Student Guide
Cyber Insider Threat

Course Introduction
Introduction
Screen 1 of 1

Sammy: Welcome to the Cyber Insider Threat course!

Take a moment to review the course objectives.

Screen Text: Course Objectives:

- Explain cyber insider threat and associated indicators
- Apply cybersecurity countermeasures to mitigate risk

Lesson 1
Introduction to Cyber Insider Threat

Introduction
Screen 1 of 13

Screen Text: Intro to Cyber Insider Threat

Sammy: Let's start the course by watching this video.

Video: We really have to try to attack the issue from the root of the problem and really understand what an insider threat means. So along those lines, the core feature of insider threat is betrayal. These are individuals who betray their positions of trust and use their positions and legitimate access for illegitimate means.
Along that line, the key factor is that it's purposeful.

Sammy: Hey, our internet service has been hacked! Well, we can't use the TV anymore, so I'll pull out the old projector. Can you hit the lights?

Sammy: Okay, great – glad it's working. Let's start out by defining cyber insider threat and then identifying the cyber risks associated with trusted insiders.

Screen Text: Learning Objectives

- Define cyber insider threat
- Identify the cyber risks associated with trusted insiders

Definition
Screen 2 of 13

Screen text: Insider Threat

Sammy: First, we're going to define insider threat.

An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly cause harm to an organization and its resources including information, personnel, and facilities.

A cyber threat is simply defined as the possibility of a malicious attempt to damage or disrupt a computer network or system. However, this is just the beginning.

So much of our lives and our business are conducted on line – cyber-attacks are often the first step in a larger attempt to commit a variety of acts such as fraud, theft, sabotage, espionage, copy right and intellectual property violations, just to name a few.

Threats and Targets
Screen 3 of 13

Sammy: To begin our talk about cyber threats, here's an excerpt from former FBI Director, James Comey's, remarks about cyber security.

Director Comey: "Let me start with the threat. I actually try to describe to people in very simple ways what we're talking about today because I don't see cyber as a thing, I see it as a way. As a vector. Because my children play on the Internet. Because that's where I bank. Because that's where my health care is. Because that's — I don't have a social life, but if I had one, that's where I'm sure it would be. That's where our nation's critical infrastructure is, that's where our government's secrets are and that's - because life is there - that's where bad people come who want to hurt children, who want to steal money, who want to take identities, who want to steal secrets, who want to damage dams and critical infrastructure in the United States. It's the way they come at us because that's where life is.

I harken back to what I believe was the great vector change that gave birth to the FBI. And this popped in my head when I was visiting the field office that we have in Indianapolis. A local sheriff gave me a round that had been fired from John Dillinger's Thompson submachine gun. It occurred to me that the great vector change of the 1920's into the 1930's was the confluence of the automobile and asphalt. It gave birth to an entirely new way of doing bad things. Suddenly criminals could move at breathtaking speeds, right? Forty miles an hour. Fifty downhill. Right? They could go from Ohio to Indiana to Illinois in the same day and do bank robberies in each of those locations. They were blowing away traditional notions of county line and state line. Right? It was straining the framework that law enforcement used and so a national force was needed and there was — I'm the seventh director — there was the first director of the FBI, J. Edgar Hoover. And a national force was born to respond to that entirely new way of

crimes being committed. A new vector that required a new approach.

This is that times a million. Dillinger or Bonnie and Clyde could not do a thousand robberies in all 50 states in the same day from their pajamas from Belarus. That's the challenge we face today The traditional notions of space and time and venue and border and my jurisdiction and your jurisdiction are blown away by a threat that moves not at 40 miles an hour or 50 downhill, but at 186,000 miles per second. The speed of light."

Threats and Targets (cont.)
Screen 4 of 13

Screen text:
State Actors
Terrorists
Criminals
Hackers
Business Competitors
Employees

Sammy: The challenge Comey is referring to, involves cyber threats from various sources, including state actors, terrorist groups, criminals, hackers, business competitors, and even trusted insiders. In fact, it's the threat from trusted insiders that poses the most significant cyber risk because they can easily access the organization's information system.

Sometimes it's the very people charged with protecting the system, such as the information security system staff, those with administrative rights, or other privileged users.

Whether as a malicious act — the deliberate exfiltration of information or introduction of malware or other harmful code — or inadvertent actions by careless employees, the greatest threat to an organization's information system is often on the inside.

