

## **Student Guide**

# **Critical Thinking for Insider Threat Analysts**

---

### **CDSE Video – Screen 1 of 2**

CDSE Center for Development of Security Excellence Learn. Perform. Protect.

### **Course Menu – Screen 2 of 2**

Course Introduction, Thinking for Insider Threat Analysts, Analytic Standards, Critical Thinking Tools, and Course Conclusion.

## **Course Introduction**

### **Why Critical Thinking? - Screen 1 of 2**

Screen text: You can't make good decisions unless you have good information and can separate facts from opinion and speculation. Facts are verified information, which is then presented as objective reality.

Narrator: General Colin Powell once wrote: You can't make good decisions unless you have good information and can separate facts from opinion and speculation. Facts are verified information, which is then presented as objective reality. The question is the verified. How do you verify verified?

Narrator: Critical thinking addresses General Powell's challenging question because it involves actively and skillfully analyzing and evaluating information. Thinking critically is your way of verifying and making sense of information. It eventually leads you to crafting your assumptions and judgements for analytic products.

### **Learning Objectives - Screen 2 of 2**

Screen text: Critical Thinking for Insider Threat Analysts

Screen text: Course Objectives

- Demonstrate an understanding of critical and analytic thinking as it relates to Insider Threat Analysts
- Identify the analytic standards, to include analytic tradecraft, that apply to analysis and the development of a comprehensive analytic product
- Select critical thinking tools most appropriate to develop a sound and comprehensive insider threat analytic product

Narrator: Welcome to the Critical Thinking for Insider Threat Analysts course. This course provides a high-level explanation of analytical and critical thinking and how it relates to producing comprehensive analytic products for your insider threat program.

Narrator: During this course, you will gain a broad understanding of critical thinking, analytic thinking, and intellectual standards; learn about analytic standards and analytic tradecraft; and be introduced to critical thinking tools and their use in creating a comprehensive analysis.

## **Thinking for Insider Threat Analysts Lesson**

### **Lesson Objectives - Screen 1 of 16**

Screen text: Insider Threat

- Gather
- Integrate
- Review
- Assess
- Respond

Screen text: Lesson Objectives:

- Contrast critical and analytic thinking
- Recognize the eight elements of thought
- Identify the nine intellectual standards and their relationship to analytic thinking
- Relate critical and analytic thinking to an Insider Threat Analyst's role
- Recognize challenges to applying reasoning skills
- Recognize common analytic mistakes

Narrator: The insider threat program is designed to deter, detect, and mitigate risks from trusted insiders. As an insider threat analyst, you are required to gather, integrate, review, assess, and respond to information from a variety of sources. This information integration and analysis requires both analytical and critical thinking.

Narrator: In this lesson, you'll be introduced to critical and analytic thinking, the elements of thought, and intellectual standards. This lesson will also relate critical and analytic thinking to your role as an Insider Threat Analyst, identify analytical challenges, and identify common analytic mistakes. Take a moment to review the lesson learning objectives.

### **Thinking for Insider Threat Analysts Introduction - Screen 2 of 16**

Screen text: Analytic thinking and critical thinking are similar but each has specific standards and practices. In this lesson, you'll be introduced to critical and analytic thinking, the elements of thought, and intellectual standards.

Screen text:

- Critical Thinking
- Analytic Thinking

Narrator: Analytic thinking and critical thinking are similar but each has specific standards and practices. In this lesson, you'll be introduced to critical and analytic thinking, the elements of thought, and intellectual standards.

So, it's important that you understand both of these tactics and the vital roles they play in your analysis.

### **What is Critical Thinking? - Screen 1 of 1**

Screen text: Critical Thinking involves:

1. Gathering relevant information
2. Evaluating information for accuracy and currency
3. Asking questions
4. Assessing bias or unsubstantiated assumptions
5. Interpreting and making inferences from the information
6. Formulating ideas theories
7. Weighing opinions, arguments, or solutions against criteria
8. Considering alternative possibilities
9. Testing conclusions to verify that evidence supports the conclusions
10. Making judgements

Narrator: Critical thinking is the objective analysis and evaluation of information to form a judgment. Critical thinking involves gathering all relevant information and evaluating the information to determine how to best interpret it. You will evaluate the information by asking questions, assessing value such as bias and unsubstantiated assumptions, using abstract ideas to interpret information, and making inferences. You will then use the results of your evaluation to formulate ideas and theories; weigh opinions, arguments, or solutions against criteria; consider alternative possibilities and form a clear line of reasoning through to conclusions. Finally, test your conclusions to verify that evidence supports your conclusions and then make your judgment.

### **What is Analytic Thinking? - Screen 1 of 1**

Screen text: Analytical Thinking involves:

1. Gathering and organizing relevant information
2. Separating more complex information into smaller parts
3. Focusing on facts and evidence
4. Using logic and reasoning to process information
5. Identifying key issues

6. Finding patterns and recognizing trends
7. Identify cause and effect
8. Understanding connections and relationships
9. Eliminating extraneous information
10. Drawing appropriate conclusions

Narrator: Analytic thinking is the systematic examination of information to identify significant facts and draw conclusions. Analytic thinking involves gathering and organizing relevant information in order to reach a conclusion. During Analytic thinking, you will break down complex information into smaller, manageable parts and examine each part to understand the facts and evidence. Use logic and reasoning to process the information and look for key issues. Search for patterns, trends, and cause and effect. Strive to understand connections and relations between the parts of information and eliminate extraneous information. Finally, you will draw appropriate conclusions from the information in order to arrive at appropriate solutions.

### **How is Critical Thinking Different from Analytical Thinking? - Screen 3 of 16**

Screen text:

Analytical Thinking

- Breaking down complex information into smaller parts
- More linear and systematic breakdown of information
- Use facts within the information gathered to support your conclusion

Critical Thinking

- Taking outside knowledge, including your personal knowledge and experience, into account while evaluating information
- More holistic as it seeks to assess, question, verify, infer, interpret, and formulate
- Taking other information to make a judgment or formulate innovative solutions
- Make a judgment based on your opinion formed by evaluating various sources of information including your own knowledge and experiences

Critical thinking – Judgment Based

Analytical Thinking – Fact Based

Narrator: Analytical thinking involves breaking down complex information into smaller parts while critical thinking involves taking outside knowledge, including your personal knowledge and experience, into account while evaluating information. Analytical thinking is more linear and systematic breakdown of information. Critical thinking is more holistic as it seeks to assess, question, verify, infer, interpret, and formulate. Analytical thinking can be considered a step in the critical thinking process. When you have a complex problem to solve, you would want to use your analytical skills before your critical thinking skills. Critical thinking does involve breaking down information into parts and analyzing the parts in a logical, systematic manner. However, it also involves taking other information to make a judgment or formulate innovative solutions. Additionally, with analytical thinking, you use facts within the information gathered to support your conclusion. Conversely, with critical thinking, you make a judgment based on your opinion formed by evaluating various sources of information including your own knowledge and experiences.

### **The Reasoning Process and Analysis - Screen 4 of 16**

Screen text:

- Why is the analysis of thinking important?
- Misthinking is costly

Examples of Misthinking

- missing information
- incorrect assumption or conclusion
- misinterpretation

Narrator: As an insider threat analyst, you will gather data, analyze it, and apply critical and analytic thinking to assess it. You may be called upon to create analytic products in support of your program. These can include informational reports, incident reports, decision papers, and/or contributions to after action reports, or damage assessments. In addition, you will be responsible for making recommendations on policy and procedures for the deterrence, detection, and mitigation of potential insider threats.

Narrator: These tasks require complex thought and reasoning. It is important to understand thinking and its components to avoid misthinking. Misthinking is a mistaken or improper thought or opinion. Misthinking can be costly in terms of money, time, and national security and can adversely affect outcomes of insider threat program actions. But, if we intentionally consider the thinking process, we can prevent or mitigate those adverse consequences.

### **The Reasoning Process and Analysis - Screen 5 of 16**

Screen text: Purpose: All reasoning has a purpose. State it clearly, make it realistic, and distinguish it from related purposes.

Problem/Question: In your attempt to solve the problem or answer a question, define the problem. State the question clearly and precisely. Ask the question in several ways to help define its meaning and scope. Consider whether the answer to your question involves definitive answers versus matters of opinions or whether you need to consider multiple viewpoints.

**Information:** Gather information to answer your question. Your data, information, evidence should be clear, accurate, and relevant. Gather enough evidence to support your claims. Look for information that both supports AND opposes your claims.

**Concepts:** All reasoning is shaped by and expressed through concepts and ideas. Identify key concepts and clearly explain them. Consider alternative definitions of concepts and alternative concepts.

**Interpretation/Inference:** Reasoning always contains inferences/interpretations that lead to conclusions. Be aware of your inferences and check them for consistency. Identify assumptions that could be influencing your inferences.

**Assumptions:** Assumptions will shape your point of view. Clearly identify your expectations and determine if they are warranted and defensible.

**Point of View:** Examine your point of view. Endeavor to be impartial and seek other points of view, looking at the strengths and weaknesses, and objectivity of each of them.

**Implications/Consequences:** Your reasoning leads to implications and consequences. Consider all possible implications and consequences, searching for both the negative and positive ones.

**Narrator:** The thought process naturally consists of eight basic structures or elements, each of which bears equal weight. All reasoning is tied to these elements of human thought. The elements of thought are purpose, problem or question, information, interpretation and inference, concepts, assumptions, point of view, and implications or consequences. By applying the elements of thought to our analytic thinking, a problem can be broken down into multiple parts. This close, detailed examination of information will identify causes, key factors, and possible solutions. The analytic thought process sounds simple enough, but it takes practice to apply these elements with conscious intent. Having a checklist for reasoning can be helpful. Select each element to learn more about improving your analytic thought process.

### **Intellectual Standards for Analysts – Screen 6 of 16**

Screen text: Intellectual Standards

Standards to assess logic of your mind to the thing to be understood

Logic – a system of reasoning, a means of figuring something out (the elements of thought)

**Narrator:** It's important to use the elements of thought with sensitivity to intellectual standards. Intellectual standards assess whether the logic, that is, the system of reasoning, in your mind mirrors the logic in the thing to be understood. There are nine intellectual standards. They are clarity, accuracy, precision, relevance, depth, breadth, logic, significance, and fairness. The application of intellectual standards to your reasoning naturally improves your analytic skills. Strive to apply the intellectual standards throughout your reasoning process. To think critically requires a command of these standards. Select each tab to learn more about intellectual standards.

### **Clarity – Screen 1 of 1**

Screen text: Clarity - Understandable, the meaning can be grasped.

- Could you elaborate further?
- Could you give an example?
- Could you illustrate what you mean?

