DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

SAND2025-11801R

Bayesian Attack Model (BAM) User Story

Lee T. Maccarone, Romuald Valme, Ted R. Anaya

Revision 0

2025

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

ABSTRACT

This document presents a user story for the Bayesian Attack Model (BAM) tool designed to aggregate and analyze cyber-attack observables for operational technology (OT) systems. BAM aims to empower cybersecurity analysts by providing a streamlined interface for collecting observable data from various sources, enabling real-time analysis of potential adversary activity. By enhancing the response capabilities of security teams, BAM facilitates risk-informed decision-making and improves organizational security posture. This user story outlines the key functionalities, user interactions, and requirements necessary to successfully integrate BAM with other security information and event management (SIEM) technology and cybersecurity operations centers (CSOCs).

VALUE PROPOSITION

BAM aggregates observer experiences of anomalous events across OT environments to provide actionable decision intelligence. BAM can comprehensively analyze anomalous host-based, network-based, and physical environment observables. The primary benefit of aggregating a wide range of observables is to enhance the cybersecurity incident response process via earlier detection of adversarial activity and more effective response. Successful interruption of an OT cyber-attack may result in averting significant consequences including loss of revenue, damage to property, and loss of safety to facility staff and the public.

BACKGROUND

BAM is a Bayesian network developed to characterize the stage of cyber-attacks on OT systems given observable evidence. A Bayesian network is a graphical method for representing the probabilistic relationship between variables and enables inference about the state of some variables given the known state of other variables. As shown in Figure 1, observable evidence propagates through BAM based on the MITRE ATT&CK for ICS taxonomy [1]. Observables may come from a variety of sources, including hosts, networks, and the physical environment. The overall cyber-attack is characterized by the probabilities of four adversary behavior phases: Early, Middle, Late, and Impact. Inference can also be performed on the intermediate MITRE ATT&CK for ICS techniques and tactics. For more information on BAM, readers are encouraged to refer to [2, 3].

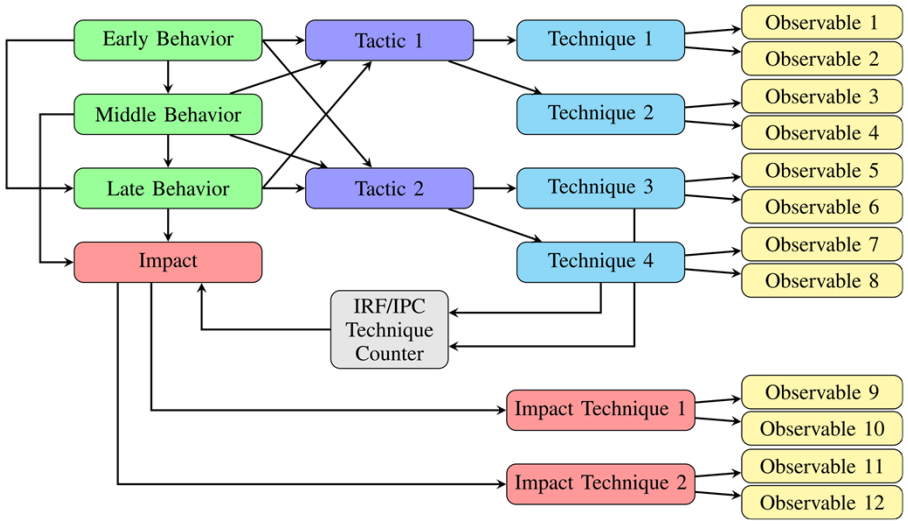

Figure 1. BAM's Structure [3]

USERS

For simplicity, the BAM user groups were defined based on the SANS ICS job role to competency level recommendations [4]. These recommendations divide job roles into seven groups: Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff (we have divided the original OT group into OT Staff and OT Cybersecurity to mirror the IT groups defined by SANS). Individuals with the titles defined by these groups may perform one or more of the work roles defined by the U.S. National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework [5]. For brevity, we will discuss the NICE Framework alignment only within the context of the BAM user groups.

BAM users are categorized into two groups: Observers and Analysts. These groups are not mutually exclusive – one individual may perform functions corresponding to both groups. Observers often perform the Implementation and Operation (IO) and/or Protection and Defense (PD) work role categories in the NICE Framework. Analysts often perform the PD and/or Investigation (IN) work role categories in the NICE Framework. These work role categories are defined below:

- Implementation and Operation (IO): "Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security." [6]
- Protection and Defense (PD): "Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks." [6]
- Investigation (IN): "Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence." [6]

Observers are responsible for providing observable evidence to BAM. Observables may come from a variety of sources, so observers may support a variety of roles within the organization. Examples of observers are provided in Table I. This table is intended to communicate BAM's primary users and is not an exhaustive list.