Who, What, and How?
Screen 5 of 13

Screen text:
Who is at risk for cyber attacks?

- Federal, state, & local government
- Private corporations
- Critical infrastructure sectors
- Non-governmental organizations
- Universities
- Health care facilities

What is being targeted?

- Sensitive company documents
- Employee information and PII
- Export-controlled technology
- National security information
- Civilian and dual use technologies
- Sensitive technological specification documents
- Usernames/passwords
- Financial data
- Security procedures

How do attacks occur?

- Hacking
- Malware
- Sabotage
- Covert channels

Sammy: Who is at risk for cyber-attack? All of these agencies and facilities have had their information systems targeted by insider threats with significant negative effects. Threats often target sensitive company documents, national security information, usernames and passwords, and personally identifiable information, or PII.

So, how do these attacks occur? Technology is both the target of these cyber threats and the means by which they attack. Cyber criminals often use covert channels to install malware and transmit data.
As you can imagine, all of these methods are far easier for insiders – those with authorized access – to pull off.

Before we continue, I have a couple questions for you.

Knowledge Check
Screen 6 of 13

Criminals pose the most significant cyber risk because they can easily access the organization's system.

Select the best response; then select Submit.

- o True
- o False

Knowledge Check
Screen 7 of 13

Screen text:

Cyber insider threat is an individual with authorized access who wittingly or unwittingly attempts to disrupt a computer network or system.

Select the best response; then select Submit.

- True
- False

Insider Threat Indicators
Screen 8 of 13

Screen text:

Theft - An insider's use of IT to direct specific harm at an organization or an individual
Fraud - An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data for personal gain, or theft of information.
Sabotage - An insider's use of IT to direct specific harm at an organization or an individual
Espionage - The transmittal of national defense information with intent to aid a foreign power or harm the U.S.
Malware - Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

Sammy: As we discussed, there are specific cyber risks associated with trusted insiders. These include theft, fraud, sabotage, espionage, malware, and more.

Cyber risks can be accomplished through direct control of information systems or the intentional or unwitting introduction of malware such as a Trojan horse, keystroke logging, backdoors, and more.

Insider Threat Indicators (cont.)
Screen 9 of 13

Screen text:
Unwitting:

- Harmful malware
- Providing access to malicious actors

Witting:

- Predisposition
- Opportunity
- Specific motive

Sammy: So, what makes a trusted insider become a cyber insider threat? Unwitting insiders cause harm by inadvertently introducing harmful malware into a system or unknowingly provide access to malicious actors.

Poor security practices such as clicking links, sharing or using weak passwords, using tainted removable media and other actions increase cyber threat vulnerability. Failure to follow security protocol is one indicator of insider risk.

Some insiders have a personal predisposition that, when combined with opportunity and specific motivations causes them to react to stressful events – or triggers – by committing malicious acts. For example, opportunity comes in the form of access to the information system; the motive may be financial gain, and the trigger may be disgruntlement or personal problems. To see an example of this, view the case study in the course resources.

Screen text: Insider Threat Potential Risk Indicators

- Foreign contacts
- Foreign loyalty
- Intentional mishandling of protected information
- Unexplained affluence
- Unexplained absences
- Unauthorized removal of classification markings
- Working outside of normal work hours
- Security violations

Sammy: Insider Threats, both witting and unwitting, display a variety of potential risk factors. Here's a list of possible indicators. It includes, having foreign contacts, unexplained affluence, or working outside of normal work hours.

Insider Threat Indicators (cont.)
Screen 10 of 13

Screen text:
Cyber Insider Threat Perpetrators
Explorers
Samaritans
Hackers
Machiavellians
Proprietors
Avengers
Career Thieves
Moles

Sammy: Explorers commit violations in the process of learning a system, usually without malicious intent. Samaritans bypass protocol and will hack into a system with the intent of fixing a problem but cause a much bigger issue. Hackers typically have a prior history of hacking and continue penetrating systems after they are hired. Machiavellians engage in sabotage or espionage to advance their career or other personal agendas. Proprietors act as if they "own" the system and are willing to damage the system rather than give up control. Avengers are classically disgruntled employees, who act impulsively out of revenge for perceived wrongs done to them. Career thieves will take employment with a company solely to commit theft, fraud, or embezzlement. Moles enter an organization solely for the purpose of stealing information, for a competing company or foreign country.

