CODE42

OVERVIEW

Departing Employee Operational Framework

Ensure data doesn't depart with employees

Protecting intellectual property as employees and contractors depart is a core component of an insider threat program. A successful operational framework to protect your organizations intellectual property (IP) from theft begins with focusing on departing employees. You'll need to organize and align the necessary people, process and technology to provide your organization with the ability to stop intellectual property theft. Begin by gaining visibility to activity within core vectors most commonly used for insider exfiltration.

Whether you are building your organizations insider threat program from the ground up, or continuing to refine it, here's where to start:

- Update or create your insider threat program risk objectives. Quantify financial risk as thoroughly as possible for these risks. For inspiration, we recommend CERT's Common Sense Guide to Insider Threats.
- Present your risk objectives and financial risk analysis to your existing insider threat program executive sponsor and confirm their understanding and support.
- Create key metrics to be used to baseline and measure the progress of reducing departing employee risk. Start simple with number of employees reviewed and findings for each employee.
- Create, distribute and get employee acknowledgement of security policies, such as:
  - Acceptable Use Policy (AUP)
  - Data Privacy Policy
  - Employee Code of Conduct Policy
  - Employee Termination Policy
  - Insider Threat Discipline Policy

With this broader insider threat program framework in place, you're ready to start developing your departing employee intellectual property theft protection operational framework.

People

Teams to work with:

- **HR** will help to develop appropriate due process and fairness procedures for disciplinary actions against employees. They can also provide a list of departing employees on an ongoing basis.
- **Security Operations** will incorporate appropriate employee termination procedures into the insider threat program. Ensure that part of the procedures includes offboarding data.
- **Legal** will provide guidance on how to handle severe events including interaction with state, federal or international criminal organizations. The legal team can also identify when an employee should be put into a legal hold status.

Process

Tactics to implement:

- Insider risk assessment
  - Insider indicator prioritization
- Key exfiltration vector monitoring, alerting and incident response integration
- Insider threat incident response
  - Alter existing incident response and case/investigation processes to add insider threat incident type
- Insider threat breach response
- Quarterly insider threat program executive report
- Execute annual insider threat scenario based assessment

Technology

Capabilities you'll need:

- Monitor USB and other removable media for data exfiltration that is non-compliant with an Acceptable Use Policy (AUP)
- Monitor personal email use for data exfiltration that is non-compliant with AUP
- Monitor personal web storage i.e. Dropbox use for data exfiltration that is non-compliant with AUP
- Monitor corporate web storage i.e. OneDrive or Google Drive for data exfiltration that is non-compliant with AUP
- Detect large web uploads and whether or not the uploads are to a trusted destination
- Detect ZIP creation
- Insider threat data correlation on SIEM, UBA or logging system
- Insider threat SOAR process development to automate investigation
- Complementary data sets:
  - User & privileged access activity
  - Social media activity
  - Network source and destination activity
  - Traditional AV or EDR security activity
  - Security awareness/training history
  - Employee promotion/demotion/job change

Annual Audit & Review Activity

Through continual audit and review, your team will continue to strengthen your risk posture by identifying and filling gaps in the current departing employee operational framework. Annual key audit activities will ensure your program remains current and is optimized:

- Third party insider threat program assessment using Capability Maturity Model
- Semi-annual insider threat report for executives and board
- Review top ten most critical assets list
- Create reports usable as audit evidence/artifacts:
  - User compliance/non-compliance with AUP or other policies
  - Personal email use for data exfiltration that is non-compliant with AUP
  - Personal web storage i.e. Dropbox use for data exfiltration that is non-compliant with AUP

CODE42

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM

OV2004190