Table I. BAM Users – Observers

Job Role	IT Host-Based Observables	IT Network-Based Observables	OT Host-Based Observables	OT Network-Based Observables	Physical Environment Observables
IT Staff	X	X			
IT Cybersecurity	X	X			
OT Staff			X	X	X
OT Cybersecurity			X	X	
Engineering			X	x	X
Support Staff	x	x	x	x	x
Management					x
X = greater frequency of observations, x = lesser frequency of observations					

The core user story for the Observer is:

> As an Observer, I want to document the anomalous events that I see in my workplace so that cybersecurity experts in my organization can investigate them and respond appropriately.

Analysts are responsible for performing inference in BAM, and for interpreting and communicating BAM's output to decision-makers. BAM may be used to support decision-making at the operational, tactical, and strategic levels. The specific Analyst users are OT Cybersecurity Analysts and IT Cybersecurity Analysts, and they are responsible for communicating their findings and recommending courses of action to Management.

The core user story for the Analyst is:

> As an Analyst, I want to identify and understand adversarial activity in my environments earlier so that I can begin response activities earlier, more effectively, and with data-supported justification.

As noted previously, the Analyst and Observer user groups are not mutually exclusive. It is anticipated that when a user belongs to both groups, the user's primary role is that of the Analyst.

PRECONDITIONS

This section describes the preconditions that should be achieved before a user can successfully begin the main BAM workflow. These preconditions are primarily focused on operational aspects of BAM's implementation. Installation requirements will be provided in the BAM User's Guide.

1. Observer is equipped with the processes and technology to enable the perception of observables pertinent to the Observer's job role
2. Observer is equipped with the processes and technology to enable the logging of observables in a SIEM tool applicable to their job role and responsibilities
3. Data pipelines exist for the passing of observable data in Structured Threat Intelligence eXpression (STIX) format from their SIEM tool collection source to BAM
4. Data pipelines exist for the passing of BAM output data in STIX format to other SIEM tools as appropriate
5. Processes exist for the Analyst to communicate cybersecurity decision intelligence to Management

POSTCONDITIONS

This section describes the postconditions that should occur after the main BAM workflow has been executed.

1. Analyst has successfully generated a JSON file containing the probability of all levels of adversary activity (MITRE ATT&CK for ICS Techniques and Tactics, and adversary behavior phase) as a function of observable evidence accumulated over time
2. Analyst has successfully generated graphical representations of the MITRE ATT&CK for ICS Techniques and adversary behavior phase data contained in the JSON file
3. Analyst has identified if any risk thresholds have been exceeded at the MITRE ATT&CK for ICS Technique or adversary behavior levels

4. Analyst has identified the most critical observables corresponding to each MITRE ATT&CK for ICS Technique
5. Analyst is equipped with knowledge to inform risk-informed decision-making at the tactical and operational levels. The tactical level of decision-making is moderate-term, often on the order of months, and informs the schedule of tasks for an organization to achieve its goals [7]. The operational level of decision-making is short-term, often on the order of days, and informs actions to be taken by individuals across the ICS job roles to achieve the organization's goals [7]
6. Analyst is equipped with knowledge to engage in risk-informed decision-making conversations with Management at the strategic level. The strategic level of decision-making is long-term, often on the order of years, and defines the organization's security purpose in alignment with the organization's broader mission and goals [7].

MAIN WORKFLOW

This section outlines the main workflow for BAM users. It is important to note that although this workflow is written below in a linear fashion, this workflow should be continuously implemented with feedback between analysts and observers. The incident response life cycle model in the NIST Incident Response Recommendations and Considerations for Cybersecurity Risk Management (NIST SP 800-61r3) was adopted as a framework for describing this continuous feedback process [8]. The NIST life cycle model describes the roles of the Cybersecurity Framework (CSF) Functions in incident response. This incident response life cycle model is integrated with the BAM workflow in Figure 2. The parenthetical steps referenced in Figure 2 correspond to the steps of the main BAM workflow discussed below.