Knowledge Check
Screen 11 of 13

Three employees at a law firm managed to use Dropbox to transfer approximately 78,000 documents from their firm to their Dropbox account before abruptly quitting and moving on to another firm.

They then modified confidential client information on those documents in the Dropbox account and set their accounts to sync both ways so that faulty information would be transmitted back to the original employer's cache of documents.

The law firm is conducting business on faulty information which, of course, cost them their clients, who then went to the competitor.

What risks are most associated with this case?

Select all that apply; then select Submit.

- Theft
- Fraud
- Workplace violence
- Sabotage

Knowledge Check
Screen 12 of 13

An employee used his access to the country's terrorist watch list to put his wife's name on it while she was out of the country. Her appeals fell on deaf ears for three years until her husband was on tap for promotion and his superiors ran a routine background check only to find out that the employee's wife was on the terrorist watch list. The employer saw her appeals and discovered the employees plot against his wife.

What type of cyber insider threat did the employee represent?

Select the best response; then select Submit.

- Samaritan
- Machiavellian
- Avenger
- Career Thief

Lesson Conclusion
Screen 13 of 13

Screen text: Learning Objectives

- ✓ Define cyber insider threat
- ✓ Identify the cyber risks associated with trusted insiders

Lesson 2
Cybersecurity in Insider Threat Operations

Leeson Objectives
Screen 1 of 10

Screen text:
Learning Objectives:

- Summarize the role of cybersecurity in an Insider Threat Hub
- Apply cybersecurity mitigation strategies posed by trusted insiders

Sammy: Glad you're back! Here are your lesson learning objectives.

Cybersecurity Role
Screen 2 of 10

Sammy: I have to get this projector rolling again. Then we'll hop into the role of cybersecurity in the Insider Threat Hub.

Cybersecurity plans, implements, upgrades, and monitors security measures for the protection of computer networks and information. Part of its mission includes ensuring that appropriate security controls are in place to safeguard digital files and responding to computer security breaches and viruses.

Oh, the thrills of using old technology. Could you hit the lights, I need a sec to fix this dinosaur.

Cybersecurity Role (cont.)
Screen 3 of 10

Sammy: Alright, now where were we… oh yeah, cybersecurity capabilities.

Specific cybersecurity capabilities include: focusing on technical requirements and incidents, developing countermeasures and monitoring systems, spotting indicators from User Activity Monitoring, or UAM, increasing UAM as permitted by the law, and implementing organization-wide changes to information system policies or configuration.

Screen text:
Cybersecurity Capabilities include:

- Focusing on technical requirements and incidents and their impact on the organization's mission
- Developing countermeasures and monitoring systems
- Responding to insider threat incidents
- Spotting indicators from User Activity Monitoring (UAM)
- Removing permissions and access to information systems
- Increasing UAM as permitted by law
- Implementing organization-wide changes to information system policies or configuration

Knowledge Check
Screen 4 of 10

Cybersecurity would perform which of the following tasks in an insider threat situation?

- o Refer an employee to the Employee Assistance Program
- o Increase security measures
- o Reassign an employee to another department

Knowledge Check
Screen 5 of 10

Which of the following is considered a cybersecurity capability?

- o Implementing changes to information system policies
- o Providing a behavioral analysis perspective
- o Arresting an insider threat perpetrator

Incident Reporting
Screen 6 of 10

Screen text: Mitigating the Threat
User Activity Monitoring (UAM)

Sammy: Now that you understand the cyber threats posed by trusted insiders, let's talk about effective means of mitigating the threat. All insider threat programs require UAM on classified systems in order to minimize the risk to those systems and identify potential risk indicators.

Logging, monitoring, and auditing of information system activities can lead to early discovery and mitigation of behaviors indicative of insider threat.

Insider threat policies require UAM on classified networks in support of insider threat programs for these policies.

Screen text:
Insider Threat Policies

- DoD Components under DoDD 5205.16
- Federal Agencies under E.O. 13587 and National Minimum Standards
- Cleared Industry under the NISPOM and associated Industrial Security Letters

Implementation from your organization must:

- Define what will be monitored
- Indicate how monitoring will be instituted
- Inform users of monitoring actions via banners
- Identify indicators that require review (e.g., trigger words, activities)
- Protect user activity monitoring methods and results
- Develop a process for verification and review of potential issues
- Establish referral and reporting procedures

Prevention Assistance Response (PAR)

Sammy: Implementation will be specific to your location, but all organizations must: define what will be monitored, indicate how monitoring will be instituted, inform users of monitoring actions via banners, identify indicators that require review, protect user activity monitoring methods and results, develop a process for verification and review of potential issues, establish referral and reporting procedures.

