Working-group update

Integration of the Securing the GREN Working Group

Steve Kennet, Executive Director e-infrastructure, JISC;
Charles Sterner, Chief Information Security Officer, AARNet

8 December, 2020

Securing the GREN Working Group

The “Securing the GREN Working Group” (SGWG) was created as a directive by the CEOs’ Global Forum to establish a GREN body that will sponsor and facilitate cyber security collaboration amongst member NRENs to create capabilities entirely unique to the global research and education sector.

As part of the SGWG charter, this body will establish a framework to leverage the unique position of each NREN, creating a set of compelling and competitive features and services that cannot be found within the commercial markets.

Proposed Approach

Bilateral cyber security collaboration based on a 3 phase approach:

- Compliance
- Sharing
- Capacity Building

Compliance

Developing (e.g. standard vendor requirements) or adopting (e.g. MANRS) models which provide a more uniform security posture for the GREN as a whole.

Items under discussion

- ISO 27001/2
- MANRS

Sharing

Leveraging each NREN's unique position, the potential to share threats, intelligence, strategies, and technical content that would enable a compelling differentiator between the GREN and commercial networks. Furthermore, NRENs that operate teleco infrastructure can directly implement high-trust IOCs for mitigation across their entire customer base.

Items under discussion:

- Threat Intelligence
- Orchestration Playbooks
- Security Content (SIEM rule logic)
- Operational Practices

Capacity Building

- Cybersecurity practitioners from more mature (N)RENs will provide support to those with less developed cybersecurity offerings to help raise the baseline of the GREN as a whole.

Items under discussion:

- Training
- Mentorships
- Service White-Labeling
- Service Cooperation / Coordination

Items Under Consideration

Proposal Name	Category	Participant NRENs
MANRS Alignment	Compliance	JISC, AARNet, Internet2
ISO 27001 Services Standard	Compliance	TBD
Threat Intelligence MOU	Sharing	JISC, AARNet, OmniSOC, CanSSOC
Threat Intelligence Sharing	Sharing	JISC, AARNet, OmniSOC, CanSSOC
SOAR Playbook Collaboration	Sharing	JISC, AARNet, OmniSOC, CanSSOC
GREN Training & Mentorships	Capacity Building	TBD
SOC Service Coordination	Capacity Building	JISC, AARNet
Pen Testing Coordination	Capacity Building	JISC, AARNet
AI Red Team Service	Capacity Building	JISC, AARNet