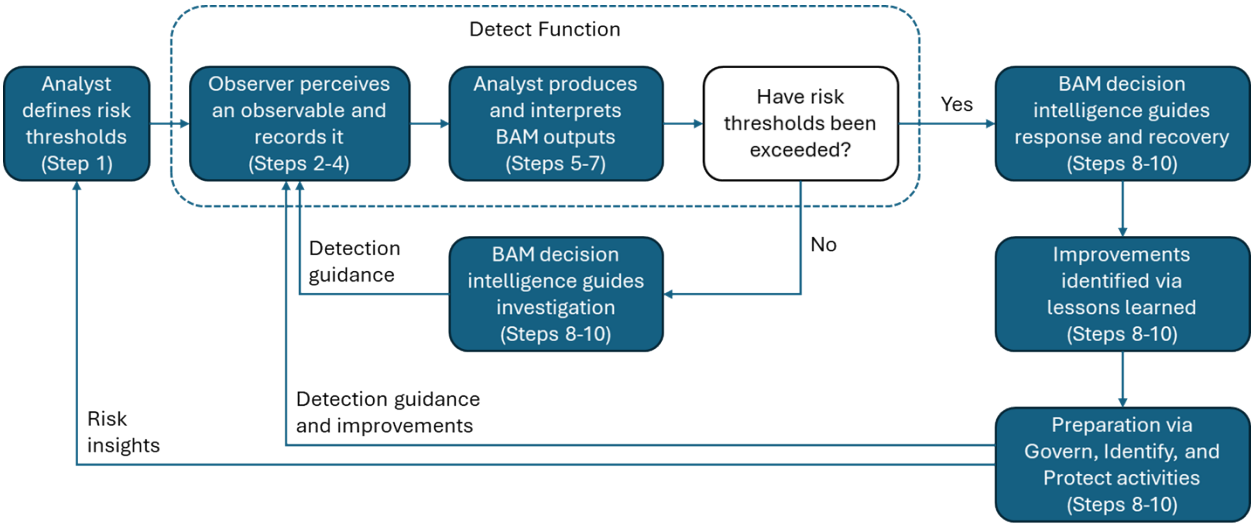

Figure 2. BAM Workflow Integrated with the NIST Incident Response Life Cycle

The following is a list of the steps in the main BAM workflow. Appendix B contains NICE task statements applicable to each step in the main workflow sequence listed below.

1. Analyst defines risk thresholds for BAM's adversary behavior phases and MITRE ATT&CK for ICS Techniques. This is an initial step that should occur upon BAM's implementation. This step should be revisited as needed during BAM's operation. More information about defining risk thresholds for BAM's adversary behavior phases can be found in [9].

2. Observer perceives an Observable. Observables may occur in the IT or OT environments, and may be host-based, network-based, or based on the physical process.
3. Observer records Observable in SIEM Tool
    a. Observer assesses Observable timestamp
    b. Observer provides Observable description
    c. Observer assesses Observable MITRE ATT&CK for ICS Technique (if known)
    d. Observer assesses Observable MITRE ATT&CK for ICS Tactic (if known)
    e. Observer assesses Observable normal frequency (if known)
    f. Observer assesses Observable probability given the MITRE ATT&CK for ICS Technique & Tactic (if known)
4. SIEM Tool produces STIX 2.1 file [10, 11]. The upcoming BAM User's Manual will contain several STIX input examples.
5. Analyst executes BAM import function to import observables from STIX file to BAM log
    a. If necessary, Analyst assesses any unassessed Observable attributes
    b. If necessary, Analyst identifies Observable sequence for any observables with identical timestamps
    c. BAM import function assigns Observable ID
    d. This step may be executed in several ways:
        i. Manually
        ii. Automatically update log with individual observables as they are recorded
        iii. Automatically update log with batches of observables at a specified frequency
        iv. Automatically update log with batches of observables when a specific quantity of STIX files have been aggregated
6. Analyst executes BAM process function to attach Observable nodes to BAM network, perform Bayesian inference, and output inference data in JSON format. The output format is structured based on the observable input, and inference is performed based on the sequential and cumulative evidence provided to BAM by the observables. The upcoming BAM User's Manual will contain an example of this output in JSON format. The output data includes:
    a. Observable timestamp
    b. Observable description
    c. Observable ID
    d. Adversary behavior probabilities given individual observable evidence
    e. MITRE ATT&CK for ICS Tactic probabilities given individual observable evidence
    f. MITRE ATT&CK for ICS Technique probabilities given individual observable evidence
    g. Adversary behavior probabilities given the sequential accumulation of observable evidence
    h. MITRE ATT&CK for ICS Tactic probabilities given the sequential accumulation of observable evidence
    i. MITRE ATT&CK for ICS Technique probabilities given the sequential accumulation of observable evidence
7. Analyst executes the BAM Dashboard function to view BAM results. The following bullets describe the elements of the BAM Dashboard. A complete visual of the BAM Dashboard is provided in Appendix C.