UAM plays a key role in prevention, assistance, and response, also known as PAR, to insider threats that manifest as the potential for harm to self or others. UAM helps identify users who are abusing their access and may be potential insider threats. This includes monitoring file activities, such as downloads which can identify abnormal user behaviors that may indicate a potential insider threat.

System Activity Monitoring will allow your program to identify possible system misuse. Activities to monitor include logons and logoffs and system restarts. Monitoring these activities identifies when the network is being accessed and whether someone is accessing or making changes to the root directory of a system or network. Organizations may find it challenging to maintain employee privacy while collecting data to establish a baseline. The collection, use, maintenance, and dissemination of information used to counter insider threats must comply with all applicable laws and policy issuances, including those regarding whistleblower, civil liberties, and privacy protections.

In addition to user activity monitoring requirements there are some basic cybersecurity best practices to consider. You should clearly document and consistently enforce policies, conduct periodic security awareness training, and implement strict password and account management policies. It's also important to enforce separation of duties and log, monitor, and audit employee online actions. Here's a document with a list of best practices that you can take with you.

Screen text: For more information see the CDSE course: INT260 Privacy and Civil Liberties in Insider Threat

Prevention and Detection Methods

- Enforce policies
- Conduct security awareness training
- Implement strict password
- Enforce separation of duties
- Monitor employees

User Activity Monitoring
Screen 7 of 10

Screen text:
Incident Reporting Policies:

- NISPOM, 1-301 (a&b)
- United States Codes
- National Security Presidential Directive
- Homeland Security Presidential Directive-7
- National Cyber Incident Response Plan
- Federal Information Security Management Act of 2002
- Directive 811 of the Intelligence Authorization Act of 1995

Sammy: Depending on the nature of the insider cyber threat incident, you may be required by law and regulations to report externally. These reports are in addition to the insider threat reporting requirements fulfilled under Insider Threat Program policy and may include reporting to: The FBI which has the authority and responsibility to investigate and enforce all violations of federal law that are not exclusively assigned to another federal agency. The Internet Crime Complaint Center or IC3, serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber-crime. Other incidents may require reporting and/or coordination with the U.S. Computer Emergency Readiness Team or Department of Homeland Security.

Consider whether your organization is obligated to report to the Defense Counterintelligence and Security Agency, FBI Cyber Division, the Internet Crime Complaint Center, U.S. Computer Emergency Readiness Team, or Department of Homeland Security. Work with legal counsel to ensure you understand the responsibilities for reporting certain insider cyber incidents.

Screen text: Cyber Incident Reporting Authorities:

- Investigate and enforce all violations not exclusively assigned to another federal agency
- Receive, develop and refer criminal complaints regarding cyber-crime

Knowledge Check
Screen 8 of 10

A traffic court clerk was able to modify the court's database to replace reported fines for individuals with a code indicating that there had been an error in data entry.

She also was able to modify money orders and checks to be payable to herself.

There were no business practices in place requiring supervisor approval for correcting a stated fine or to ensure integrity in the financial process.

The insider, who netted $1,800 for her illicit acts, was indicted on 15 counts of forgery, counterfeiting, embezzlement, wrongful conversion, and accessing a computer for fraud. She pled nolo contendere, was convicted, and received a five-year suspended sentence and five years' probation.

Which of the following practices for prevention and detection could have been implemented?

- Enforce separation of duties
- Log, monitor, and audit employee online actions
- Institute periodic security awareness training

Knowledge Check
Screen 9 of 10

A software developer worked for a subcontractor on a large government project. This insider, who had become disgruntled because of increased security measures, downloaded a password cracking program from the Internet, copied the government agency's password file to his Desktop, and executed the password cracker against it.

He successfully broke 40 out of 160 passwords, including the system administrator password. Unfortunately for him, he bragged about his knowledge of the system administrator password to the system administrator, who immediately reported the security breach.

An investigation ensued before the insider had a chance to use the passwords.

Which of the following prevention methods could have best mitigated this incident?

