Outsiders Versus Insiders

By Divaco Colbert

Insider Threats: Warning Signs and Detection

When it comes to insider threats, detecting suspicious behavior can be a challenge. However, certain warning signs can indicate an employee is attempting to steal sensitive information. These may include changes in behavior or performance, access to data or systems beyond their job duties, or attempts to bypass security protocols.

One of the difficulties with detecting insider threats is that these individuals already have authorized access to the systems and data they are targeting. This makes it even more important to pay attention to any deviations from normal behavior. For example, an employee who suddenly starts working late takes confidential information home or engages in unusual network activity could be trying to steal information. Similarly, an employee who repeatedly fails to follow security protocols, such as failing to lock their computer screen when stepping away, may be attempting to bypass security measures.

Outsider Threats and Security Monitoring

In order to protect against outsider threats, security administrators must constantly monitor and analyze data to detect any suspicious activity. This includes watching for attempts by outsiders to access a system using stolen or brute-forced credentials, as well as any attempts to install malware or backdoors onto the system.

Some of the key indications of outsider threats include unusual network traffic patterns, attempts to access restricted files or systems, the use of unauthorized/unfamiliar devices, software, and user accounts. Outsiders hold more power than insiders because the focus may shift from just financial control to a potential loss of strategic control.

Conclusion

In conclusion, consider both outsider and insider threats when developing cybersecurity protocols. The warnings about these threats may differ, an approach to cybersecurity that includes regular monitoring and training can help organizations detect and prevent security incidents. By implementing strong security measures and organizational policies, security administrators can better protect their organizations from both outsider and insider threats.