a. Exceedance of risk thresholds. A panel specifies whether the probabilities of adversary behavior are within their established thresholds. The display prominently indicates when thresholds are exceeded.
b. Probability of adversary behavior by phase given cumulative observable evidence. An example of this graphical output is shown in Figure 3. Requires the following information:
    i. Probability of Early/Middle/Late/Impact "Ongoing" state
    ii. Probability of Early/Middle/Late/Impact "Complete" state
    iii. Timestamps for each data point
    iv. User interaction with plot: For digestibility, the Analyst may need look at the probability of adversary behavior data over a specific window of time. Sliders are available for the user to specify the starting and ending times to be displayed.

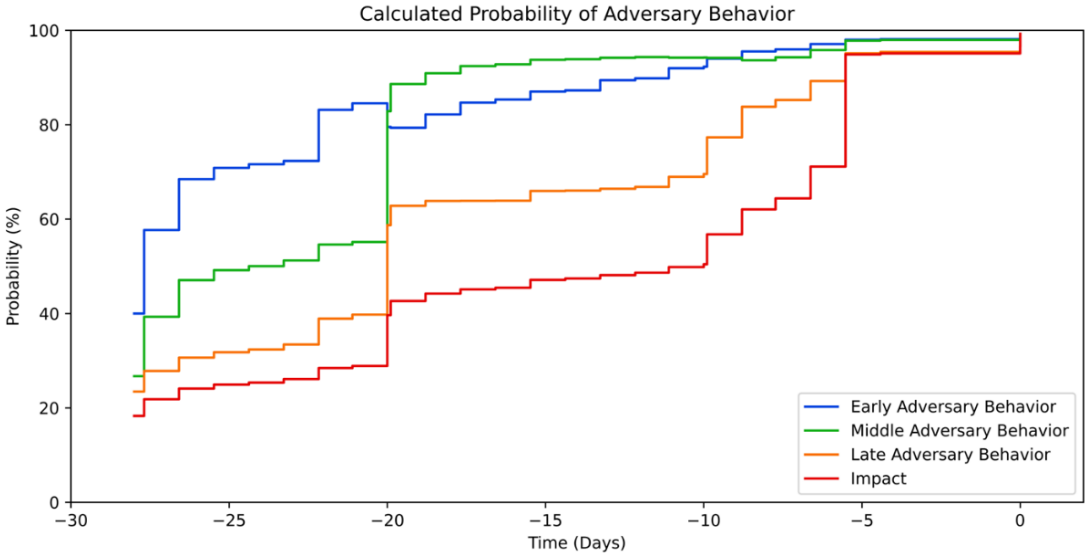

Figure 3. Example Graphical Output of Adversary Behavior by Phase

c. Probability of MITRE ATT&CK for ICS Techniques given cumulative observable evidence. Graphically, this output appears nearly identical to the adversary behavior data shown in Figure 3, except the probability of a specific MITRE ATT&CK for ICS Technique is shown. Requires the following information:
    i. Probability of every MITRE ATT&CK for ICS Technique "Yes" state
    ii. Timestamps for each data point
    iii. Observable description for each data point
    iv. User interaction with plot:
        1. For digestibility, the Analyst may need to look at the probability of specific MITRE ATT&CK for ICS Techniques over time. The Analyst may toggle buttons to select which techniques are displayed.
        2. For digestibility, the Analyst may need look at the probability of MITRE ATT&CK for ICS Techniques data over a specific window of time. Sliders are available for the user to specify the starting and ending times to be displayed.
d. This step may be executed in several ways:
    i. Manually
    ii. Automatically graph after process function

8. Analyst leverages knowledge gained from BAM analysis for risk-informed decision-making at the operational level. Examples of applications at the operational level are provided below. These examples are quoted from NICE Framework components [6] and additional examples are provided in Appendix B.
    a. Investigate suspicious activity and alleged digital crimes (T1137)
    b. Perform cyber defense incident triage (T1250)
    c. Recommend security changes to systems and system components (T1162)
9. Analyst leverages knowledge gained from BAM analysis for risk-informed decision-making at the tactical level. Examples of applications at the tactical level are provided below. These examples are quoted from NICE Framework components [6] and additional examples are provided in Appendix B.
    a. Advise senior management on risk levels and security posture (T0158)
    b. Prioritize critical cyber defense infrastructure resources (T1353)
    c. Serve as OT engineering subject matter expert for development of organizational cybersecurity risk management plan (T2050)
10. Analyst leverages knowledge gained from BAM analysis for risk-informed decision-making at the strategic level. Examples of applications at the strategic level are provided below. These examples are quoted from NICE Framework components [6] and additional examples are provided in Appendix B.
    a. Advise senior leadership and authorizing official of changes affecting the organization's cybersecurity posture (T1061)
    b. Serve as OT engineering subject matter expert for cybersecurity standards, policies, and procedures development (T2049)
    c. Develop risk acceptance documentation for senior leaders and authorized representatives (T1574)