Narrator: The question "What can be done about insider threats in America?" lacks clarity. However, a question such as "How can our organization identify potentially risky behavior by employees?" provides a clearer message and something specific to resolve. Purpose, point of view, concepts and ideas, inferences, assumptions, implications, and consequences all benefit from clarity—whether for your understanding or others'. To achieve the clarity intellectual standard, you could ask questions that seek additional details.

### **Accuracy – Screen 1 of 1**

Screen text: Accuracy – Free from errors or distortions, true

- How could we check on that?
- How could we find out if that is true?
- How could we verify or test that?

Narrator: A statement can be clear but inaccurate. "The sun is purple" is a clear statement but not an accurate one. Accuracy refers to truthfulness and error-free content. Thus, information or data related to the problem should be factual, and your search for factual information should be thorough and detailed. When evaluating accuracy, you could ask questions about how to check on or verify the information presented.

### **Precision – Screen 1 of 1**

Screen text: Precision - Exact to the necessary level of detail

- Could you be more specific?
- Could you give me more details?
- Could you be more exact?

Narrator: The standard of precision relates to the necessary level of detail. A statement can be accurate and clear but may not be precise. For example, the statement "The car is heavy" is accurate and clear, but not precise. Ask questions that probe for more details and specifics.

### **Relevance – Screen 1 of 1**

Screen text: Relevance - Relating to the matter at hand

- How does that relate to the problem?
- How does that bear on the question?
- How does that help with the issue?

Narrator: Information related to the analysis or problem shouldn't only be accurate and precise, but also relevant. Question how information relates to the problem. Determining the degree of relevance helps you sort the major factors from the lesser ones.

### **Depth - Screen 1 of 1**

Screen text: Depth - Containing complexities and multiple interrelationships

- What factors make this a difficult problem?
- What are some of the complexities of this question?
- What are some of the difficulties we need to deal with?

Narrator: When you examine a question, issue, data, or possible solution, applying depth to your analysis will help ensure that you've exhausted the matter at hand. Treating an issue superficially fails to deal with complexities. You can ask a variety of questions relating to depth, such as inquiring about the complexities and difficulties related to the problem.

### **Breadth - Screen 1 of 1**

Screen text: Breadth - Encompassing multiple viewpoints

- Do we need to look at this from another perspective?
- Do we need to consider another point of view?
- Do we need to look at this in other ways?

Narrator: Breadth is another intellectual standard that ensures your reasoning has covered its bases. This standard confirms that your reasoning considered multiple perspectives and viewpoints. For example, one political party's standpoint may be accurate, precise, relevant, and deep, but will not have breadth because it encompasses one point of view. To ensure your reasoning has breadth, ask questions about others' perspectives and points of view.

### **Logic - Screen 1 of 1**

Screen text: Logic - The parts that make sense together, no contradictions

- Does all this make sense together?
- Are there flaws in this reasoning?
- Does your first paragraph fit with your last?
- Does what you saw follow the evidence?

Narrator: Logic determines whether the reasoning process makes sense. If something isn't making sense to you, it may be an indication of flawed logic. Here are some questions that probe the logic of your reasoning.



## **Significance - Screen 1 of 1**

Standards to assess logic of your mind to the thing to be understood

Logic – a system of reasoning, a means of figuring something out (the elements of thought)

Screen text: Significance - Focusing on the important and not the trivial

- Is this the most important problem to consider?
- Is this the central idea to focus on?
- Which of these facts are most important?

Narrator: Similar to Relevance, the Significance standard evaluates facts and ideas in terms of their pertinence and weight. The significance standard applies to many aspects of reasoning: the problem, facts, solution, and/or ideas. You can weigh the significance of the problem, facts, solution, or ideas by asking questions relating to their importance.

## **Fairness - Screen 1 of 1**

Screen text: Fairness - Justifiable, not self-serving, or one-sided

- Do I have any vested interest in this issue?
- Am I sympathetically representing the viewpoints of others?

Narrator: The Fairness standard requires active effort to consider the rights and needs of others as well as your own. Check the fairness of your reasoning by questioning your motives and asking yourself whether you sympathetically represented others' viewpoints.

## **Analysis on the Job - 7 of 16**

Screen text: Gathering data, Analyzing data, Providing assessments, Producing products.

Screen text: Insider Threat Analysts:

- Conduct comprehensive all-source research to gather data
- Aggregate, analyze, and evaluate data
- Identify trends and patterns in data
- Extract and organize facts, evidence, and issues into intelligence products
- Summarize issues, patterns, and trends
- Recommend courses of action

With analytic products to:

- Inform
- Advise
- Provide Subject Matter Expertise
- Provide Direct Support

Narrator: Insider Threat Analysts are responsible for gathering data, analyzing the data, providing assessments of threats and vulnerabilities, and producing analytic products to support leadership decisions.

Narrator: In order to become competent in this role, analysts must have the ability to conduct comprehensive all-source research to gather data; aggregate, analyze, and evaluate data; identify trends and patterns in data; extract and organize facts, evidence, and issues into intelligence products; summarize issues, patterns, and trends; and recommend courses of action. To fulfill these responsibilities, you will need to apply the analytic and critical thinking processes along with using critical thinking tools. Applying critical and analytic thinking will help you produce analytic products that inform the team of insider threat incidents; provide sound advice to leadership that can facilitate their review, response, and resolution of insider threat incidents; and provide subject matter expertise and direct support to the insider threat program in matters related to potential insider threats.

### **Knowledge Check Activity - Thinking for Insider Threat Analysts – Screen 8 of 16**

Your job as an insider threat analyst includes gathering data, analyzing it, and applying critical thinking to assess it.

- True
- False

The thought process consists of eight elements that can be applied to analytical thinking. Which of the following can be identified by applying these elements?

- Possible causes
- Timely analysis
- Possible solutions
- Key factors

Which intellectual standard are you complying with if you are examining the complexity of the problem or the various factors causing a problem to be difficult?

- Breadth
- Depth
- Significance
- Relevance

### **Defense Assembly Agency Scenario - Screen 9 of 16**

Narrator: Let's get acquainted with the Defense Assembly Agency. We will use this scenario to help you better understand the concepts associated with critical thinking as an Insider Threat Analyst. The Defense Assembly Agency builds computer systems to mission specifications for organizations within the agency. Eighteen months ago, the agency began supporting organizations outside of its agency. With significant new additions to the agency's mission and workload, Defense Assembly Agency was able to hire additional people.

Narrator: Chris, the agency director, and Caroline, the assistant director, recognized the need for qualified personnel. Lance was hired to replace the lead system administrator, because of his education and experience. James was hired as a junior system administrator to share the growing systems administration workload and responsibilities with Ian, one of the agencies original employees and who had built the original system from the ground up. Productivity was high, but personnel problems began to plague the agency. After numerous complaints about Ian's behavior management considered terminating him but took no action. None of Ian's behaviors were reported to the Insider Threat Team.

Narrator: Thereafter, Caroline discovered that something wiped out their entire system configuration and operational tools, and she cannot locate the backups. Caroline suspects this incident might be sabotage and an insider job. She talked to two employees about the situation and then reported the matter to the insider threat team.

Employee 1: We were one lean operating machine. We had to extend the systems to support our new mission area. Ian thought of and implemented the idea to centralize the agency's core functions on a central server to coordinate operations more efficiently. We made vast improvements to the flexibility and sophistication of the supporting operational tools and software programs over a very short period. The extensions worked well with very few glitches. Of course, we had to cut some corners, giving people access when and where they needed it to make things happen. If something did not contribute to extending the systems, it just did not seem worth doing. This was how we were able to accomplish as much as we did.

Screen text: We were one lean operating machine. We had to extend the systems to support our new mission area. Ian thought of and implemented the idea to centralize the agency's core functions on a central server to coordinate operations more efficiently. We made vast improvements to the flexibility and sophistication of the supporting operational tools and software programs over a very short period. The extensions worked well with very few glitches. Of course, we had to cut some corners, giving people access when and where they needed it to make things happen. If something did not contribute to extending the systems, it just did not seem worth doing. This was how we were able to accomplish as much as we did.

Employee 2: That's right. The entire staff adopted a "do whatever it takes" attitude to their job in order to keep up with the demands placed on us due to the growth. We only had one Systems Administrator at that time, but we got everything done.

Screen text: That's right. The entire staff adopted a "do whatever it takes" attitude to their job in order to keep up with the demands placed on us due to the growth. We only had one Systems Administrator at that time, but we got everything done.

### **Defense Assembly Agency Scenario Exercise 1 – Screen 10 of 16**

Screen text: Given this information on the Defense Assembly Agency, what is the first step you should take in the reasoning process?

- Address implications
- Brainstorm who is the culprit and the motivation
- Define the problem
- Gather information

Which intellectual standards should you apply as you begin your analysis of the situation at the Defense Assembly Agency?

- Logic
- Point of view
- Assumptions
- Relevance

Continue thinking about applying the intellectual standards to this situation.

You have statements from two managers and two employees that relate the state of the work environment. Do these statements provide enough information for you to begin your analysis of the problem? Why or why not?

- Yes, because the information that you have covers all points of view.
- Yes, because the statements are relevant.
- No, because the current statements do not provide depth and breadth of the situation.
- No, because problem analysis requires you to interview all members of the staff regardless of their knowledge or level of involvement in the situation.

As you begin your analysis of the problem, you determine that you should direct your focus specifically on employee access to the agency's server. This focus is an example of complying as with which of the following intellectual standards?

- Accuracy
- Clarity
- Precision
- Significance

### **Challenges to Applying Reasoning Skills – Screen 11 of 16**

Narrator: When using analytical and critical thinking skills to develop analytic products for the Insider Threat Program, it's important to understand that the brain's natural inclinations may pose challenges to our reasoning skills. Select each tab to learn more about these natural thinking processes and means of overcoming them.

Screen text:

1. Emotional Thinking
2. Mental Shortcuts
3. Seeing Patterns
4. Biases and Assumptions
5. Subconscious Explanations

Screen Text: 1. Emotional Thinking - Emotions affect nearly every thought and decision we make.

Attempt to overcome the emotional factor.

- Avoid decision making when your emotions are high.
- Always check your emotions when making a decision.

Narrator: First, we're emotional beings and emotions influence nearly every thought and decision we make. Even subtle emotions play into our decisions. You dread writing a report and thus you delay writing it. Or you feel elated because of some good news and sign off on something without really digesting the material. How do you combat this natural inclination? First, avoid decision making when your emotions are high. Second, always check your emotions when making a decision.

Screen text: 2. Mental Shortcuts - Our brains innately and continuously take unconscious mental shortcuts—similar to computer subroutines.

- Reflexive actions such as catching a ball
- Preconceived conclusions
- Intuition
- Prejudice
- Stereotyping
- Jumping to conclusions

Narrator: Another natural mental process is our brain's innate ability to make mental shortcuts. Much like a computer's subroutines running in the background, the brain's vast neural network reacts to, recalls, and links everything it senses. Because this is an innate process, it's bound to occur. Recognizing this process can allow you to consider it and overcome the influence it may have on your analysis.

