

All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Actionable metrics

Yes, threat information (demographics, impact, controls, etc.) are useful. But for the most part, we can really only act on our controls and processes, so actionable security metrics will be about controls and processes, and not about threats.

Guest editor Vicente Aceituno Canal - Managing Director - www.inovement.es

Threat as environment

Threat metrics are environmental metrics, akin to understanding the temperature and humidity outdoors. Controls and processes are akin to what heaters you start, how you make the air flow in a building, etc. You can act on what you control to influence the results; in this example the temperature and humidity indoors.

Mature controls

Controls and processes can be implemented in a variety of maturity levels, they are not only Present/Not Present. Another complication is that certain controls and processes are extremely effective against threats, whereas others are of little effect. You can call this the effectiveness of the control or process.

In order to manage your security or risk, you need metrics about the environment, metrics to understand how effective your controls and processes are, and metrics on the maturity of your controls and processes. Threat metrics alone are not enough.

I would argue controls and process metrics are the most important. Understanding what other people in the industry are doing and what their results are would produce the most actionable metrics we can use to improve security.

Barriers to mature controls

I understand the many barriers present in order to get metrics about the maturity and effectiveness of controls. The lack of uniform terminology, the many different frameworks for controls (ISO27001, PCI-DSS, SANS CSC 20, O-ISM3) make it difficult to make fair comparison of the controls and processes of different organizations. I am actually preparing a tool for this kind of information sharing.

The value of ISACs

Today, there are increasingly groups being formed called Information Sharing and Analysis Centers (ISACs). They provide a venue for sharing between and across similar and diverse critical infrastructure providers. They are an outstanding model of how sharing can be done, and while they aren't yet producing the sorts of metrics we need to improve the control system that security management is, they are a good starting point. Perhaps with cooperative efforts, we in the security space can develop sound and comparable metrics to allow us all to do better.