CONCLUSION

BAM is an OT cybersecurity tool designed to aggregate observer experiences of anomalous events across OT environments to provide actionable decision intelligence. By connecting the primary BAM user groups of Observers and Analysts, BAM can comprehensively analyze anomalous host-based, network-based, and physical environment observables. The primary benefit of aggregating a wide range of observables is to enhance the cybersecurity incident response process via earlier detection of adversarial activity and more effective response. If BAM is implemented as part of the complete incident response lifecycle, there is opportunity to apply lessons learned from BAM analysis to further improve the perception and comprehension of anomalous observables. By integrating BAM with the people, processes, and technology of existing CSOCs, asset owners can more effectively characterize adversary activity in their environments and interrupt cyber-attacks before consequences occur.

ACKNOWLEDGMENTS

This project was funded by the U.S. Department of Energy Office of Cybersecurity, Energy Security, & Emergency Response (CESER) via Idaho National Laboratory (INL). The authors would like to thank the Idaho National Laboratory Cybersecurity for the Operational Technology (CyOTE) and Cybersecurity Operational Research, Experimentation, Innovation, and Integration (COREII) teams for their support of BAM's development [12, 13].

REFERENCES

[1] The MITRE Corporation, "ICS Matrix," [Online]. Available: https://attack.mitre.org/matrices/ics/. [Accessed February 24 2024].

[2] L. T. Maccarone, D. M. Buede, S. T. Bowman, C. D. Burdick, M. C. Bracken, J. A. Jones and G. A. Weaver, "Development of a Bayesian Network to Model Malicious Cyber-Activity in Operational Technology Environments," in *Conference on Uncertainty in Artificial Intelligence, Bayesian Modeling Applications Workshop*, Eindhoven, Netherlands, 2022.

[3] L. T. Maccarone, D. M. Buede, S. T. Bowman, P. Ambrozewicz, C. D. Burdick, J. C. Grady and S. X. Wen, "Identifying Adversarial Cyber-Activity in Operational Technology Environments Using Bayesian Networks," *IEEE Transactions on Information Forensics and Security,* 2025.

[4] The SANS Institute, "ICS Job Role to Competency Level Recommendation," 18 January 2016. [Online]. Available: https://www.sans.org/posters/ics-job-role-to-competency-level-recommendation/. [Accessed 2 November 2024].

[5] R. Peterson, D. Santos, M. C. Smith, K. A. Wetzel and G. Witte, "Workforce Framework for Cybersecurity (NICE Framework)," U.S. National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2020.

[6] U.S. National Institute of Standards and Technology (NIST), "NICE Framework Components," 7 May 2025. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions. [Accessed 14 May 2025].

[7] G. White, "Strategic, Tactical, & Operational Management Security Model," *Journal of Computer Information Systems,* vol. 49, no. 3, pp. 71-75, 2009.

[8] A. Nelson, S. Rekhi, M. Souppaya and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61r3)," U.S. National Institute for Standards and Technology (NIST), Gaithersburg, MD, 2025.

[9] J. C. Grady, S. X. Wen, L. T. Maccarone and S. T. Bowman, "Stastical Methods for Developing Cybersecurity Response Thresholds for Operational Technology Using Historical Data," in *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, Washington, D.C., 2024.

[10] OASIS Standard, "STIX Version 2.1," [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html. [Accessed 11 March 2025].

[11] The MITRE Corporation, "ATT&CK STIX Data," 12 November 2024. [Online]. Available: https://github.com/mitre-attack/attack-stix-data/. [Accessed 8 April 2025].

[12] Idaho National Laboratory, "Cybersecurity for the Operational Technology Environment (CyOTE)," U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), 2024. [Online]. Available: https://cyote.inl.gov/. [Accessed 30 April 2024].

[13] Idaho National Laboratory, "Cybersecurity Operational Research, Experimentation, Innovation, and Integration (COREII)," U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), 2024. [Online]. Available: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_125970.pdf. [Accessed 30 April 2025].

