Sirtfi WG google folderC

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Task List

Who	What	When	Status
Nicole	Collect several fed security plans.	Feb 28	https://wiki.refeds.org/display/GROUPS/Federation+Incident+Response+Plans
Nicole	Check with WAYF on how they do their incident response - is it like other hub and spokes?	Feb 28	Request sent. Response pending.
Shannon	Report on REN-ISAC information sharing guidelines (2.d)	Jan 31	REN-ISAC ISP Public, Limited, Privileged, Restricted Use information are of interest
Romain	Gather IR plans from some e-infrastructures	Feb 6	
Hannah, Romain	Update templates with experience from table tops. Hannah has already outlined these in another report. Place results in subfolder of the sirtfi google folder, for now.		
Laura	2.c Incident response team communication: Outline a set of requirements for a communications tool (to help with tool selection)	Feb 28	
Mario	Brief Geant 4-3 IR meeting people of Laura's task, maybe arrange Laura's remote participation		
Shannon	Bullets that describe how REN sharing agreement doc should be transformed for (1) federated IR management team context, and (2) broader notification, sharing, or publishing		

Scott	Contact InCommon to see if keeping security contact information fresh could become part of baseline requirements, and use InCommon to investigate and draw out both the policy and the technical implementation. Keep Nicole, Laura, Mario, and Pål in loop.		

January 31, 2019

Attending (11): Tom, Brook, Mario, Uros, Scott, David G, Shannon, Nicole, Laura, Romain, Pål.
Apologies: Hannah, Alan

Proposed agenda:

1. Task review
2. New tasks - define next steps towards each of the following ends:
    a. Improve procedures and message templates (Suggested improvements from AARC)
        i. Where should this type of info be kept? (https://refeds.org/sirtfi ?)
    b. Notifications are sent as appropriate to the broader community, i.e., outside of managing response to an incident
    c. Technical means by which incident management info is shared among members of an incident response team
        i. Secure communication channels, acknowledgement of receipt...
    d. People joining incident response teams understand rules for sharing and any other onboarding needs
        i. Who is on the IR Team?
        ii. How does one gain access
        iii. What are the rules of engagement?
        iv. What about https://en.wikipedia.org/wiki/Traffic_Light_Protocol ?
    e. How to check freshness of security contact info, and how the security contact checking tool that Mario Reale developed should be used
    f. Routine (annual?) table top exercises to keep procedures and technology fresh and introduce new R&E fed ops people to incident response
    g. Packaging of completed tasks into white papers and other artifacts or actions
    h. Other ends to work towards?
3. Proposed deadline: a complete initial draft to discuss at REFEDS at TNC19. Yes/no?
4. Other business