- Implement strict password policies
- Enforce separation of duties
- Perform threat analysis

Conclusion
Screen 10 of 10

Screen text: Learning Objectives

- ✓ Summarize the role of cybersecurity in an Insider Threat Hub
- ✓ Apply cybersecurity mitigation strategies posed by trusted insiders

Sammy: You've completed the Cybersecurity in Insider Threat Operations lesson. You should now be able to perform these tasks.

Course Conclusion

Screen 1 of 1

Course Summary

Screen text: Course Objectives

- ✓ Explain cyber insider threat and associated indicators
- ✓ Apply cybersecurity countermeasures to mitigate risk

Sammy: In this course we focused on cyber insider threat and how to prevent and mitigate these threats.

It's best said by James Comey, "The traditional notions of space and time and venue and border and my jurisdiction and your jurisdiction are blown away by a threat that moves at not 40 miles an hour or 50 downhill, but at 186,000 miles per second."

Cyber threats are becoming more prevalent and happening faster than before. It's vital for an organization to incorporate cybersecurity as part of a multi-disciplinary strategy to deter, detect, and mitigate risk associated with trusted insiders.

For more information refer to CDSE course INT201 "Developing a Multidisciplinary Insider Threat Capability."

Screen text: For more information refer to CDSE course INT201 "Developing a Multidisciplinary Insider Threat Capability."

Congratulations!
You have completed the Cyber Insider Threat course.

Practical Exercise

Screen 1 of 6

Practical Exercise Introduction

Screen text: Now that you have completed the Cyber Insider Threat course, it's time to compete the Practical Exercise.

Screen 2 of 6

Practical Exercise 1

Which of the following scenarios best describes a cyber insider threat?

- An employee was passed over for promotion, returned to work the next day, and fired shots throughout the entire first floor of the building.
- An employee downloaded a password cracking program from the Internet, copied the government agency's password file to his Desktop, and executed the password cracker against it.
- An employee stole blueprints from an agency to sell them to a foreign entity in Mexico.

Screen 3 of 6
Practical Exercise 2

The undercover agent paid Martin $11,500 in exchange for three packets of documents containing Secret and Top Secret information about current naval operations and intelligence assessments.

What risk is this most associated with?

- Espionage
- Sabotage
- Malware
- Fraud

Screen 4 of 6
Practical Exercise 3

An organization's employee changed positions to another department.

The department head allowed the employee to retain all existing permissions to the organization's servers. Using that access and his knowledge of the pervious department's security protocols; the employee intentionally increased his access to open and retrieve confidential personnel and payroll information which he was not authorized to obtain.

Cybersecurity would perform which of the following tasks in this insider threat situation?

- Provide legal guidance
- Interpret medical files
- Reassign the employee to another position
- Remove permissions and access

Screen 5 of 6
Practical Exercise 4

A system administrator, who was reprimanded for frequent tardiness, absence, and unavailability at work, inserted a logic bomb onto his employer's production servers and set it to be executed in two different ways. In an effort to conceal his actions, the insider deleted all records of his actions from all system and network logs, removed history files, and constructed the logic bomb to overwrite itself after execution. Fortunately for the organization, the logic bomb was detected prior to detonation.

Which of the following strategies could be used against this threat?

- Institute peer monitoring
- User Activity Monitoring
- Increase the employee's access
- Prevention Assistance Response

Screen 6 of 6
Practical Exercise 4
Conclusion

Screen text: Congratulations!
You've completed the Practical Exercise!
By completing this practical exercise you have successfully finished the course. Please select Next to Exit.

Answer Key

Introduction to Cyber Insider Threat

Knowledge Check
Screen 6 of 13

Criminals pose the most significant cyber risk because they can easily access the organization's system.

- True
- False

Answer: False

Knowledge Check
Screen 7 of 13

Cyber insider threat is an individual with authorized access who wittingly or unwittingly attempts to disrupt a computer network or system.

- True
- False

Answer: True

Knowledge Check
Screen 11 of 13

Three employees at a law firm managed to use Dropbox to transfer approximately 78,000 documents from their firm to their Dropbox account before abruptly quitting and moving on to another firm.

They then modified confidential client information on those documents in the Dropbox account and set their accounts to sync both ways so that faulty information would be transmitted back to the original employer's cache of documents.

The law firm is conducting business on faulty information which, of course, cost them their clients, who then went to the competitor.

What risks are most associated with this case? Select all that apply.