APPENDIX A. REVISION HISTORY

Revision	Description
0	Initial document

APPENDIX B. MAIN WORKFLOW NICE TASK STATEMENTS

This appendix contains exemplar NICE task statements corresponding to the steps of the main BAM workflow. The steps of the main BAM workflow in this appendix are abbreviated versions of the full descriptions contained earlier in this document. This task statement list is not exhaustive and may be supplemented by the user's organization based on the role of BAM in their CSOC. For each step of the main BAM workflow, the relevant task statements are categorized as either descriptive statements or supporting statements. Descriptive task statements directly describe the corresponding BAM workflow step and supporting task statements describe actions that may be undertaken as part of the corresponding BAM workflow step. All task statements in this appendix are quoted directly from the NICE Framework components [6].

1. Analyst defines risk thresholds for BAM's adversary behavior phases and MITRE ATT&CK for ICS Techniques.
    a. Descriptive task statement:
        i. Define unacceptable risk threshold triggers for continuous data monitoring (T1948)
    b. Supporting task statements:
        i. Apply standards to identify safety risk and protect cyber-physical functions (T1011)
        ii. Determine the operational and safety impacts of cybersecurity lapses (T1020)
        iii. Develop a cybersecurity risk management plan (T1265)
        iv. Develop cybersecurity risk profiles (T1079)
        v. Develop risk, compliance, and assurance monitoring strategies (T1154)
        vi. Develop risk, compliance, and assurance measurement strategies (T1155)
        vii. Develop risk, compliance, and assurance specifications (T1165)

2. Observer perceives an Observable
    a. Descriptive task statements:
        i. Collect documentary or physical evidence of cyber intrusion incidents, investigations, and operations (T1207)
        ii. Identify digital evidence for analysis (T1199)
        iii. Identify network artifacts (T1039)
    b. Supporting task statements:
        i. Perform file signature analysis (T0167)
        ii. Perform static media analysis (T0179)
        iii. Perform Windows registry analysis (T0397)
        iv. Perform continuous monitoring of system activity (T1350)
        v. Perform penetration testing (T1359)
        vi. Collect intrusion artifacts (T1370)
        vii. Scan digital media for viruses (T1381)
        viii. Analyze network traffic anomalies (T1386)
        ix. Detect concealed data (T1516)
        x. Monitor system and server configurations (T1578)
        xi. Conduct cybersecurity reviews (T1592)
        xii. Coordinate all-source collection activities (T1645)

xiii. Identify system vulnerabilities within a network (T1747)
xiv. Conduct insider threat risk assessments (T1974)
xv. Troubleshoot system hardware and software (T0237)
xvi. Perform authorized penetration testing on enterprise network assets (T1091)
xvii. Validate network alerts (T1112)
xviii. Perform dynamic analysis on drives (T1253)
xix. Identify gaps in security architecture (T1264)
xx. Report forensic artifacts indicative of a particular operating system (T1301)
xxi. Capture network traffic associated with malicious activities (T1322)
xxii. Analyze network traffic associated with malicious activities (T1323)
xxiii. Process crime scenes (T0193)

3. Observer records Observable in SIEM Tool
   a. Descriptive task statement:
      i. Document digital evidence (T1325)
   b. Supporting task statements:
      i. Escalate system alerts that may indicate risks (T1970)
      ii. Report cybersecurity incidents (T1300)
      iii. Track cyber defense incidents from initial detection through final resolution (T1315)
      iv. Document cyber defense incidents from initial detection through final resolution (T1316)

4. SIEM Tool produces STIX 2.1 file.
   a. Descriptive task statement:
      i. Document digital evidence (T1325)
   b. Supporting task statements:
      i. Escalate system alerts that may indicate risks (T1970)
      ii. Track cyber defense incidents from initial detection through final resolution (T1315)
      iii. Document cyber defense incidents from initial detection through final resolution (T1316)

5. Analyst executes BAM import function to import observables from STIX file to BAM log
   a. Descriptive task statements:
      i. Process digital evidence (T1324)
      ii. Perform real-time forensic analysis (T1072)
      iii. Perform timeline analysis (T0173)
   b. Supporting task statements:
      i. Track cyber defense incidents from initial detection through final resolution (T1315)
      ii. Document cyber defense incidents from initial detection through final resolution (T1316)