Screen text: 3. Seeing Patterns - Human brains are wired to see the world in terms of patterns.

The problems of innate pattern-seeking:

- When a pattern is detected, the brain is disinclined to consider alternatives.
- When no pattern is obvious, we may perceive relationships where none exists.

Narrator: All that neural connecting leads us to being wired to seeing the world in terms of patterns. Our brains compulsively look for patterns in faces, situations, and sequences of events—and we only need a fragment of a pattern to retrieve the whole pattern from memory. The compulsion is so strong, that when a pattern is detected, the brain is disinclined to consider alternatives. You may not want to believe that a trusted co-worker has sold classified information to a foreign government because this fact doesn't fit the pattern you've developed for this person. Patterning can cause us to perceive relationships where none exists. For example, stereotyping is a form of patterning. The brain ascribes additional attributes of one thing to other things in its effort to find a pattern.

Screen text: 4. Biases and Assumptions - Humans instinctively depend upon and are susceptible to biases and assumptions.

We give high value to that which is consistent with our own biases and low value to that which is inconsistent with our biases.

A collection of biases creates mind-sets that can preclude our ability to see a different perspective or take in new information.

Narrator: The brain's natural ability to make connections and see patterns means we're susceptible to biases and assumptions. The positive aspect of this trait is that it saves our brain time and work from rethinking. However, biases can lead one astray because the mind doesn't rigorously test the logic of every new piece of information it receives. The desire to seek patterns means that we tend to give high value to that which is consistent with our own biases and low value to that which is inconsistent with our biases. A collection of biases creates a mind-set. Mind-sets preclude our ability to view other perspectives or take in new information. For example, your favorable or unfavorable mind-set about a political party may make it hard for you to accept information contrary to your personal view.

Screen text: Subconscious Explanations - Humans compulsively explain things—regardless of the explanation's accuracy.

Narrator: There is another part of that thinking process related to patterns. People are compelled to explain things to themselves or others whether or not that explanation is accurate. The brain subconsciously fills in missing information. The noise? Must be the cat. That smoke? Must be from down the street.

The problem with the brain's ready explanation for events is that the ready solution may not be accurate. Instead, the noise might be a burglar, and that smoke might actually be a fire in your garage. Even though we're mentally equipped for problem solving, the equipment can pose as many problem-solving challenges as solutions.

More information can be found in the Course Resources.

### **Habitual Analytic Wrongdoings – Screen 12 of 16**

Narrator: Understanding common analytic mistakes can help us become more efficient and more accurate with our analytic products. Our brains often trick us by leaning toward easy solutions, patterns, and biases. Awareness of potential analytic problems at the beginning of the process may prevent mistakes. Select each one for more information.

Screen text: Common Analytic Mistakes

- Beginning the analysis by forming a conclusion first
  - Your conclusion should be at the END of the analytic process. Starting with a preconceived conclusion inhibits your ability to accept other solutions or draw other conclusions.
- Focusing on a solution that we intuitively favor
  - When you favor one solution over another, you tend to give inadequate attention to other solutions. The solution we favor may not be the best solution.

- Focusing on a satisfactory solution
  - The solution we favor is usually the first one we find satisfactory. Perhaps it's the easiest solution or the one that best mirrors our personal biases, but it may not be the best solution. Explore all alternatives.
- Confusing hard thinking and discussion with analysis
  - Thinking hard and group discussions do not equate to analysis. These activities can be useful but are not a substitute for the true work of analysis. Be sure to follow analytic standards and analytic tradecraft to avoid this problem.
- Failing to use the process of the analysis
  - Failing to use the process of the analysis wastes time and energy and yields less than satisfactory results.
- Not structuring the analysis of a problem
  - Unstructured analysis lacks open-mindedness, often ends up with the satisfactory solution, does not weigh all alternatives, and produces flawed or less effective solutions.

### **Some Insights into Analytical Problem Solving – Screen 13 of 16**

Narrator: Morgan D. Jones, a former CIA analyst who has written extensively on the subject of analysis and critical thinking, provides three elements for effective analytical problem solving.

Screen text: Effective Analytical Problem Solving - 3 ELEMENTS FOR EFFECTIVE ANALYTICAL PROBLEM SOLVING

1. Organize and structure your analysis
2. Apply convergent AND divergent thinking to the analysis process
3. Be wary of basing conclusions largely on judgment instead of fact

Screen text: 1. Organize and structure your analysis.

Structure:

- Creates analytic empowerment of the group
- Focuses the group's attention on individual aspects of the problem
- Helps the group perceive the problem in full

Narrator: First: Organize and structure your analysis.

Most likely, your analysis will be all or in part a group effort. While the group collectively can be analytically empowered, it can also offer challenges, such as conflicts over who is in authority, cliques, and individual mindsets. Structure not only focuses attention on individual aspects of a problem and helps the group perceive the problem in full, structure minimizes those less-than-helpful group interactions.

Screen text: 2. Apply convergent AND divergent thinking to the analysis process.

Convergent thinking

- Takes a narrow view
- Focuses on a single aspect

- Moves toward one point to produce a single solution

Benefit: Eliminates the weak alternatives and chooses the strong one from among them.

Divergent thinking

- Takes a broader view
- Encompasses alternative solutions

Benefit: Encourages creative thinking—opens the mind to new ideas, alternatives.

“If we are to solve problems ... we must learn how to identify and break out of restrictive mindsets and give full, serious consideration to alternative solutions. ... Failure to consider alternatives fully is the most common cause of flawed or incomplete analysis.” – Morgan D. Jones, CIA analyst

Narrator: Second: Apply convergent AND divergent thinking to the analysis process. Convergent thinking eliminates weak alternatives and permits focus on a single solution or idea. However, you need to also use divergent thinking—that broad view that looks at alternatives and explores creative solutions and ideas. In, *The Thinker’s Toolkit*, Jones discusses the necessity to break out of restrictive mindsets when trying to solve problems. Jones writes, “Failure to consider alternatives fully is the most common cause of flawed or incomplete analysis.”

Screen text: 3. Be wary of basing conclusions largely on judgment instead of fact.

Judgment is required when data is missing or incomplete.

There’s a correlation between the role of judgment and the probability of error.

Use language that accurately expresses your degree of confidence.

Narrator: Third: Be wary of basing conclusions largely on judgement instead of fact. No doubt, you will frequently find you don’t have all the facts or data you need to solve a problem. That’s where judgement comes into play. There’s a correlation between the role of judgment and the probability of error. Qualify your judgments based on probability. Those who make decisions based on your analysis need you to use language that accurately expresses your degree of confidence.

### **Defense Assembly Agency Scenario - Part 2 – Screen 14 of 16**

Narrator: Let's return to the Defense Assembly Agency Scenario.

Screen text: You have seen the Lead Systems Administrator, Lance, in the hallway a couple of times. He never smiles or speaks and seems standoffish in your opinion. If you consider this observation in your analysis of the information around this situation, you could make which of the following analytic wrongdoing mistakes? Select all that apply.

- Focusing on a solution that you may intuitively favor
- Beginning the analysis by forming a conclusion first



- Failing to use the process of analysis
- Not structuring the analysis as a problem

Chris came to your office and told you that he thinks this situation may have been an error by the trainee, Michael. The other members of the IT team could not have made such a mistake and they are loyal employees.

If you consider Chris' opinion in your analysis, you could make which of the following analytic wrongdoing mistakes?

- Focusing on a satisfactory solution.
- Focusing on a solution that you may intuitively favor
- Over analyzing the situation
- Not structuring the analysis as a problem

### Knowledge Check Activity 2 – Screen 15 of 16

Screen text: Question 1 of 4: The analytic products that you create should demonstrate your use of \_\_\_\_\_.

- Analyst Notebook
- The reasoning process
- Exhaustive intelligence
- Empowered thinking

Question 2 of 4: In your role as an insider threat analyst, what functions will the analytic products you create serve? Select all that apply.

- Inform
- Advise
- Provide subject matter expertise
- Create policy
- Provide direct support

Question 3 of 4: Create a checklist about the natural thinking processes that can interfere with the analytic process by selecting the items to go on the list. When you have finished creating the checklist, select Submit.

#### Natural Thinking Processes that Interfere with Analytical Thinking

- Biases and assumptions
- Clinging to untrue beliefs in the face of contrary evidence
- Compulsive explaining regardless of accuracy
- Emotional response
- Lack of information to process

- Overwhelming amounts of information to process
- Over-readiness to accept other ideas
- Preference for evidence supporting our belief system
- Subconscious mental shortcuts
- Subconscious pattern seeking
- Preference for evidence supporting our belief system

Question 4 of 4: You and another analyst have collaborated to work on a potential insider threat situation. Your partner suggests a solution, but your initial reaction is to prefer your own idea. The more you think about it the better your idea seems.

Which natural thinking process is happening here? Select all that apply.

- Emotional reaction
- Mental shortcuts
- Relying on biases and assumptions
- Patterning
- Compulsive explaining
- Attaching importance to evidence that supports your beliefs and judgments while dismissing or devaluing evidence that does not

### **Thinking for Insider Threat Analysts Summary – Screen 16 of 16**

Narrator: This concludes the lesson Thinking for Insider Threat Analysts. This lesson contrasted critical and analytical thinking; recognized the eight elements of thought; identified the nine intellectual standards and their relationship to analytic thinking; related critical and analytic thinking to an insider threat analyst's role; recognized intelligent analytical challenges; and recognized common analytic mistakes. There are numerous sources of information on critical thinking and reasoning. Some of this information has been compiled and is available for you in the resources tab. You can locate your Resources at any time by selecting the Menu.

Screen text: Lesson Objectives

- Contrast critical and analytic thinking
- Recognize the eight elements of thought
- Identify the nine intellectual standards and their relationship to analytic thinking
- Relate critical and analytic thinking to an insider threat analyst's role
- Recognize challenges to applying reasoning skills
- Recognize common analytic mistakes

## Analytic Standards Lesson

### Analytic Standards Introduction – Screen 1 of 9

Narrator: Analytic standards have been developed to professionalize analytic tradecraft and improve the analysis process and resulting analytic products. In this lesson we will review the Analytic Standards and elements of analytic tradecraft. Take a moment to review the lesson learning objectives.

Screen text: Lesson Objectives:

- Explain the purpose of the analytic standards.
- Describe the five analytic standards and how to use them to support the deterrence, detection, and mitigation of insider risk.
- Describe the nine elements of analytic tradecraft.
- Identify challenges to the accuracy and reliability.

### A National Directive for Analytic Standards – Screen 2 of 9

Narrator: Your insider threat team will require comprehensive analytic products to deter, detect, and mitigate insider risk. The products required will vary from day to day and situation to situation, but all must adhere to accepted analytic standards.

