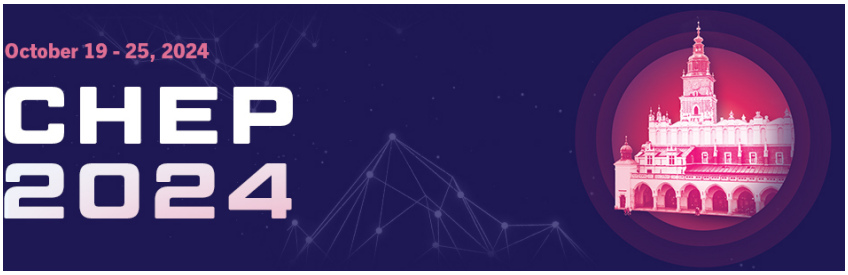

Contribution ID: **438** Type: **Talk**

Designing Operational Security systems: People, Processes and Technology

Wednesday 23 October 2024 14:42 (18 minutes)

The risk of cyber attack against members of the research and education sector remains persistently high, with several recent high visibility incidents including a well-reported ransomware attack against the British Library. As reported previously, we must work collaboratively to defend our community against such attacks, notably through the active use of threat intelligence shared with trusted partners both within and beyond our sector.

We discuss the development of capabilities to defend sites across the WLCG and other research and education infrastructures, with a particular focus on sites other than Tier1s which may have fewer resources available to implement full-scale security operations processes. These capabilities include a discussion of the pDNSSOC software which enables a lightweight and flexible means to correlate DNS logs with threat intelligence, and an examination of the use of Endpoint Detection and Response (EDR) tools in a high throughput context.

This report will include an important addition to the work of the Security Operations Centre Working Group; while this group had previously focused primarily on the technology stacks appropriate for use in deploying fine-grained security monitoring services, the people and processes involved with such capabilities are equally important.

Defending as a community requires a strategy that brings people, processes and technology together. We suggest approaches to support organisations and their computing facilities to defend against a wide range of threat actors. While a robust technology stack plays a significant role, it must be guided and managed by processes that make their cybersecurity strategy fit their environment.

Primary authors: Dr CROOKS, David (UKRI STFC); VALSAN, Liviu (CERN); TEHERAN SIERRA, Jeny Lucia (Fermi National Accelerator Lab. (US))

Presenter: Dr CROOKS, David (UKRI STFC)

Session Classification: Parallel (Track 4)

Track Classification: Track 4 - Distributed Computing