NIGC Tech Alert

Cybersecurity: Endpoint Detection and Response

The constant threat of attacks on an IT enterprise is always present and is one of many reasons to regularly assess and implement strong Information Technology system controls and security measures in your environment. Key security measures to protect against malware attacks are physical and logical security. As organizations seek to improve the security posture of their IT enterprise in this modern world, many IT leaders are focusing on ways to securely manage the endpoint devices of their network.

Protecting the network enterprise using traditional antivirus software and network level firewall protection are not enough to ensure the security of your endpoints. Endpoint Detection and Response (EDR) technology is widely available by vendors and is one of many ways to help evolve network endpoint security for organizations. EDR is a cybersecurity solution that provides capabilities for endpoint monitoring and protection against threats that may have breached a network perimeter. EDR also detects and mitigates suspicious activity from endpoint devices within the network. EDR solutions provide greater visibility into what is occurring on an organization's assets and in many instances feed intelligible event information into a centralized security incident event management software. One major aspect of EDR that makes it an excellent network endpoint solution is the capability to shift from a prevent and detect capability to a response-based utility.

EDR can also be used to record forensic data should a file pass the pre-execution phase on a compromised network. The forensic data may contain details like the time a file was opened on an endpoint device. This is how EDR vendors were able to assist in finding the impact of the SolarWinds breach (https://www.cisecurity.org/solarwinds). EDR is the starting point in lowering dwell time of a malware intrusion affecting endpoints. EDR's concentration is on endpoint devices, however advancements in cybersecurity technology have introduced Extended Detection Response (XDR) tools which perform a more extensive detection and response capabilities across entire networks, including firewalls, IoT devices and cloud systems.

EDR and XDR solutions are additional tools that can be utilized by an organization to provide endpoint and network security controls and protection through advanced threat monitoring, detection and response capabilities. For organizations with limited IT resources, third-party managed service providers exist to provide Managed Detection and Response (MDR) services which offer both EDR and XDR technology services. EDR has quickly become the industry standard for endpoint security protection over traditional antivirus solutions.

Please view the Center for Internet Security Election Security Spotlight for an in-depth look at EDR at:
https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-endpoint-detection-and-response-edr

Please view the TechTarget website for more information on the SolarWinds Hack at:
https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released a Request for Information (RFI) to garner support for the U.S. effort to maximize the potential of EDR. By gathering input from subject matter experts in the industry, CISA sought to capitalize on the opportunity to evolve endpoint security for government networks. Subsequent to the CISA RFI, and after the Colonial Pipeline Ransomware attack, President Biden signed Executive Order (EO) 14208 which addressed the need to improve the nations cybersecurity infrastructure and government networks.