Narrator: The Director of National Intelligence issued Intelligence Community Directive 203, also known as ICD 203, to improve the quality of intelligence analysis and production by adhering to specific analytic standards. While the directive applies specifically to members of the intelligence community, anyone performing insider threat analysis tasks in any organization can look to this directive for best practices and accepted standards.

Narrator: Specifically, ICD 203, Analytic Standards, articulates that intelligence analysts must strive for excellence, integrity, and rigor in their analytic thinking and work practices. Protection of workforce privacy and civil liberties is a key element of insider threat programs. ICD 203 promotes the protection of privacy and civil liberties by ensuring objectivity, timeliness, relevance, and accuracy of personally identifiable information, or PII, in analytic products.

Screen text:

Purpose

- Establishes the official Intelligence Community (IC) Analytic Standards that govern the production and evaluation of analytic products
- Articulates analysts' responsibilities:
  - Excellence
  - Integrity
  - Rigor
- Calls for including personally identifiable information (PII) in analytic products only if it:
  - Relates to a specific analytic purpose

- Is consistent with the IC element missions
- Is in compliance with IC element regulation and policy

### **The Five Analytic Standards – Screen 3 of 9**

Narrator: Five analytic standards outlined in ICD 203 guide analysis and production. It is a best practice that Insider Threat analysis efforts and analytic products are consistent with these five analytic standards. The first four standards call for all analytic products to be objective, independent of political consideration, timely, and based on all available sources of information. The last standard calls for analysts to implement and exhibit Analytic Tradecraft in their analytic products.

Screen text:

**ANALYTIC STANDARDS:** Objective; Independent of political consideration; Timely; Based on all available sources of information; Implement and exhibit Analytic Tradecraft Standards

### **Objectivity – Screen 1 of 1**

Screen text: Objective Standards

Narrator: The first analytic standard addresses objectivity. Analysts must approach their job duties with an unbiased viewpoint; lack of objectivity limits or possibly prevents our full understanding of the problem. As an insider threat analyst, you must remain objective as you gather, integrate, and assess information. Maintaining preconceived notions or biases about a particular individual or group of individuals can lead to an inappropriate response to a given situation. For example, insider threat programs rely on potential risk indicators, observable and reportable behaviors, and activities, to identify potential insider threats. By focusing on the behavior of an individual rather than their demographic characteristics or status, we can remain objective.

Narrator: So why is it so difficult to be objective? The hardwiring in our brains work against objectivity. As our subconscious innately looks for patterns and creates connections, we end up perceiving relationships where none exists, favoring one idea over others, and jumping to conclusions.

Screen text: We are naturally NOT objective. The brain innately:

- Looks for patterns
- Creates connections - perceives relationships
- Favors certain ideas - forms bias

Narrator: The objectivity problem is exacerbated by a societal focus on subjective thinking—taking a stand on a single viewpoint and defending it—such as when we write a research paper or participate in the debate club. In those situations, we engage in advocacy, a useful skill, but one that limits our critical, objective thinking on a matter. However, you can take steps to be objective and fulfill the first analytic standard.

Screen text: We are taught to be subjective in school, to take a stand on a single viewpoint and defend it.

Examples:

- Research papers
- Debate club

Narrator: First, be aware of your own assumptions and reasoning. You can also use reasoning techniques and critical thinking tools to reveal and mitigate bias. You can intentionally consider alternative perspectives and contrary information. Lastly, try to adjust your thinking when new information unfolds. Analysis shouldn't be constrained by previous judgments when new developments indicate a change of course is necessary.

Screen text: How to be objective:

- Be aware of own assumptions and reasoning.
- Employ reasoning techniques and practical mechanisms (critical thinking tools) to reveal and mitigate bias.
- Intentionally consider alternative perspectives and contrary information.
- Adjust thinking as new information unfolds.

### **Independent of Political Consideration – Screen 1 of 1**

Narrator: Analytic Standard number two – Independent of political consideration. As an extension of objectivity, analysts must ensure their analytic assessments are not distorted or shaped by advocacy of a particular audience, agenda, or policy viewpoint.

Screen text: Independent of Political Consideration

Screen text: Beware that your decisions or focus are not directed or swayed by the approval/disapproval or support of stakeholders.

Your analysis should not support or reject a specific agenda, policy, or viewpoint.

Narrator: Insider threat analysts should not politicize or try to curry favor with the decision makers by writing assessments that support a policy maker's policy preferences.

Screen text: Assessments should not be written with political intent or to support a policy maker's policy preferences.

### **Timely Analysis – Screen 1 of 1**

Narrator: Analytic Standard number three is timeliness. Analysis must be disseminated in time to be actionable by customers. Analysts should be aware of events of interest, of insider threat program leadership activities and schedules, and of requirements and priorities in order to provide useful analysis at the right time.

Screen text: Timely

To provide useful analysis at the right time, be continuously aware of:

- Events of interest
- Insider threat program leadership activities and schedules
- Insider threat program requirements and priorities

Narrator: Your awareness, anticipation, and assessment of rapidly evolving developments, both positive and negative, are essential to feeding into the informed decisions made by Insider threat program members and senior leaders. As your analytic product is reviewed, invariably more questions will be asked, and the process will begin again. Select Case Study to learn more about the critical nature of the need for timely analysis.

Screen text: The Analyst's Challenges:

- Continuous awareness, anticipation and quick assessment of rapidly evolving developments and their impact, both positive and negative
- Quick dissemination of a current analytic product
- Adjustment to new developments and updating the analysis product with the implications of new developments

Narrator: Consider the case of Aaron Alexis.

Case Study: Aaron Alexis held a position of trust with access to DoD facilities based on a favorably adjudicated background investigation and his employment with a small private company that held a subcontract with the Navy to update computer hardware at Navy facilities around the world. On September 16, 2013, Aaron Alexis walked into Building 197 of the Washington Navy Yard and murdered twelve people. Four more were injured. Despite signs of erratic and potentially threatening behavior, Alexis was able to obtain and maintain his security clearance. The inability to capture relevant, detailed information, and do it in a timely manner, permitted Aaron Alexis access to secure federal facilities.

Screen text: In 2012, the Office of Personnel Management relied largely on an automated process to conduct and maintain background investigations for low-level security clearances. It meant that key information sometimes did not reach agency adjudicators. Aaron Alexis had a questionable background before he received clearance approval. If full knowledge of his erratic behavior reached an adjudicator in a timely manner, his application and continued security clearance would have received more scrutiny, potentially leading to its denial or revocation. Unfortunately, it did not.

After receiving his clearance, Alexis continued to engage in behavior that should have raised red flags. He broke his foot jumping off stairs while intoxicated, he fired a gun into his ceiling and through the apartment above, he fired a bullet through the wall of his room, he quit his job, and he complained that individuals were using a microwave machine to send vibrations into his body. None of this information was ever given to an adjudicator who had the ability to pull Alexis' Secret level clearance, which he maintained until September 16, 2013.

The inability to capture relevant, detailed information, and do it in near real-time, permitted Aaron Alexis to receive and keep a Secret clearance. That clearance permitted him to gain access to secure federal facilities and made it possible for him to murder 12 persons and seriously injure four more before he died by gunshot himself.

### **Based on Available Sources of Intelligence Information – Screen 1 of 1**

Narrator: Base analytic products on the best available information you have at a specific point in time. A moment after you produce an assessment, a new piece of information may arrive to change your earlier assessment. Accept the cycle as an ongoing, collaborative process. You need all available relevant information to inform an analysis. Work with the insider threat program to identify and address critical information gaps. Incomplete information lowers the confidence level of the analysis. Analysts should testify to the completeness of the assessment they provide as well as to their level of confidence regarding their judgments.

Screen text: Based on all available sources of information

- Identify and address critical information gaps.

Narrator: Consider the case of Stewart Nozette. Select Case Study to learn more about the critical nature of the need for timely analysis.

Case Study: Nozette earned acclaim as an astrophysicist and consultant to several federal agencies over the course of his career. He held clearances comparable to Top Secret/SCI between 1989 and 2006. Unfortunately, this scientist, whose intellectually gifted work led to finding water on the moon, was also willing to compromise classified information. Timely reporting of anomalous behavior and activity allowed the FBI to initiate an investigation. After transmitting national defense information to an undercover FBI agent posing as a foreign intelligence officer, Nozette pled guilty. He received a thirteen-year prison sentence.

Your role, ultimately, is to provide the insider threat program team members with analytic products that give them a decision advantage to appropriately mitigate insider risk.

Screen text: Charges were brought against Nozette who ran a non-profit corporation, “Alliance for Competitive Technology,” for fraudulent billing on a NASA contract. Nozette used the funds to pay for personal expenses such as such as mortgages, automobile loans, sedan services, and other items. He also failed to pay taxes on the unreported income. That federal investigation led to another timely Justice Department probe. Based on the information available from the case of fraud, the FBI suspected greed might motivate Nozette to sell sensitive government information. In 2009, the FBI set up a sting operation targeting Nozette for insider espionage. Following a series of meetings and exchanges of money over the next several weeks, Nozette pushed to receive larger payments for the secrets he was disclosing. Nozette was arrested and sentenced after pleading guilty to one count of espionage. The information he shared with the FBI agent directly concerned satellites, early warning systems, and means of defense or retaliation against large-scale attack, communications intelligence information, and major elements of defense strategy. Nozette is serving thirteen years at the federal penitentiary in Terre Haute, Indiana. Fortunately, the FBI found no evidence that any classified materials were actually released to anyone outside the U.S. Government.

### **Implement and Exhibit Analytic Tradecraft - Screen 1 of 1**

Screen text: Implement and Exhibit Analytic Tradecraft Standards

Narrator: The last standard, implements and exhibits analytic tradecraft, comprises nine separate elements that specify standards for analytic production. Taken together, the nine elements speak to accuracy and comprehensiveness of analytic products. Let's take a quick look at each of the analytic tradecraft standards now. Select each folder on analytic tradecraft to learn more.

Screen text: Analytic Tradecraft

All analytic products must:

1. Properly describe the quality and credibility of underlying sources, data, and methodologies
2. Properly express and explain uncertainties associated with major analytic judgments
3. Properly distinguish between underlying information and the analysts' assumptions and judgments
4. Incorporate analysis of alternatives
5. Demonstrate customer relevance and address implications
6. Use clear and logical argumentation
7. Explain change to or consistency of analytic judgments
8. Make accurate judgements and assessments
9. Incorporate effective visual information where appropriate

### **Describe Quality and Credibility – Screen 1 of 1**

Narrator: Identify any factors affecting source quality and credibility. Various factors can affect source quality and credibility.

Screen text:

1. Properly describe the quality and credibility of underlying sources, data, and methodologies

Identify any factors affecting source quality and credibility.

