AUP. The WISE Baseline AUP is warmly recommended as the basis, and service providers and communities can augment it with more specific terms and conditions.* *The PDK also provides a Service Operations baseline, which obviously applies to the EOSChub core services, and is suggested inspiration for connected service providers. It is similarly concise, with just 8 issues,*

	including the SCI-derived Sirtfi framework - which has seen extremely wide global adoption already throughout R&E. *Sirtfi encourages sharing, in a world that is increasingly hostile, including both criminal and nation-state actors. Our community needs to band together in view of limited resources and effort to share threat intelligence (if only because commercial feeds are both expensive and may then even be less relevant). The only way to address it for R&E, is sharing within the community. And time is of the essence, so automated mechanisms are clearly advantageous. That sharing is the cornerstone of the effective incident response for our community.* *The "Security Operations Centre" (SOC) concept, started as a WLCG activity, has a wider relevance (and membership) from across the R&E community including NRENs. The SOC tools allow collection, enriching, and sharing of data and Indicators of Compromise (IoCs). Taken together, this is a SOC or 'analytics for security', shown in a four-phase model. The MISP component - as the threat intelligence sharing component - is at the core of the SOC, and CERN provides an 'academic' instance that gets fed with TLP:GREEN and TLP:WHITE threat intelligence from 3rd parties, and in addition with TLP:AMBER threat intelligence data created at CERN and directly applicable to protecting scientific infrastructures. Collaborating with the SOC effort is encouraged: contact David Crooks and/or Liviu Valsan!* *But incidents will happen, and once it happens sharing needs to be complemented with action, engaging a CSIRT, a Computer Security Incident Response Team. Establishing a CSIRT with authority needs both a team and a set of policies and procedures that allows them to act - within a specific scope, authority, and actionable role. And it needs contacts and establishment of personal and organisational trust with other CSIRTs, to allow collaboration to happen. Incidents are not limited to one organisation, or just one infrastructure. But building up trust takes time, and requires a team with sustainability and longevity.* *Communication, as stated before, is critical in a distributed infrastructure. And the comms channels have to be regularly exercised (in comms challenges), and any anomalies followed up actively - to maintain a consistent response fabric.* *Collaboration is where people struggle, and it's the most essential*

	component. And it has to be done globally, and exercises are critical for that. How do we develop leadership in incident response? Research and academia is in a unique position, and at the forefront of development here, since we are the most connected as well as distributed community. *Identify the key stakeholders in each of the infrastructures and approach them. Then develop a joint strategy on response, with roles and responsibilities define, since they don't stop at boundaries, not even the boundaries for R&E. Scope is fluid, and even if there is no mandate to act, helping those on the other side of the fence will be of benefit to all!* *Mark Dietrich highlights human resources and training. In ISO27k this is an important element, but it is known to be a very difficult element across organisations, countries, and jurisdictions. Is there a joint position of the federation towards ensuring training?* *Training is recommended and a baseline required, but its enforcement is down to the specific organisation. For resource admins, security training is provided both explicitly and through the security service challenges.* *And, although key capabilities are held by participants that are also part of the core team, staffing this capability is a continuous challenge.*
Future steps	*The ability to perform risk management, incident response (both security and other aspects) as well as a coherent posture spans all EOSC working groups. Architecture (and its implementation) needs to foresee mechanisms for security response, the ability to log and correlate, collect the key information needed to respond and share this information between the affected parties, within or even outside of EOSC. Authentication, Authorisation (and auditing) play a key role, and need both a technical and policy basis to ensure availability, integrity and the necessary confidentiality needed for research in the connected EOSC.* *In participating in the EOSC, a framework for risk assessment to allow for comparison will be needed and a (potentially peer or externally reviewable) assessment be part of the baseline rules. Risk assessment and vulnerability management, which initially could have been considered local, in a multi-domain world affect many.* *The core elements that enable the EOSC span all working groups, and the trust and security integrity services for the consolidated ecosystem require*

	all of collaborative risk management for service composition, coherent trust management and implementation measures across the EOSC core (so participants know what to expect), ensuring knowhow is available to foster trusted services, and of course provide the trust and response posture & resolution capabilities in case incidents do happen.