6. Analyst executes BAM process function to attach Observable nodes to BAM network, perform Bayesian inference, and output inference data in JSON format.
    a. Descriptive task statements:
        i. Identify and characterize intrusion activities against a victim or target (T0153)
        ii. Detect cybersecurity attacks and intrusions (T1347)
        iii. Perform real-time forensic analysis (T0172)
        iv. Perform timeline analysis (T0173)
        v. Detect cybersecurity attacks and intrusions (T1347)
        vi. Conduct hypothesis testing (T1445)
        vii. Distinguish between benign and potentially malicious cybersecurity attacks and intrusions (T1348)
    b. Supporting task statements:
        i. Identify cyber threat tactics and methodologies (T0845)
        ii. Document what is known about intrusions (T1104)
        iii. Conduct analysis of computer network attacks (T1192)
        iv. Determine the scope, urgency, and impact of cyber defense incidents (T1252)
        v. Determine causes of network alerts (T1299)
        vi. Prepare continuous monitoring reports (T1945)
        vii. Validate intrusion detection system alerts (T1387)
        viii. Identify cyber threat tactics and methodologies (T0845)
        ix. Develop cybersecurity risk profiles (T1079)
        x. Perform risk and vulnerability assessments (T1619)
        xi. Prepare risk management reports (T1622)
        xii. Report cybersecurity incidents (T1300)
        xiii. Track cyber defense incidents from initial detection through final resolution (T1315)
        xiv. Document cyber defense incidents from initial detection through final resolution (T1316)

7. Analyst executes BAM graphing function to view BAM results:
    a. Descriptive task statements:
        i. Identify and characterize intrusion activities against a victim or target (T0153)
        ii. Detect cybersecurity attacks and intrusions (T1347)
        iii. Perform real-time forensic analysis (T0172)
        iv. Perform timeline analysis (T0173)
        v. Detect cybersecurity attacks and intrusions (T1347)
        vi. Conduct hypothesis testing (T1445)
        vii. Distinguish between benign and potentially malicious cybersecurity attacks and intrusions (T1348)
    b. Supporting task statements:
        i. Identify cyber threat tactics and methodologies (T0845)
        ii. Document what is known about intrusions (T1104)
        iii. Conduct analysis of computer network attacks (T1192)

iv. Determine the scope, urgency, and impact of cyber defense incidents (T1252)
v. Determine causes of network alerts (T1299)
vi. Prepare continuous monitoring reports (T1945)
vii. Validate intrusion detection system alerts (T1387)
viii. Identify cyber threat tactics and methodologies (T0845)
ix. Develop cybersecurity risk profiles (T1079)
x. Perform risk and vulnerability assessments (T1619)
xi. Prepare risk management reports (T1622)
xii. Report cybersecurity incidents (T1300)
xiii. Track cyber defense incidents from initial detection through final resolution (T1315)
xiv. Document cyber defense incidents from initial detection through final resolution (T1316)

8. Analyst leverages knowledge gained from BAM analysis for risk-informed decision-making at the operational level.
   a. Descriptive task statements:
      i. Develop risk mitigation strategies (T1160)
      ii. Recommend risk mitigation strategies (T1266)
      iii. Implement risk mitigation strategies (T1968)
      iv. Recommend risk mitigation courses of action (CoA) (T1976)
      v. Recommend courses of action or countermeasures to mitigate risks (T2002)
   b. Supporting task statements:
      i. Determine the scope, urgency, and impact of cyber defense incidents (T1252)
      ii. Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cybersecurity incidents (T1428)
      iii. Perform cyber defense incident triage (T1250)
      iv. Perform real-time cyber defense incident handling (T1260)
      v. Recommend incident remediation strategies (T1251)
      vi. Coordinate incident response functions (T0510)
      vii. Mitigate potential cyber defense incidents (T1371)
      viii. Implement protective or corrective measures when a cybersecurity incident or vulnerability is discovered (T1310)
      ix. Document cybersecurity incidents (T1241)
      x. Produce incident findings reports (T1132)
      xi. Investigate suspicious activity and alleged digital crimes (T1137)
      xii. Improve network security practices (T1050)
      xiii. Isolate malware (T1388)
      xiv. Remove malware (T1389)
      xv. Employ approved defense-in-depth principles and practices (T0262)
      xvi. Acquire resources to support cybersecurity program goals and objectives (T1056)
      xvii. Recommend security changes to systems and system components (T1162)
      xviii. Develop risk mitigation strategies for systems and applications (T1164)