Various factors can affect source quality and credibility:

- Accuracy and completeness
- Possible denial and deception
- Age and continued currency of information
- Technical elements of collection
- Source access
- Validation
- Motivation
- Possible bias
- Expertise

Narrator: Use source descriptors and source summary statements in your analytic products: Provide a holistic assessment of strengths or weaknesses in the source base, Explain which sources are most important to key analytic judgments



Screen text:

Include source descriptors and source summary statements in your analytic products to:

- Provide a holistic assessment of strengths or weaknesses in the source base
- Explain which sources are most important to key analytic judgments

### **Express Uncertainties – Screen 1 of 1**

Narrator: Indicate and explain the basis for any uncertainties associated with analytic judgments. This includes expressing your confidence level for your judgments and how your uncertainties affect the analysis.

Screen text:

2. Properly express and explain uncertainties associated with major analytic judgments  
Indicate and explain the basis for uncertainties associated with analytic judgments.

Provide:

- Likelihood of occurrence of an event or development
- Analyst confidence in the basis for this judgment

Confidence is based on:

- Logic and its evidentiary base
- Quality and quantity of source material
- Understanding of the topic

For Uncertainties:

- Note the cause of uncertainty
  - Type
  - Currency
  - Amount of information
  - Knowledge gaps
  - Nature of the issue
- Explain how uncertainties affect the analysis
  - To what degree
  - How a judgment depends on assumptions

### **Information vs Assumptions/Judgments – Screen 1 of 1**

Narrator: In the analytic product, clearly distinguish between intelligence and your judgments.  
To do this:

- State assumptions explicitly when they serve as the cornerstone of your argument or when they bridge key information gaps.
- Explain the implications for judgments if assumptions prove to be incorrect.

- Identify indicators, as appropriate, that, if detected, would alter judgments.

Screen text:

3. Properly distinguish between underlying intelligence information and the analysts' assumptions and judgments

Analytic products should:

- State assumptions explicitly when they serve as the cornerstone of an argument or when they bridge key information gaps.
- Explain the implications for judgments if assumptions prove to be incorrect.
- Identify indicators, as appropriate, that, if detected, would alter judgments.

### **Analysis of Alternatives – Screen 1 of 1**

Narrator: Analytic products should identify and assess plausible alternative hypotheses. This is particularly important when major judgments must contend with significant uncertainties, or complexity (e.g., forecasting future trends), or when low probability events could produce high-impact results.

Screen text:

4. Incorporate analysis of alternatives

Analytic products should identify and assess plausible alternative hypotheses.

Analysis of alternatives – the systematic evaluation of differing hypotheses to:

- Explain events or phenomena
- Explore near-term outcomes
- Imagine possible futures to mitigate surprise and risk

Address factors such as:

- Associated assumptions
- Likelihood
- Implications related to U.S. interests
- Indicators that would affect the likelihood of identified alternatives

### **Relevance and Implications – Screen 1 of 1**

Narrator: Your analytic product should provide information and insight on issues relevant to the insider threat program. It should also address the implications provided by information and the analysis.

Screen text:

5. Demonstrate Customer Relevance and Address Implications

- Provide information and insight on issues relevant to the insider threat program
- Address the implications of the information and analysis they provide.

Add analytic value by addressing:

- Prospects
- Context
- Threats
- Factors affecting opportunities for action

### **Logical Argumentation – Screen 1 of 1**

Narrator: Never make your audience dig for your analytic message. Present your main message up front followed and supported with relevant information and coherent reasoning.

Screen text:

#### **6. Use Clear and Logical Argumentation**

Present a clear, main analytic message up front.

- If providing multiple judgments, provide a main analytic message drawn from those judgments.
- Support judgments with relevant information and coherent reasoning.
- Acknowledge significant AND contrary information affecting judgments.

### **Changes and Consistencies – Screen 1 of 1**

Narrator: If previous analysis exists on your topic, briefly state how your current judgements are consistent with or differ from previous analysis and why.

All significant differences in analytic judgment should be fully considered and brought to the attention of the insider threat program.

Screen text:

#### **7. Explain change to or consistency of analytic judgments**

State how major judgments on a topic are consistent with or represent a change from those in previously published analysis or represent initial coverage of a topic.

Analytic products:

- Need not be lengthy or detailed in explaining change or consistency
- Should avoid using boilerplate language
- Should make clear how new information or different reasoning led to the judgments expressed

Significant differences in analytic judgment should be fully considered and brought to the attention of the insider threat program.

## **Accurate Judgements and Assessments – Screen 1 of 1**

Narrator: Your analytic product must make accurate, clear, and precise judgments and assessments.

Screen text:

### 8. Make accurate judgements and assessments

Analytic products should:

- Apply expertise and logic
- Make the most accurate judgments and assessments possible
- Present all judgments that would be useful to the insider threat program
- Not avoid difficult judgments in order to minimize the risk of being wrong
- Express judgments as clearly and precisely as possible
- Reduce ambiguity by addressing the likelihood, timing, and nature of the outcome or development

## **Visual Information – Screen 1 of 1**

Narrator: Be sure to address information gaps, likelihood, timing, and outcomes and developments.

Screen text:

### 9. Incorporate effective visual information where appropriate

Incorporate effective visual information where appropriate to:

- Clarify an analytic message
- Complement or enhance the presentation of data and analysis

Visuals must:

- Be clear and pertinent to the subject
- Adhere to other analytic tradecraft standards

Select each item to view examples of using visuals used in analytic products.

Clarify      Enhance

## **What is a Sound and Comprehensive Analytic Product? - Screen 4 of 9**

Narrator: Our insider threat team members depend on us to provide analytic products with accurate information as well as professional judgments, conclusions, and recommendations. Retired four-star General Colin Powell had four rules for his intelligence officers and these rules

aptly describe what analysts and their comprehensive analytic products must do: "Over time I developed for my intelligence staffs a set of four rules to ensure that we saw the process from the same perspective and to take off their shoulders some of the burden of accountability: Tell me what you know. Tell me what you don't know. Then tell me what you think. Always distinguish which is which."

Screen text: "Over time I developed for my intelligence staffs a set of four rules to ensure that we saw the process from the same perspective and to take off their shoulders some of the burden of accountability: Tell me what you know. Tell me what you don't know. Then tell me what you think. Always distinguish which is which."

Narrator: To achieve a sound, comprehensive analytic product, analysts must apply intellectual and analytic standards which includes analytic tradecraft. Analytic tradecraft is supported by and demonstrated with critical thinking tools. Let's look at how you can use critical thinking tools in your analysis and analytic product.

Screen text: A sound, comprehensive analytic product applies:

- Intellectual Standards
- Analytic Standards
  - Analytic Tradecraft
  - Critical Thinking Tools

### **Challenges in Analysis Accuracy and Reliability - Screen 5 of 9**

Narrator: Sometimes it's difficult to verify your sources accuracy and reliability. New sources may have an unknown or low reliability rating. Sources may not offer you true or accurate information because of their own agenda or because they unknowingly obtained inaccurate or untruthful information. To counter these challenges, attempt to corroborate the information with other sources and to employ identity resolution techniques within your program to ensure accurate attribution of information to particular individuals. Your insider threat program will work with your legal counsel to determine approved sources of information for the program that are consistent with law, policy, and regulation.

Screen text: Meeting the standards of ICD 203 can be complicated by your sources of information.

- Sources with unknown or low reliability rating
- Sources may have their own agenda, may fabricate information
- Sources may have unknowingly obtained inaccurate or untruthful information

The fix? Attempt to corroborate the information with other sources.

Always include statements that provide:

- Source reliability assessment
- Confidence level assessment

### **Analytic Standards – Knowledge Check Activity - Screen 6 of 9**

Screen text: Working with the insider threat team to identify information gaps exemplifies which analytic standard?

- Objective
- Independent of political consideration
- Timely
- Available sources of information
- Analytic Tradecraft

To improve the integrity of analytic products, Intelligence Community Directive (ICD) 206 mandates that all analysis and analytic products must abide by intellectual standards and analytic standards, to include analytic tradecraft.

- True
- False

Analytic products should accomplish which of the following? Select all that apply.

- State assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps.
- Not provide assumptions with explaining judgments
- Explain the implications for judgments if assumptions prove to be incorrect.
- Identify indicators, as appropriate, that, if detected, would alter judgments.
- Be precise and directly get to the point and avoid listing underlying background information

“We judge with probable confidence that foreign entities will expand their attempts to access our company’s personnel data within the next two years.”

According to ICD 203, what should accompany this confidence statement in the analytic product? (Select all that apply.)

- The quality and quantity of source material
- The evidentiary base for the judgment
- Causes of uncertainty
- Analyst intuition
- Personal Identifying Information

### **Defense Assembly Agency Scenario - Part 3 - Screen 7 of 9**

Narrator: Let's return to the Defense Assembly Agency Scenario. Recall that employees interviewed stated that the agency took process shortcuts to ensure that deadlines were met but they had a positive outlook on how the organization worked together to accomplish the work. Now let's see what other office personnel had to say.

Ian: That idiot Lance thinks he knows how to run these networks. He is making wrong decisions about the networks that I designed and built while I am doing paperwork. He does not understand the hardware, software, and processes that we have in place here. The things that were working for us before I was pushed aside.

James: Ian should be managing these networks instead of Lance. Ian knows more about them than anyone. After all, he's been here since day one. He is really unhappy since he is no longer working directly on the hardware and software.

Lance: Ian is an arrogant jerk. He harasses and bullies his coworkers. Ian has held up several of our projects, making us miss deadlines. Larry even suspects Ian has been messing with the code that he is developing to make him look bad.

Caroline: Things have been different with Ian since we hired Lance and James. Ian became overtly hostile to his coworkers. I had to counsel him on two separate occasions. The second time seemed to have corrected his hostile behavior, but his work performance was still lacking. Finally, I had to speak with Chris about Ian's performance. All of this came to mind when I discovered that our system had been tampered with. I suspect it is an inside job.

Chris: When our agency first stood up, Ian was our backbone. He developed our computer system's software from scratch. That software is the foundation of our current automation processes. We had to bring more resources in to help Ian upgrade the agency's central server to meet requirements. We were very happy to get Lance because his degree enabled us to use him as the senior SA and he could also be our new project manager. I was really surprised the first time I heard complaints from coworkers about Ian's aggressive behavior. Josh, a software developer left us a couple of months ago. He said that he could no longer work with Ian. Caroline had to document unprofessional behavior with coworkers twice. So, after the series of run-ins with coworkers and his marginal performance, I had to consider letting him go. Now that our system has been damaged, I'm ready to fire him.

### **Defense Assembly Agency Scenario – Exercise – Screen 8 of 9**

Narrator: Here is a summary of the data collected from interviews with Defense Assembly Agency personnel.

