SIA EDUCATION at ISC

Unveiling Shadows: Navigating the Nexus of Background Checks and Insider Threats in Organizational Security

MODERATOR
TYLER HOSFORD
Security Director
International SOS

DAVE KOMENDAT
Senior Security Advisor,
International SOS
Former CSO, Boeing

SPENCER EVANS
Special Agent in Charge,
Federal Bureau of
Investigation

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

OVERVIEW

In today's interconnected corporate environment, insider threats pose significant risks to organizational security.

OBJECTIVE

To explore the critical role of comprehensive background checks in identifying and mitigating potential insider threats.

UNDERSTANDING INSIDER THREATS

Definition: Insider threats involve individuals within an organization who may intentionally or unintentionally compromise security protocols.

MALICIOUS INSIDERS:

Employees who intentionally misuse their access for personal gain or to harm the organization.

NEGLIGENT INSIDERS:

Employees who inadvertently cause security breaches due to carelessness or lack of awareness.

COMPROMISED INSIDERS:

Employees whose credentials have been stolen or compromised by external actors.

THE ROLE OF BACKGROUND CHECKS

Purpose: Background checks serve as a proactive measure to assess the suitability and reliability of potential and current employees.

- ✓ **CRIMINAL HISTORY:** Identifying past legal issues that may indicate risk.
- ✓ **EMPLOYMENT VERIFICATION:** Confirming previous job roles and performance.
- ✓ **CREDIT CHECKS:** Assessing financial stability, which can be a factor in susceptibility to coercion.
- ✓ **EDUCATION VERIFICATION:** Ensuring the authenticity of academic qualifications.

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

CASE STUDY: THE IMPORTANCE OF THOROUGH VETTING

INCIDENT OVERVIEW

- An American cybersecurity company unknowingly hired a North Korean IT worker who later attempted to extort the company by stealing sensitive data.

LESSONS LEARNED

- The critical need for rigorous background checks, especially in remote hiring scenarios.
- The importance of continuous monitoring and verification to detect and prevent insider threats.

BEST PRACTICES FOR MITIGATING INSIDER THREATS

- ✓ **IMPLEMENT COMPREHENSIVE BACKGROUND SCREENING:** Conduct thorough checks during the hiring process to identify potential risks.

- ✓ **CONTINUOUS MONITORING:** Regularly update and review employee information to detect any emerging threats.

- ✓ **EMPLOYEE TRAINING:** Educate staff on security protocols and the importance of safeguarding sensitive information.

- ✓ **ACCESS CONTROL:** Limit data access based on roles and responsibilities to minimize potential misuse.

- ✓ **INCIDENT RESPONSE PLAN:** Develop and maintain a robust plan to address insider threat incidents promptly.

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

BEST PRACTICES FOR MITIGATING INSIDER THREATS

✓ IMPLEMENT COMPREHENSIVE BACKGROUND SCREENING:

Conduct thorough checks during the hiring process to identify potential risks.

✓ CONTINUOUS MONITORING:

Regularly update and review employee information to detect any emerging threats.

✓ EMPLOYEE TRAINING:

Educate staff on security protocols and the importance of safeguarding sensitive information.

✓ ACCESS CONTROL:

Limit data access based on roles and responsibilities to minimize potential misuse.

✓ INCIDENT RESPONSE PLAN:

Develop and maintain a robust plan to address insider threat incidents promptly.

CONCLUSION:

By integrating comprehensive background checks with ongoing security measures, organizations can effectively navigate the complex landscape of insider threats, thereby safeguarding their assets and maintaining operational integrity

THANK YOU!

Scan the QR Code on the left to provide your feedback on SIA Education@ISC Sessions at ISC West

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses