A cyber threat lingua franca

"Removing Barriers to Sharing Threat Information" ranks as one of the top initiatives in the Biden Administration's Executive Order on Improving the Nation's Cybersecurity. The administration issued the order in the wake of the Colonial Pipeline ransomware attack and other recent high profile breaches, but sharing information has been a persistent and systemic challenge across government, and officials consistently voice their frustration with information sharing.

Cybersecurity officials have pointed to MITRE's STIX™ Framework (Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression) as important for

improving cyber threat information sharing. STIX is a standard programming language that conveys the full range of potential cyber threat information, to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. Used in conjunction with MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) and D3FEND, which are openly-available knowledge bases of offensive and defensive tactics and techniques based on real-world observations, a potential roadmap emerges for improving cyber defenses across government and critical infrastructure.

Leidos is using ATT&CK to improve how cyber security professionals can defend against cyber-attacks by simulating cyber incidents and automating analytics and defensive responses. And our cybersecurity professionals already use both ATT&CK and STIX at-scale to facilitate critical information sharing with the Defense Department and other government customers.

ATT&CK-ing cyber threats

Leidos uses ATT&CK techniques across our Security Operations Center portfolio to help characterize attacks and threats. One of our innovative approaches enables us to profile cyber actors for multiple large national security customers. This approach to ATT&CK comprises five key steps: characterize, visualize, analyze, respond, and automate.

First, Leidos cyber professionals characterize a threat using alerts and tips. Our analysts store each potential threat, with a reference to its source, in a database so that it can be easily identified in the future.

Next, Leidos employs specialized, user-friendly dashboards to better visualize each threat, allowing analysts to sort threats by event, actor, network, subscriber, date, and more. Leidos provides advanced analytics through these dashboards, such as heat maps that illustrate network risk, to determine the validity, frequency, severity, and even potential intent of attacks. Finally, our cyber professionals connect that information with corresponding infrastructure, and then to courses of action, such as those in the complementary D3FEND framework, and automate future responses to similar threats using security orchestration, automation, and response (SOAR) technologies.

Each of these steps enables front-line national security agencies to respond faster and more effectively to cyber threats, as well as build profiles of malicious actors to prepare against future incidents.

STIX and stones

Better and more frequent communication about cyber threats between the private sector and government could accelerate the response to malicious attacks. But this information sharing could

deposit the proverbial "stone in the road" if the additional information that isn't processed, correlated, and applied, or if it cannot be used by the receiving organization. Across the country, different organizations have different levels of maturity – both in their cybersecurity capabilities and in their IT capabilities. While STIX provides the common language for entities to share cyber threat information and make after-incident reports, it is still important to improve overall cybersecurity, and to increase the holistic awareness across organizations. These activities were highlighted in the recent executive order. Leidos is leading the way in driving improvement across the cybersecurity spectrum.

Leidos is also developing new, innovative ways to facilitate information sharing with its government customers using STIX. In one internal research and development project, Leidos cyber professionals showed how they can automate attacks in a digital sandbox using catalogued combinations of ATT&CK techniques to refine detection analytics and to test remediation responses. This kind of continuous improvement enables Leidos to share the cyber threat information and effective responses needed to defend against evolving attacks.

RELATED INSIGHTS

VIEW MORE INSIGHTS

How to speed R&D and deter advanced cyber threats

Zero Trust is critical for managing your organization's network security