Screen text: Ian: That idiot Lance thinks he knows how to run these networks. He is making wrong decisions about the networks that I designed and built while I am doing paperwork. He does not understand the hardware, software, and processes that we have in place here. The things that were working for us before I was pushed aside.

James: Ian should be managing these networks instead of Lance. Ian knows more about them than anyone. After all, he's been here since day one. He is really unhappy since he is no longer working directly on the hardware and software.

Lance: Ian is an arrogant jerk. He harasses and bullies his coworkers. Ian has held up several of our projects, making us miss deadlines. Larry even suspects Ian has been messing with the code that he is developing to make him look bad.

Caroline: Things have been different with Ian since we hired Lance and James. Ian became overtly hostile to his coworkers. I had to counsel him on two separate occasions. The second time seemed to have corrected his hostile behavior, but his work performance was still lacking. Finally, I had to speak with Chris about Ian's performance. All of this came to mind when I discovered that our system had been tampered with. I suspect it is an inside job.

Chris: When our agency first stood up, Ian was our backbone. He developed our computer system's software from scratch. That software is the foundation of our current automation processes. We had to bring more resources in to help Ian upgrade the agency's central server to meet requirements. We were very happy to get Lance because his degree enabled us to use him as the senior SA and he could also be our new project manager. I was really surprised the first time I heard complaints from coworkers about Ian's aggressive behavior. Josh, a software developer left us a couple of months ago. He said that he could no longer work with Ian. Caroline had to document unprofessional behavior with coworkers twice. So, after the series of run-ins with coworkers and his marginal performance, I had to consider letting him go. Now that our system has been damaged, I'm ready to fire him.

#### Incident Data

The Defense Assembly Agency hired two new people, Lance and James, to work with Ian, the agency's established systems administrator. They were tasked to coordinate efficient operations the agency's core functions on its central server. The new employees were tasked to improve the flexibility and sophistication of supporting operational tools and software programs in a short window of time. However, the agency discovered frequent glitches in the systems functions that seemed to correlate to efforts to hastily upgrade the functions.

Interviews with Ian, Lance, and James indicate a deteriorating work environment between Ian and Lance. Interviews with coworkers indicate that standard procedures were set aside with a "do whatever it takes" approaches to system operations and to cutting corners.

Narrator: Here is a draft findings report summary based on the situation.

#### Screen text: Incident Analysis Summary

Network functionality has been impaired. Ian presents disregard for Lance, the new lead system administrator who assumed Ian's former position. Lance is much younger than Ian and has the support of James, who is also young but has less education than Lance. Ian, in his forties and a member of Generation X, developed his knowledge of systems through experience. With his recent university degree, Lance a millennial, has little experience with security environments or access protocols, and less appreciation for traditional code documentation, procedures, and processes.

With a high degree of confidence, we conclude that the system failure was not an act of sabotage, but that Lance inadvertently caused the system failure by functional testing new code in the system production environment instead of the development environment. Lance's actions



created a problematic work environment that has negatively affected network reliability and agency productivity.

**Recommendation:** The agency director should confer with the assistant director about corrective work environment actions. Given the current situation, we recommend the following:

- Clearly separate the system development environment from the production environment.
- Require a separate password for access to the two network environments.
- Implement a process that requires system backup prior to any updates.
- Implement team-building activities to strengthen the working relationship between the systems administrators.

After reviewing the summary, which analytical standards were not followed?

- Objectivity
- Independent of political consideration
- Timely
- Based on all available sources of information

### **Analytic Standards Summary – Screen 9 of 9**

**Narrator:** This concludes the lesson Analytic Standards. This lesson explained the importance of the analytic standards; described the five analytic standards and how to use them to support the deterrence, detection, and mitigation of insider risk; described the nine elements of analytic tradecraft; and identified challenges in analysis accuracy and reliability.

**Screen text:** Lesson Objectives

- Explained the importance and purpose of the analytic standards.
- Described the five analytic standards and how to use them to support the deterrence, detection, and mitigation of insider risk.
- Described the nine elements of analytic tradecraft.
- Identified challenges in analysis accuracy and reliability.

## **Critical Thinking Tools**

### **Critical Thinking Tools Introduction – Screen 1 of 9**

**Narrator:** Critical thinking plays heavily into the accuracy of your analysis and your application of Analytic Tradecraft. During this lesson, we will examine what makes a sound and comprehensive analytic product and the critical thinking tools required to achieve that goal.

**Screen text:** Lesson Objectives

- Recognize critical thinking tools.
- Select the critical thinking tools most appropriate for a given situation.

## **Critical Thinking in Analysis – Screen 2 of 9**

Narrator: Recall that critical thinking involves actively and skillfully analyzing and evaluating information. Critical thinking allows you to structure your analysis. It helps make sense of complex problems, allows comparison and weight of elements against each other, and focuses on one element at a time. It forces the conscious examination of intuition and provides visual evidence via critical thinking tools. Critical thinking applies meaning to analyzed data. Applying critical thinking tools will build comprehensive, analytic products that may guide the actions of the insider threat program.

Screen text: Structure your analysis with critical thinking.

Critical thinking – The intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action.

Meaningful data + your judgments regarding that data = analytic product □ decision and policy making

## **Common Critical Thinking Tools – Screen 3 of 9**

Narrator: Here are some of the most useful critical thinking tools. Select each tool to learn more.

Screen text: Selectable tabs:

Critical Thinking Tools

- Problem Restatement
- Pros-Cons-Fixes
- Divergent/Convergent Thinking
- Chronologies/Timelines
- Causal Flow Diagram
- The Matrix
- Scenario/Decision Tree
- Weighted Ranking
- Hypothesis Testing
- Devil's Advocacy
- Probability Tree
- Utility Tree/Matrix

## **Problem Restatement – Screen 1 of 1**

Narrator: Restating the problem in various ways allows you to look at the problem from other perspectives as well as adjust the focus of your analysis.

Screen text: Problem Restatement – A means of looking at problem from other perspectives.

Steps:

1. Paraphrase: Restate using your own words.
2. 180 degrees: Turn the problem on its head.
3. Broaden the focus: Restate the problem in a larger context.
4. Redirect the focus: Boldly, consciously change the focus.

### **Pros-Cons-Fixes – Screen 1 of 1**

Narrator: Critical Thinking Tools

Listing Pros-Cons-Fixes helps you evaluate positive and negative elements, compare, and choose among alternative solutions.

Screen text: Pros-Cons-Fixes – A means of compensating for negative thinking by looking at the positives first.

Steps:

1. List all pros.
2. List all cons.
3. Review and consolidate the cons by merging those that are similar and eliminating those that are redundant.
4. Neutralize as many cons as possible.
5. Compare the Pros and unalterable Cons for all options.
6. Pick one option.

### **Divergent/Convergent Thinking – Screen 1 of 1**

Narrator: Divergent thinking helps generate alternative ideas. As you winnow out the less important ones, convergent thinking helps you select the single idea that correctly identifies the logical idea.

Screen text: Critical Thinking Tools

Divergent/Convergent Thinking – A brainstorming technique that lets ideas build upon another, without judgment so that they can be clustered and winnowed to select promising ideas. In divergent thinking or brainstorming, all ideas are permitted.

Rules for Divergent Thinking:

- The more ideas the better.
- Build one idea upon another.
- All ideas are accepted.
- Don't evaluate the ideas.
- Use at every stage of problem solving.

Convergent thinking selects one idea from a list of ideas.

### **Chronologies/Timelines – Screen 1 of 1**

Narrator: Chronologies or timelines can help you understand the context of events and look for cause and effect relationships.

Screen text: Critical Thinking Tools

Chronologies/Timelines – A means of orderly examination of information related to our instinctual nature to look for cause and effect relationships. It allows us to understand and appreciate the context that events occur.

Steps:

1. Make a list of relevant events and dates; list dates first.
2. Construct a chronology, crossing off events on the list as they are included.

### **Causal Flow Diagram – Screen 1 of 1**

Narrator: Use a causal flow diagram to identify and understand how these factors are interacting to create the problem. Using divergent/convergent thinking with the causal flow diagram can help you generate ways to resolve or at least mitigate the problem.

Screen text: Critical Thinking Tools

Causal Flow Diagram – Identifies a system's components and how they interact (cause and effect relationships).

Steps:

1. Identify major factors.
2. Identify cause-and-effect relationships.
3. Characterize the relationships as direct or inverse.
4. Diagram the relationships.
5. Analyze the behavior of the relationships as an integrated system.

### **The Matrix – Screen 1 of 1**

Narrator: A matrix separates elements of a problem in grid form.

Let's say a commercial satellite company's proprietary information has been leaked to another country. You can use a matrix to list and determine who had access to that particular trade information.

In this matrix, analysts examined possible connections that might serve as links to disproving a hypothesis about a terrorist who launched a deadly gas attack at a Tokyo railroad station in 1995.

Screen text: Critical Thinking Tools

Matrix – Enables separating elements of a problem, categorizing information by type, comparing one type of information as well as same types with another, and seeing correlations.

A matrix presents information in a grid and uses as many cells as necessary for whatever you need to analyze. Use a matrix to:

- Separate elements of the problem
- Categorize information by type

- Compare one type of information to another
- Compare information of the same type
- See patterns among the information

### **Scenario/Decision Tree – Screen 1 of 1**

Narrator: A Scenario or Decision Tree allows you to map out choices and outcomes.

Screen text: Critical Thinking Tools

Scenario/Decision Tree – A graphic illustration of choices and outcomes at different junctures in alternative sequences or chains of events. Each sequence or chain is a separate scenario.

Steps:

1. Identify the problem.
2. Identify the major factors/issues (the decisions and events) to be addressed in the analysis.
3. Identify alternatives for each of these factors/issues.
4. Construct a tree portraying all-important alternative scenarios.

### **Weighted Ranking - Screen 1 of 1**

Narrator: Use weighted ranking to compare, evaluate, and choose among alternatives. When ranking criteria, be sure to employ analytic and critical thinking skills so that appropriate rank is assigned to specific criteria.

Screen text: Critical Thinking Tools

Weighted Ranking – Assigns positions of something relative to other things to aid decision making.

Steps:

1. List all of the major criteria for ranking.
2. Pair-rank the criteria (rank the first against the second, the first against the third, etc.).
3. Select the top several criteria and weight them in percentiles (their sum must equal 1.0).
4. Construct a Weighted Ranking Matrix and enter the items to be ranked, the selected criteria, and the criteria weights.
5. Pair-rank all of the items by each criterion, recording in the appropriate spaces the number of “votes” each item receives.
6. Multiply the number of votes by the respective criterion’s weight.
7. Add the weighted values for each item and enter the sums in the column labeled “Total Votes.”
8. Determine the final rankings and enter them in the last column, labeled “Final Ranking.”
9. The items with the most points are ranked highest.
10. Verify outcome

## **Hypothesis Testing - Screen 1 of 1**

Narrator: Hypothesis testing helps you evaluate, compare, and choose among the alternative solutions with a visual matrix.