- Theft
- Fraud
- Workplace violence
- Sabotage

Answer: Theft, Sabotage

Knowledge Check
Screen 12 of 13

An employee used his access to the country's terrorist watch list to put his wife's name on it while she was out of the country. Her appeals fell on deaf ears for three years until her husband was on tap for promotion and his superiors ran a routine background check only to find out that the employee's wife was on the terrorist watch list. The employer saw her appeals and discovered the employees plot against his wife.

What type of cyber insider threat did the employee represent?

- Samaritan
- Machiavellian
- Avenger
- Career Thief

Answer: Machiavellian

Cybersecurity in Insider Threat Operations

Knowledge Check
Screen 4 of 10

Cybersecurity would perform which of the following tasks in an insider threat situation?

- Refer an employee to the Employee Assistance Program
- Monitor systems
- Reassign an employee to another department

Answer: Monitor systems

Knowledge Check
Screen 5 of 10

Which of the following is considered a cybersecurity capability?

- Implementing changes to information system policies
- Providing a behavioral analysis perspective
- Arresting an insider threat perpetrator

Answer: Implementing changes to information system policies

Knowledge Check
Screen 8 of 10

A traffic court clerk was able to modify the court's database to replace reported fines for individuals with a code indicating that there had been an error in data entry.

She also was able to modify money orders and checks to be payable to herself.

There were no business practices in place requiring supervisor approval for correcting a stated fine or to ensure integrity in the financial process.

The insider, who netted $1,800 for her illicit acts, was indicted on 15 counts of forgery, counterfeiting, embezzlement, wrongful conversion, and accessing a computer for fraud. She pled nolo contendere, was convicted, and received a five-year suspended sentence and five years' probation.

Which of the following practices for prevention and detection could have been implemented? Select all that apply.

- Enforce separation of duties
- Log, monitor, and audit employee online actions
- Institute periodic security awareness training

Answer: All answers correct.

Knowledge Check
Screen 9 of 10

A software developer worked for a subcontractor on a large government project. This insider, who had become disgruntled because of increased security measures, downloaded a password cracking program from the Internet, copied the government agency's password file to his Desktop, and executed the password cracker against it.

He successfully broke 40 out of 160 passwords, including the system administrator password. Unfortunately for him, he bragged about his knowledge of the system administrator password to the system administrator, who immediately reported the security breach.

An investigation ensued before the insider had a chance to use the passwords.

Which of the following prevention methods could have best mitigated this incident?

- Implement strict password policies
- Enforce separation of duties
- Perform threat analysis

Answer: Implement strict password policies

Practical Exercise

Practical Exercise 1
Screen 2 of 6

Which of the following scenarios best describes a cyber insider threat?

- An employee was passed over for promotion, returned to work the next day, and fired shots throughout the entire first floor of the building.
- An employee downloaded a password cracking program from the Internet, copied the government agency's password file to his Desktop, and executed the password cracker against it.
- An employee stole blueprints from an agency to sell them to a foreign entity in Mexico.

Answer: An employee downloaded a password cracking program from the Internet, copied the government agency's password file to his Desktop, and executed the password cracker against it.

Practical Exercise 2
Screen 3 of 6

The undercover agent paid Martin $11,500 in exchange for three packets of documents containing Secret and Top Secret information about current naval operations and intelligence assessments.

What risk is this most associated with?

- Espionage
- Sabotage
- Malware
- Fraud

Answer: Espionage

Practical Exercise 3
Screen 4 of 6

An organization's employee changed positions to another department.

The department head allowed the employee to retain all existing permissions to the organization's servers. Using that access and his knowledge of the pervious department's security protocols; the employee intentionally increased his access to open and retrieve confidential personnel and payroll information which he was not authorized to obtain.

Cybersecurity would perform which of the following tasks in this insider threat situation?

- Provide legal guidance

- Interpret medical files
- Reassign the employee to another position
- Remove permissions and access

Answer: Remove permissions and access

Practical Exercise 4
Screen 5 of 6

A system administrator, who was reprimanded for frequent tardiness, absence, and unavailability at work, inserted a logic bomb onto his employer's production servers and set it to be executed in two different ways. In an effort to conceal his actions, the insider deleted all records of his actions from all system and network logs, removed history files, and constructed the logic bomb to overwrite itself after execution. Fortunately for the organization, the logic bomb was detected prior to detonation.

Which of the following strategies could be used against this threat?

- Institute peer monitoring
- User Activity Monitoring
- Increase the employee's access
- Prevention Assistance Response

Answer: User Activity Monitoring