Topic 7 Discussion 1

Examine how the use of threat information and intelligence helps cybersecurity emergency response teams (CERT) identify and respond to threats in a timely manner.

Hello Class,

The utilization of threat information and intelligence is pivotal for cybersecurity emergency response teams (CERT) in proactively identifying, understanding, and mitigating cyber threats. Threat intelligence offers insight into the tactics, techniques, and procedures (TTPs) of cyber adversaries, providing context to the vast array of potentially malicious activities that might target an organization. By analyzing this data, CERTs can anticipate attack vectors, recognize vulnerabilities that may be exploited, and understand the modus operandi of threat actors. This proactive approach enables organizations to patch known vulnerabilities, heighten monitoring on high-risk assets, and put preventative measures in place before an attack transpires, greatly reducing the potential damage.

Furthermore, when a cybersecurity incident occurs, having access to real-time and historical threat intelligence allows CERTs to respond more efficiently and effectively. By correlating current incidents with past threat intelligence, CERTs can quickly discern the nature of the attack, the potential impact, and the most appropriate response strategy. This accelerates the decision-making process, enabling faster containment of the threat and reducing dwell time for adversaries within the network. Overall, the integration of threat information and intelligence ensures that CERTs are better equipped, both preemptively and reactively, to protect their organizations from the ever-evolving landscape of cyber threats.

References:

*Cyber Threat Intelligence & Information Sharing | ConnectWise*. (2023, January 6). Www.connectwise.com. https://www.connectwise.com/cybersecurity-center/glossary/threat-intelligence-sharing#:~:text=Cyber%20threat%20intelligence%20is%20the

*Cyberthreat Intelligence as a Proactive Extension to Incident Response*. (n.d.). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/cyberthreat-intelligence-as-a-proactive-extension-to-incident-response

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. *Guide to Cyber Threat Information Sharing*. https://doi.org/10.6028/nist.sp.800-150

Sullivan, P. (2023, February). *What is CERT?* WhatIs.com. https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team