Screen text: Critical Thinking Tools

Hypothesis Testing – A means of testing all hypotheses sufficiently by a matrix that compares significant evidence to different hypotheses.

Steps:

1. Generate hypothesis.
2. Construct a matrix.
3. List “significant” evidence down the left-hand margin, including “absent” evidence.
4. Working across the matrix, test the evidence for consistency with each hypothesis, one item of evidence at a time.
5. Refine the matrix.
6. Working downward, evaluate each hypothesis.
7. Rank the remaining hypotheses by the weakness of inconsistent evidence. The hypothesis with the weakest inconsistent evidence is the most likely.
8. Verify outcome.

## **Devil’s Advocacy - Screen 1 of 1**

Narrator: Using devil's advocacy, you can examine other points of view.

Screen text: Critical Thinking Tools

Devil’s Advocacy – A means of challenging the rationale presented by:

11. Focus on the contrary or opposite viewpoint
12. Examine the opposing side’s supporting arguments and evidence
13. Critique and attempt to disprove arguments and evidence

This tool is not concerned with negative, contradictory evidence. The pro for one side is the con of the other.

Devil’s advocacy:

- Promotes objectivity
- Can undermine and show weakness of the primary view.

## **Probability Tree - Screen 1 of 1**

Narrator: Construct a probability tree to determine the likelihood of scenario.

Screen text: Critical Thinking Tools

Probability Tree or Matrix – A means to address random and indeterminate problems by assigning a statistical probability or likelihood; a means of estimating an outcome when we run out of data.

Steps:

1. Identify the problem.
2. Identify the major decisions and events to be analyzed.
3. Construct a scenario tree portraying all-important alternative scenarios.
4. Assign a probability to each decision/event. Probabilities at each branch must equal 1.0.
5. Calculate the conditional probability of each individual scenario.
6. Calculate the answers to probability questions relating to the decisions/events.

### **Utility Tree/Matrix - Screen 1 of 1**

Narrator: A utility tree helps you select from several solutions by weighing and ranking benefits of each.

Screen text: Critical Thinking Tools

Utility Tree/Matrix – A means of looking at options and outcomes, determining their utility (benefit), and ranking them.

Steps:

1. Identify the options and outcomes to be analyzed.
2. Identify the perspective of the analysis.
3. Construct a utility matrix.
4. Assign a utility value of 0 to 100 (unless dollars are used) to each option-outcome-combination—each cell of the matrix—by asking the Utility Question: If we select this option, and this outcome occurs, what is the utility from the perspective of...? There must be at least one 100 unless dollars are used.
5. Assign a probability to each outcome. Determine or estimate this probability by asking the Probability Question: If this option is selected, what is the probability this outcome will occur? The probabilities of all outcomes for a single option must add up to 1.0.
6. Determine the expected values by multiplying each utility by its probability and then adding the expected values for each option.
7. Determine the ranking of the alternative options.
8. Verify outcome.

### **Knowledge Check - Screen 4 of 9**

Screen text: Using critical thinking tools provides \_\_\_\_\_ to the analysis process.

- Data
- Honesty
- Structure
- Verification

### **Critical Thinking Tools – Activity - Screen 5 of 9**

Screen text: Match the tool to its description.

Use this tool to determine outcomes.

This tool helps us understand context.

Use this objective approach to determine weakness to a primary view.

This tool is for selecting the best option by weighing and ranking benefits.

A decision-making tool for comparing alternatives and assigning values to them.

This tool freely explores options/causal factors that can later be winnowed down to the most important.

Use this to identify and understand how factors interact.

Scenario tree

Chronologies/Timelines

Devil's Advocacy

Utility Tree

Weighted Ranking

Divergent/Convergent thinking

Causal Flow Diagram

### **Defense Assembly Agency Scenario/Exercise – Part 3 - Screen 6 of 9**

Narrator: A potential insider threat incident has occurred. Caroline just discovered that something has wiped out their entire system configuration and operational tools, and she cannot locate the backups. Caroline suspects this incident might be an insider job. She reported the matter to the insider threat team. The team gathered some background information on the agency and some transcripts from interviews with several employees. Select each folder to learn more.

Screen text:

#### Employee Interviews

Employee 1: We were one lean operating machine. We had to extend the systems to support our new mission area. Ian thought of and implemented the idea to centralize the agency's core functions on a central server to coordinate operations more efficiently. We made vast improvements to the flexibility and sophistication of the supporting operational tools and software programs over a very short period. The extensions worked well with very few glitches. Of course, we had to cut some corners, giving people access when and where they needed it to make things happen. If something did not contribute to extending the systems, it just did not seem worth doing. This was how we were able to accomplish as much as we did.

Employee 2: That's right. The entire staff adopted a "do whatever it takes" attitude to their job in order to keep up with the demands placed on us due to the growth. We only had one Systems Administrator at that time, but we got everything done.

Ian: That idiot Lance thinks he knows how to run these networks. He is making wrong decisions about the networks that I designed and built while I am doing paperwork. He does not



understand the hardware, software, and processes that we have in place here. The things that were working for us before I was pushed aside.

James: Ian should be managing these networks instead of Lance. Ian knows more about them than anyone. After all, he's been here since day one. He is really unhappy since he is no longer working directly on the hardware and software.

Lance: Ian is an arrogant jerk. He harasses and bullies his coworkers. Ian has held up several of our projects, making us miss deadlines. Larry even suspects Ian has been messing with the code that he is developing to make him look bad.

Caroline: Things have been different with Ian since we hired Lance and James. Ian became overtly hostile to his coworkers. I had to counsel him on two separate occasions. The second time seemed to have corrected his hostile behavior, but his work performance was still lacking. Finally, I had to speak with Chris about Ian's performance.

Chris: When our agency first stood up, Ian was our backbone. He developed our computer system's software from scratch. That software is the foundation of our current automation processes. We had to bring more resources in to help Ian upgrade the agency's central server to meet requirements. We were very happy to get Lance because his degree enabled us to use him as the senior SA and he could also be our new project manager. I was really surprised the first time I heard complaints from coworkers about Ian's aggressive behavior. Josh, a software developer left us a couple of months ago. He said that he could no longer work with Ian. Caroline had to document unprofessional behavior with coworkers twice. So, after the series of run-ins with coworkers and his marginal performance, I was considering terminating his employment.

### Agency Background

Defense Assembly Agency builds computer systems to mission specifications for organizations within the agency. Eighteen months ago, the agency began supporting organizations outside of its agency. With significant new additions to the agency's mission and workload, Defense Assembly Agency hired additional people. Chris, the agency director, and Caroline, the assistant director, recognized the need for qualified personnel. Lance was hired to replace the lead system administrator, Ian, because of his education and experience. James was hired as a junior system administrator to share the growing systems administration workload and responsibilities with Ian, one of the agency's original employees who had built the original system from the ground up.

### The Incident

Caroline just discovered that something has wiped out their entire system configuration and operational tools, and she cannot locate the backups. Caroline suspects this incident might be an insider job. She reported the matter to the insider threat team.

In this early stage of the problem-solving process, what critical thinking tool could be useful to determine who had access to the system?

- Problem Restatement

- Pros-Cons-Fixes
- Divergent/Convergent Thinking
- Chronologies/Timelines
- The Matrix
- Scenario/Decision Tree

### **Defense Assembly Agency Scenario/Exercise – Part 3 - Screen 7 of 9**

Narrator: Your chronology of events and a matrix indicate that James and Ian had access to the server and system the day of the system wipeout. Additional intelligence from system logs traces the launch of a logic bomb to James' machine.

Narrator: You recommend gathering additional information from the system files. An available file indicates James used his password on a date he was not in the building. You recommend that additional information about James and Ian be gathered appropriately and in accordance with privacy and civil liberties. Available files reveal no further info on James, but they show that Ian recently had a DUI and it occurred just weeks after his father passed away. The insider threat team has multiple strategies to mitigate risk associated with this incident. First, the team refers their findings for criminal investigation and reports the matter to other organizations as required. While being mindful of the ongoing investigation, the insider threat team deploys additional responses to mitigate risk.

Screen text: Using information from the User Activity Monitoring capability, you developed a chronology of events and a matrix that indicate:

- James and Ian had access to the server and system the day of the system wipeout.
- System logs trace the launch of a logic bomb to James' machine.

You recommend gathering additional information from the system files. An available file indicates James used his password on a date he was not in the building. You recommend that additional information about James and Ian be gathered appropriately and in accordance with privacy and civil liberties. Available files reveal no further info on James, but they show that Ian recently had a DUI and it occurred just weeks after his father passed away. The insider threat team has multiple strategies to mitigate risk associated with this incident. First, the team refers their findings for criminal investigation and reports the matter to other organizations as required. While being mindful of the ongoing investigation, the insider threat team deploys additional responses to mitigate risk.

What critical thinking tool will be of greatest use to you now?

- Divergent/Convergent thinking
- Problem restatement
- Scenario Tree

### **Defense Assembly Agency Scenario/Exercise – Part 3 - Screen 8 of 9**

Narrator: You will use a number of tools to help with the analysis, but first they should restate the problem to help focus the problem and the analysis. The question should be clear and precise.

Screen text: Restate the problem so that you can develop clearer, more precise questions. Don't forget to look at the questions from different points of view.

Here are some ways to restate the question:

- What can employees do to prevent system sabotage?
- What can management do to prevent system sabotage?
- Are there security protocols that were violated or not enforced?
- Are additional security protocols required?
- Why did Ian commit the sabotage?
- Did Ian present potential risk indicators?
- Where these indicators reported?
- If not, why not?
- If so, to whom and what was the response?

### **Critical Thinking Tools Summary - Screen 9 of 9**

Narrator: This concludes the lesson Critical Thinking. This lesson recognized critical thinking tools and selected critical thinking tools most appropriate for a given situation.

Critical thinking tools visually structure, facilitate, and empower thinking by presenting the information and facts and the reasoning process and help explain our uncertainties, conclusions, and judgments.

Screen text: Lesson Objectives

- Recognized critical thinking tools.
- Selected the critical thinking tools most appropriate for a given situation.

### **Course Conclusion**

#### **Course Summary - Screen 1 of 3**

Narrator: This concludes the lesson Critical Thinking. This lesson recognized critical thinking tools and selected critical thinking tools most appropriate for a given situation. Critical thinking tools visually structure, facilitate, and empower thinking by presenting the information and facts and the reasoning process and help explain our uncertainties, conclusions, and judgments.

Screen text:

Lesson Objectives

- Recognized critical thinking tools.
- Selected the critical thinking tools most appropriate for a given situation.

