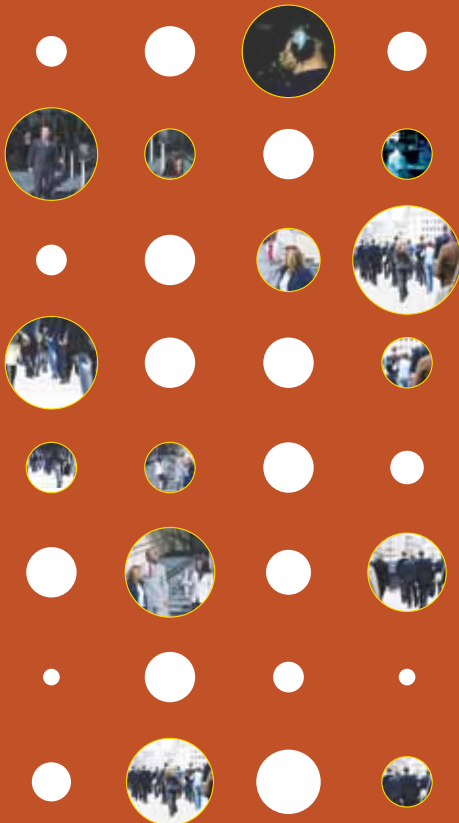




Detecting Insider Threat Requires a Multi-Faceted Approach

Relying on tools may not be sufficient for identifying malicious insider activities. In this workshop, we teach attendees how to develop an effective, comprehensive monitoring strategy.



Insider Threat Workshop

Insiders Use What They Know

The following activities are not unusual:

- a system administrator creates a user account and writes a script
- a researcher or an engineer sends a file to an external collaborator
- a customer service representative adds or modifies account information

But what if those tasks are being performed with malicious intent? For example, suppose that

- the account that the system administrator created was a backdoor, and the scripts contained malicious code
- the file sent by the researcher or engineer contained proprietary information and was sent to an unauthorized recipient
- the account information created by the customer service representative was not legitimate and was created in return for a bribe by an outsider

Malicious insiders are dangerous and difficult to identify because they typically use authorized access and regular business processes to commit fraud, theft, sabotage, or espionage.

We Can Help You Identify Threats

Although technical controls such as monitoring and logging tools have evolved, they have limitations. They may fail to identify malicious activities that appear to be legitimate tasks. Also, they tend to generate significant amounts of data that needs to be processed and significant amounts of false positives.

For the past decade, members of the CERT® Insider Threat Center have been researching insider threat, conducting assessments of organizations, and presenting workshops. We also have a database of more than 550 actual insider threat cases, from which we have extracted a list of technical and non-technical methods used by malicious insiders, including current and former employees, contractors, and business partners.

Our “crime profiles” describe patterns of insider behaviors, organizational issues, and technical actions over time for each type of crime. The profiles suggest practical policies and practices which, in conjunction with logging and monitoring tools, can provide an effective logging and monitoring strategy.

In this workshop, we will spend a significant amount of time exploring those crime profiles. Attendees can compare our list of technical methods against their



Software Engineering Institute

Carnegie Mellon

For more information about our research, visit the CERT® website:

www.cert.org/insider_threat

For more information about this workshop, email Insider Threat Center staff:

insider-threat-feedback@cert.org

We Can Help You Identify Threats (continued)

organizations' technical controls to identify gaps in their controls. To reinforce the principles taught in the workshop, we will also present technical demonstrations of monitoring techniques that could have detected malicious activity in actual insider threat cases.

This workshop is designed for individuals who are responsible for designing and implementing monitoring strategies within their organizations. We also strongly recommend that executives, human resources, legal, physical security, and data owners also attend the workshop. Attendees will leave the workshop with a list of actions they should consider in order to implement an effective insider threat detection solution across the organization.