DCL: SaTC: Early-Stage Interdisciplinary Collaboration:

A Sociotechnical Metrics Framework for Network and Security Operation Centers

Alexandru G. Bardas, University of Kansas (www.alexbardas.com)

Bradley R. Fidler, Stevens Institute of Technology (https://faculty.stevens.edu/bfidler)

How Metrics Are Used to Secure Enterprise Networks Today

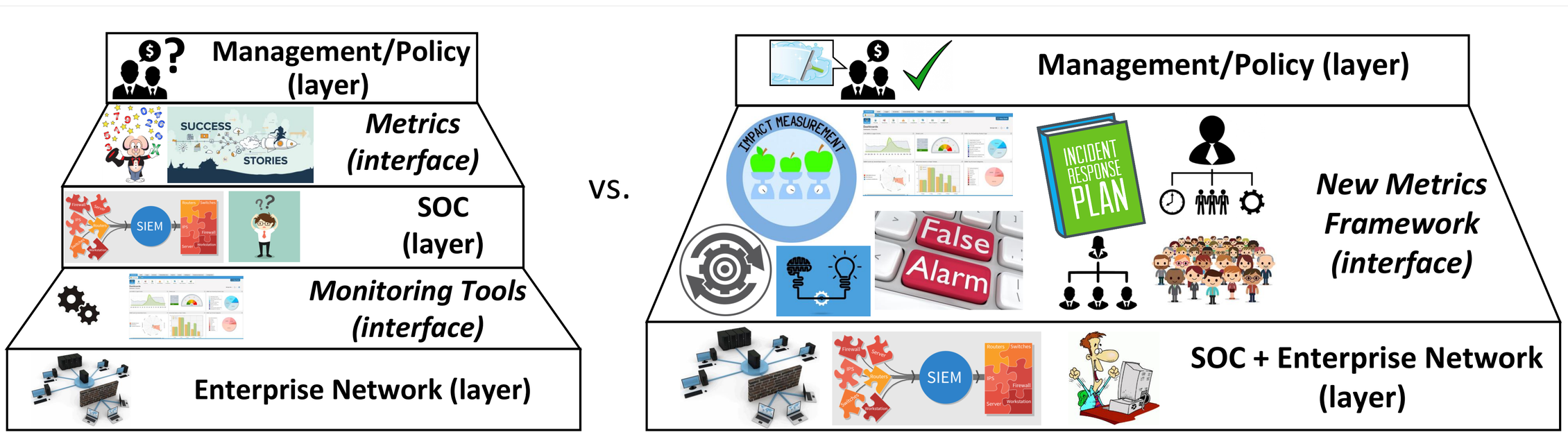
We secure networks with Network and **Security Operations Centers** (SOCs). Organizations use SOCs to defend against cyber threats and manage their network operations. SOCs use **metrics frameworks** to monitor networks, prioritize tasks, and communicate network facts to management. Metrics sit between the network and the SOC, and the SOC and management.

The Problem

SOC metrics are deficient at linking these components together, especially the security posture of the network and the SOC. These metrics lead to inefficiencies and maladaptive behavior on the part of the SOC analysts and degrade enterprise network security.

What We're Doing

We are developing a new metrics framework that will harmonize SOC performance against enterprise network security—by treating the SOC as an integrated part of the network itself:



Current Setups

Proposed Research

Deliverables

- Detailed analysis of the present-day network/SOC tasks (before and during COVID-19) using ethnographic, technical, and historical perspectives: informing us what can reasonably be changed and what is the consequence of the objective requirements of network management with a flexible network perimeter
- An adaptable metrics *framework* for handling security incidents that can be fine-tuned for specific network/SOC cases

Inclusion in STEM

- Today, SOC metrics frameworks degrade workplace culture and do not reward contributions effectively: better metrics may help us construct more equitable SOCs
- Including under-represented groups in this research project

Impact on Network and Internet Security

- Ignite a major shift in the network (and thus internet) security landscape by changing the way networks are monitored: with tailored metrics for real-world environments
- Fundamentally alter SOC operations by incentivizing behavior that is aligned with the realities of that network