Narrator: This course introduced you to critical and analytic thinking, the reasoning process, intellectual and analytic standards; analytic tradecraft; and critical thinking tools required for sound and comprehensive analysis. You can employ these skills to support your insider threat program in the deterrence, detection, and mitigation of insider risks while protecting the privacy and civil liberties of the workforce.

Screen text:  
Course Objectives

Demonstrated an understanding of critical and analytic thinking as it relates to Insider Threat Analysts.

- Contrasted critical and analytic thinking.
- Recognized the eight elements of thought.
- Identified the nine intellectual standards, their purpose, and their relationship to analytic thinking.
- Related critical and analytic thinking to an insider threat analyst's role.
- Recognized challenges to applying reasoning skills.

Recognized common analytic mistakes.

Identified the analytic standards, to include analytic tradecraft, that apply to analysis and the development of a comprehensive analytic product.

- Explained the importance and purpose of the analytic standards.
- Described the five analytic standards and how to use them to support the deterrence, detection, and mitigation of insider risk.
- Described the nine elements of analytic tradecraft.
- Identified challenges in analysis accuracy and reliability.

Selected critical thinking tools most appropriate to develop a sound and comprehensive insider threat analytic product.

- Recognized critical thinking tools.
- Selected the critical thinking tools most appropriate for a given situation.

### **Course Conclusion – Screen 2 of 3**

Narrator: Congratulations! You have completed the Critical Thinking for Insider Threat Analysts course.

Screen text: Congratulations! You have completed the Critical Thinking for Insider Threat Analysts course.

### **Course Examination – Screen 3 of 3**

Screen text: To receive course credit, you must take the course examination. Select the Take Exam button to launch the online exam.



## Answer Key

### Thinking for Insider Threat Analysts Lesson

#### Knowledge Check Activity - Thinking for Insider Threat Analysts - Screen 8 of 16 –

Screen text: Which intellectual standard are you complying with if you are examining the complexity of the problem or the various factors causing a problem to be difficult?

- Breadth
- Depth
- Significance
- Relevance

Answer: Depth

Analytic thinking requires breaking a problem down into multiple parts and thinking each part through to find a solution.

Order Elements of the Analytic Thinking Process

1. Define the problem/state the question
2. Think about the purpose
3. Check assumptions
4. Clarify concepts
5. Gather information
6. Address implications
7. Regard point of view
8. Be aware of inferences

Answer:

1. Think about the purpose
2. Define the problem/state the question
3. Gather information
4. Be aware of inferences
5. Check assumptions
6. Clarify concepts
7. Regard point of view
8. Address implications

#### Defense Assembly Agency Scenario Exercise 1 – Screen 10 of 16

Screen text: Given this information on the Defense Assembly Agency, what is the first step you should take in the reasoning process?

- Address implications
- Brainstorm who is the culprit and the motivation
- Define the problem
- Gather information

Answer: Define the problem

Which intellectual standards should you apply as you begin your analysis of the situation at the Defense Assembly Agency?

- Logic
- Point of view
- Assumptions
- Relevance

Answer: Logic and Relevance

Continue thinking about applying the intellectual standards to this situation.

You have statements from two managers and two employees that relate the state of the work environment. Do these statements provide enough information for you to begin your analysis of the problem? Why or why not?

- Yes, because the information that you have covers all points of view.
- Yes, because the statements are relevant.
- No, because the current statements do not provide depth and breadth of the situation.
- No, because problem analysis requires you to interview all members of the staff regardless of their knowledge or level of involvement in the situation.

Answer: No, because the current statements do not provide depth and breadth of the situation.

As you begin your analysis of the problem, you determine that you should direct your focus specifically on employee access to the agency server. This focus is an example of complying with which of the following intellectual standards?

- Accuracy
- Clarity
- Precision
- Significance

Answer: Significance

### **Defense Assembly Agency Scenario - Part 2 – Screen 14 of 16**

You have seen the Lead Systems Administrator, Lance, in the hallway a couple of times. He never smiles or speaks and seems standoffish in your opinion. If you consider this observation in

your analysis of the information around this situation, you could make which of the following analytic wrongdoing mistakes? Select all that apply.

- Focusing on a solution that you may intuitively favor
- Beginning the analysis by forming a conclusion first
- Failing to use the process of analysis
- Not structuring the analysis as a problem

Answer:

Focusing on a solution that you may intuitively favor  
Beginning the analysis by forming a conclusion first  
Failing to use the process of analysis

Chris came to your office and told you that he thinks this situation may have been an error by the trainee, Michael. The other members of the IT team could not have made such a mistake and they are loyal employees.

If you consider Chris' opinion in your analysis, you could make which of the following analytic wrongdoing mistakes?

- Focusing on a satisfactory solution.
- Focusing on a solution that you may intuitively favor
- Over analyzing the situation
- Not structuring the analysis as a problem

Answer: Focusing on a satisfactory solution.

### **Knowledge Check Activity 2 - Screen 15 of 16**

Screen text: The analytic products that you create should demonstrate your use of \_\_\_\_\_.

- Analyst Notebook
- The reasoning process
- Exhaustive intelligence
- Empowered thinking

Answer: The reasoning process

In your role as an insider threat analyst, what functions will the analytic products you create serve? Select all that apply.

- Inform
- Advise
- Provide subject matter expertise
- Create policy
- Provide direct support



Answer: Inform, Advise, Provide subject matter expertise, Provide direct support

Create a checklist about the natural thinking processes that can interfere with the analytic process by selecting the items to go on the list. When you have finished creating the checklist, select Submit.

Natural Thinking Processes that Interfere with Analytical Thinking

- Biases and assumptions
- Clinging to untrue beliefs in the face of contrary evidence
- Compulsive explaining regardless of accuracy
- Emotional response
- Lack of information to process
- Overwhelming amounts of information to process
- Over-readiness to accept other ideas
- Preference for evidence supporting our belief system
- Subconscious mental shortcuts
- Subconscious pattern seeking

Answer:

Biases and assumptions

Clinging to untrue beliefs in the face of contrary evidence

Compulsive explaining regardless of accuracy

Emotional response

Preference for evidence supporting our belief system

Subconscious mental shortcuts

Subconscious pattern seeking

You and another analyst have collaborated to work on a potential insider threat situation. Your partner suggests a solution, but your initial reaction is to prefer your own idea. The more you think about it the better your idea seems.

Which natural thinking process is happening here? Select all that apply.

- Emotional reaction
- Mental shortcuts
- Relying on biases and assumptions
- Patterning
- Compulsive explaining
- Attaching importance to evidence that supports your beliefs and judgments while dismissing or devaluing evidence that does not

Answer: Relying on biases and assumptions and attaching importance to evidence that supports your beliefs and judgments while dismissing or devaluing evidence that does not

## Analytic Standards

### Analytic Standards – Knowledge Check Activity – Screen 6 of 9

Working with the insider threat team to identify information gaps exemplifies which analytic standard?

- Objective
- Independent of political consideration
- Timely
- Available sources of information
- Analytic Tradecraft

Answer: Available sources of information

To improve the integrity of analytic products, Intelligence Community Directive (ICD) 206 mandates that all analysis and analytic products must abide by intellectual standards and analytic standards, to include analytic tradecraft.

- True
- False

Answer: False

Analytic products should accomplish which of the following? Select all that apply.

- State assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps.
- Not provide assumptions with explaining judgments
- Explain the implications for judgments if assumptions prove to be incorrect.
- Identify indicators, as appropriate, that, if detected, would alter judgments.
- Be precise and directly get to the point and avoid listing underlying background information

Answer:

State assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps.

Identify indicators, as appropriate, that, if detected, would alter judgments.

Be precise and directly get to the point and avoid listing underlying background information

“We judge with probable confidence that foreign entities will expand their attempts to access our company’s personnel data within the next two years.”

According to ICD 203, what should accompany this confidence statement in the analytic product? (Select all that apply.)

- The quality and quantity of source material
- The evidentiary base for the judgment
- Causes of uncertainty
- Analyst intuition
- Personal Identifying Information

Answer:

The quality and quantity of source material

The evidentiary base for the judgment

Causes of uncertainty

### **Defense Assembly Agency Scenario - Exercise – Screen 8 of 9**

After reviewing the summary, which analytical standards were not followed?

- Objectivity
- Independent of political consideration
- Timely
- Based on all available sources of information

Answer: Objectivity

### **Knowledge Check – Screen 4 of 9**

Using critical thinking tools provides \_\_\_\_\_ to the analysis process.

- Data
- Honesty
- Structure
- Verification

Answer: Structure

### **Critical Thinking Tools – Activity - Screen 5 of 9**

Match the tool to its description.

Use this tool to determine outcomes.

This tool helps us understand context.

Use this objective approach to determine weakness to a primary view.

This tool is for selecting the best option by weighing and ranking benefits.

A decision-making tool for comparing alternatives and assigning values to them.

This tool freely explores options/causal factors that can later be winnowed down to the most important.

Use this to identify and understand how factors interact.

Scenario tree  
Chronologies/Timelines  
Devil's Advocacy  
Utility Tree  
Weighted Ranking  
Divergent/Convergent thinking  
Causal Flow Diagram

Answer:

Use this tool to determine outcomes. Scenario tree

This tool helps us understand context. Chronologies/Timelines

Use this objective approach to determine weakness to a primary view. Devil's Advocacy

This tool is for selecting the best option by weighing and ranking benefits. Utility Tree

A decision-making tool for comparing alternatives and assigning values to them.

Weighted Ranking

This tool freely explores options/causal factors that can later be winnowed down to the most important. Divergent/Convergent thinking

Use this to identify and understand how factors interact. Causal Flow Diagram

### **Defense Assembly Agency Scenario/Exercise – Part 3 – Screen 6 of 9**

In this early stage of the problem-solving process, what critical thinking tool could be useful to determine who had access to the system?

- Problem Restatement
- Pros-Cons-Fixes
- Divergent/Convergent Thinking
- Chronologies/Timelines
- The Matrix
- Scenario/Decision Tree

Answer: The Matrix

### **Defense Assembly Agency Scenario/Exercise – Part 3 – Screen 7 of 9**

What critical thinking tool will be of greatest use to you now?

- Divergent/Convergent thinking
- Problem restatement
- Scenario Tree

Answer: Problem restatement

### **Defense Assembly Agency Scenario/Exercise – Part 3 – Screen 8 of 9**

Screen text: Restate the problem so that you can develop clearer, more precise questions. Don't forget to look at the questions from different points of view.

Answer:

Here are some ways to restate the question:

- What can employees do to prevent system sabotage?
- What can management do to prevent system sabotage?
- Are there security protocols that were violated or not enforced?
- Are additional security protocols required?
- Why did Ian commit the sabotage?
- Did Ian present potential risk indicators?
- Where these indicators reported?
- If not, why not?
- If so, to whom and what was the response?