xix. Determine if appropriate threat mitigation actions have been taken (T1317)
xx. Determine impact of malicious activity on systems and information (T1351)
xxi. Mitigate risks in systems and system components (T1560)
xxii. Implement dedicated cyber defense systems (T1561)
xxiii. Implement system security measures (T1563)
xxiv. Resolve computer security incidents (T1616)
xxv. Recommend cost-effective security controls (T1620)
xxvi. Recommend potential courses of action (T1712)
xxvii. Implement cybersecurity action plans (T1932)
xxviii. Track cyber defense incidents from initial detection through final resolution (T1315)
xxix. Document cyber defense incidents from initial detection through final resolution (T1316)
xxx. Track cyber defense incidents from initial detection through final resolution (T1315)
xxxi. Document cyber defense incidents from initial detection through final resolution (T1316)

9. Analyst leverages knowledge gained from BAM analysis for risk-informed decision-making at the tactical level.
   a. Descriptive task statements:
      i. Develop risk mitigation strategies (T1160)
      ii. Recommend risk mitigation strategies (T1266)
      iii. Implement risk mitigation strategies (T1968)
      iv. Recommend risk mitigation courses of action (CoA) (T1976)
      v. Recommend courses of action or countermeasures to mitigate risks (T2002)
   b. Supporting task statements:
      i. Advise management, staff, and users on cybersecurity policy (T1605)
      ii. Advise senior management on risk levels and security posture (T0158)
      iii. Communicate the value of cybersecurity to organizational stakeholders (T1088)
      iv. Advise on Risk Management Framework process activities and documentation (T1294)
      v. Recommend new or revised security, resilience, and dependability measures (T1303)
      vi. Develop cybersecurity policy recommendations (T1307)
      vii. Provide cybersecurity guidance to organizational risk governance processes (T1343)
      viii. Coordinate critical cyber defense infrastructure resources (T1352)
      ix. Prioritize critical cyber defense infrastructure resources (T1353)
      x. Identify system and network protection needs (T1556)
      xi. Plan implementation strategies (T1597)
      xii. Advise stakeholders on enterprise cybersecurity risk management (T1601)
      xiii. Recommend threat and vulnerability risk mitigation strategies (T1603)
      xiv. Establish cybersecurity risk assessment processes (T1862)
      xv. Establish organizational risk management strategies (T1908)
      xvi. Determine if continuous monitoring data provides situational awareness of risk levels (T1947)

xvii. Serve as OT engineering subject matter expert for development of organizational cybersecurity risk management plan (T2050)

xviii. Track cyber defense incidents from initial detection through final resolution (T1315)

xix. Document cyber defense incidents from initial detection through final resolution (T1316)

10. Analyst leverages knowledge gained from BAM analysis for risk-informed decision-making at the strategic level.
    a. Descriptive task statements:
        i. Develop risk mitigation strategies (T1160)
        ii. Recommend risk mitigation strategies (T1266)
        iii. Implement risk mitigation strategies (T1968)
        iv. Recommend risk mitigation courses of action (CoA) (T1976)
        v. Recommend courses of action or countermeasures to mitigate risks (T2002)
    b. Supporting task statements:
        i. Advise senior leadership and authorizing official of changes affecting the organization's cybersecurity posture (T1061)
        ii. Communicate the value of cybersecurity to organizational stakeholders (T1088)
        iii. Provide cybersecurity guidance to organizational risk governance processes (T1343)
        iv. Analyze organizational cybersecurity posture trends (T1539)
        v. Serve as OT engineering subject matter expert for cybersecurity standards, policies, and procedures development (T2049)
        vi. Advocate organization's official position in legal and legislative proceedings (T0006)
        vii. Develop risk acceptance documentation for senior leaders and authorized representatives (T1574)
        viii. Recommend organizational cybersecurity resource allocations (T1304)
        ix. Advise stakeholders on enterprise cybersecurity risk management (T1601)
        x. Develop risk, compliance, and assurance monitoring strategies (T1154)
        xi. Develop risk, compliance, and assurance measurement strategies (T1155)
        xii. Track cyber defense incidents from initial detection through final resolution (T1315)
        xiii. Document cyber defense incidents from initial detection through final resolution (T1316)

APPENDIX C. BAM DASHBOARD

Figure 4 shows the BAM Dashboard where the Analyst can visualize and interact with the BAM data. The BAM Dashboard contains risk threshold alerts, plotted time series of probability of adversary behavior, plotted time series of probability of selected MITRE ATT&CK for ICS Techniques, and a snapshot of the probability of all MITRE ATT&CK for ICS Techniques at the current time.

Figure 4. BAM Dashboard