Darktrace Response: Evaluating and Improving NIST Cybersecurity Resources

The NIST Cybersecurity Framework is essential in the cyber defense space. With its increasing popularity, the framework's accessibility and ease of use is critical and should be able to scale seamlessly, especially for new practitioners of cybersecurity. This will help address one of the primary challenges that may prevent organizations from using the NIST cybersecurity framework more easily and extensively: that is, the lack of navigability and intuitive access in the current presentation of the NIST framework.

The website for the NIST Cybersecurity Framework is packed with information and navigating through the website is not intuitive. The "Framework Resources" section of the website is a step in the right direction, but unfortunately the resource is not readily discoverable, and the control information is only high-level. Ultimately, the different sections of the "Framework Resources" link back to a series of PDFs that are difficult to parse through individually. PDFs, excels, and PowerPoints are certainly necessary forms of documentation, but they lack the degree of visualization and navigability that could be achieved by a web page with an intuitive design that optimizes user experience.

Increasing the visualization capabilities of the NIST Cybersecurity website will significantly improve NIST Cybersecurity awareness and education. Ideally, the site could readily showcase the Cybersecurity Framework sections (i.e., function, category, subcategory, and informative references) rather than focusing on all the supporting information present today. The ability to automatically see and work with the framework upon opening the site, being able to click on a function, quickly pullout all the categories and subcategories, and allow the user to export their results is a sampling of possible enhancements.

Other ease of use considerations could include the ability to create a NIST Cybersecurity scoring and reporting capability to compare the security posture of a company against the NIST Cybersecurity Framework. Further, creating a Mobile App to showcase the NIST Cybersecurity Framework that increases navigability and intuitive access would be widely used for practitioners on the go.

When it comes to the content of the framework, more actions should be added that explicitly address the increasing convergence of information technology (IT) and operational technology (OT). This trend has been driven by the rise in recent adoption of remote access for OT, industrial internet of things (IIoT), and cloud and SaaS systems for industrial control systems (ICS). Oftentimes, this convergence can even be unintentional, as when an organization has poor network segmentation or unwittingly uses an OT protocol on an IT network.

Many major cyber-attacks against critical infrastructure over the past several years have demonstrated that when critical infrastructure's IT becomes compromised, mission-critical OT assets are jeopardized. Attacks that rapidly spread laterally such as ransomware can easily spread from IT to OT systems in converged ecosystems. Moreover, as with the Colonial Pipeline incident, OT systems may have to be shut down manually, even though only IT systems are affected, due to the threat that underlying, unseen points of convergence could pose to mission-critical OT assets.

It is crucial for critical infrastructure organizations to discover potential points of IT/OT convergence across their digital environments, illuminating the various pathways by which attackers can move from enterprise to industrial networks. Potential areas where NIST can add recommendations explicitly concerning IT/OT convergence include the following: asset management, risk assessment, and risk management strategy.

We are no longer are in a time at which critical infrastructure organizations can assume that an air gap will protect mission critical assets. Both intentional and unintentional forms of IT/OT convergence present a significant risk to critical infrastructure that must be dealt with in a rigorous fashion.