INL/MIS-24-79012-Revision-0

Bayesian Attack Model (BAM)

July 2024

Changing the World's Energy Future

Alycia Brooke Honas

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed 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. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-79012-Revision-0

Bayesian Attack Model (BAM)

Alycia Brooke Honas

July 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

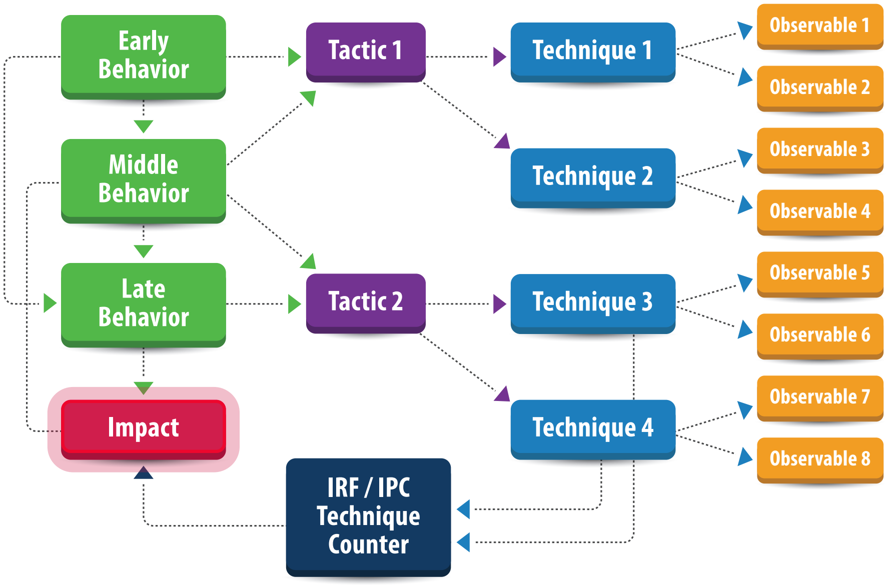
http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Bayesian Attack Model (BAM)

Overview

The Bayesian Attack Model (BAM) is an analytical tool designed to enhance the comprehension of adversarial activity in OT environments. BAM leverages both expert cybersecurity insights and historical data to characterize the likelihood of adversarial behavior given anomalous observable events. This tool will be made available for free download to industry.



BAM applies Bayesian inference methods to calculate the likelihood of adversarial techniques, tactics, and behaviors given observed evidence. Techniques and tactics are defined using the MITRE ATT&CK® for ICS framework, and adversary behavior phases are defined as high-level characterizations of the progress of an attack. By using BAM, OT professionals can better identify and characterize adversarial behavior in their systems to enable risk-informed investigations and interruptions before impact occurs.

BAM was developed by Sandia National Laboratories (SNL) and Idaho National Laboratory (INL) as part of the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) research, development, and demonstration (RD&D) mission to improve and strengthen energy security.

Use Cases

BAM has two main use cases:

Facilitates Strategic Decision-Making

BAM aids in strategic decision-making by estimating the likelihood of different stages of adversarial behavior. BAM serves as a platform to break down organizational information silos by aggregating evidence across the observer experiences of various OT roles and responsibilities. This enables security teams to prioritize resources and responses effectively, focusing on the most probable threats at any given time.

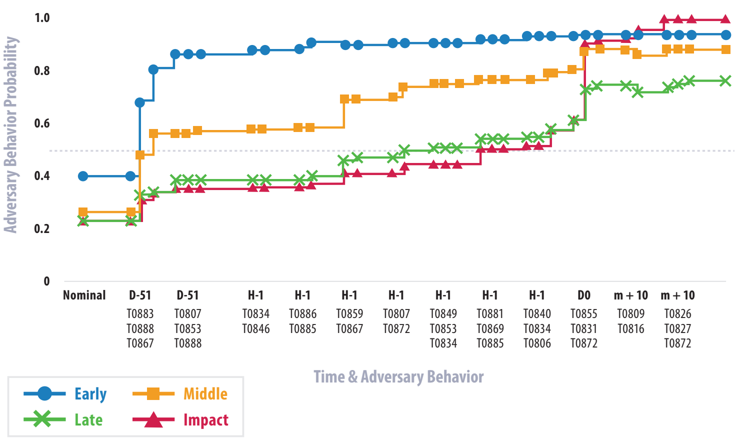
Enhanced Learning from Past Incidents

BAM has been applied to 27 historical case studies of cyber-attacks on OT systems. The results of these analyses are a useful tool for identifying opportunities for earlier perception and comprehension of adversarial activity.

Workflow

An observer of an anomalous event logs the event into the BAM application. Historical data and expert-elicited insights are used to correlate the observable to a technique. For every perceived observable, the likelihoods of the adversary behavior phases and of every MITRE ATT&CK® for ICS technique and tactic are calculated. The user can visualize changes in each of these likelihoods as evidence is introduced. These likelihoods can be used to inform the prioritization of resources and responses.

Industroyer2 Analysis of Adversary Behavior by Phase



Adversary Behavior

Nominal	No Adversary Behavior
T0883	Internet Accessible Device
T0888	Remote System Information Discovery
T0867	Lateral Tool Transfer
T0807	Command-Line Interface
T0853	Scripting
T0888	Remote System Information Discovery
T0834	Native API
T0846	Remote System Discovery
T0886	Remote Services
T0885	Commonly Used Port
T0859	Valid Accounts
T0867	Lateral Tool Transfer
T0807	Command-Line Interface
T0872	Indicator Removal on Host
T0849	Masquerading
T0853	Scripting
T0834	Native API
T0881	Service Stop
T0869	Standard Application Layer Protocol
T0885	Commonly Used Port
T0840	Network Connection Enumeration
T0834	Native API
T0806	Brute Force I/O
T0855	Unauthorized Command Message
T0831	Manipulation of Control
T0872	Indicator Removal on Host
T0809	Data Destruction
T0816	Device Restart/Shutdown
T0826	Loss of Availability
T0827	Loss of Control
T0872	Indicator Removal on Host

Key Benefits

BAM enables dynamic risk assessment by continuously updating the probability estimates as new evidence is collected.

BAM can be customized to the specific characteristics of different OT environments.

BAM enables security teams to prioritize resources and responses effectively, focusing on the most probable threats at any given time.

Utilizing historical data in BAM allows for a learning component where past incidents inform future detection.

Leveraging the MITRE ATT&CK® framework ensures compatibility with widely used security standards and practices.

Capabilities Under Development

Integration with the Operational Process for Trigger Identification and Comprehension (OPTIC) application for entry of human-identified observables.

Integration with the Collection and Analysis of Telemetry for CyOTE Heuristics (CATCH) pipeline for entry of machine-identified observables.

Integration with the Cyber Capability Maturity Model (C2M2) to add additional organizational context to the calculation of adversary behavior.

email: CyOTE.Program@hq.doe.gov