MBEAR

Model-Based Engineering for Automated Risk Management

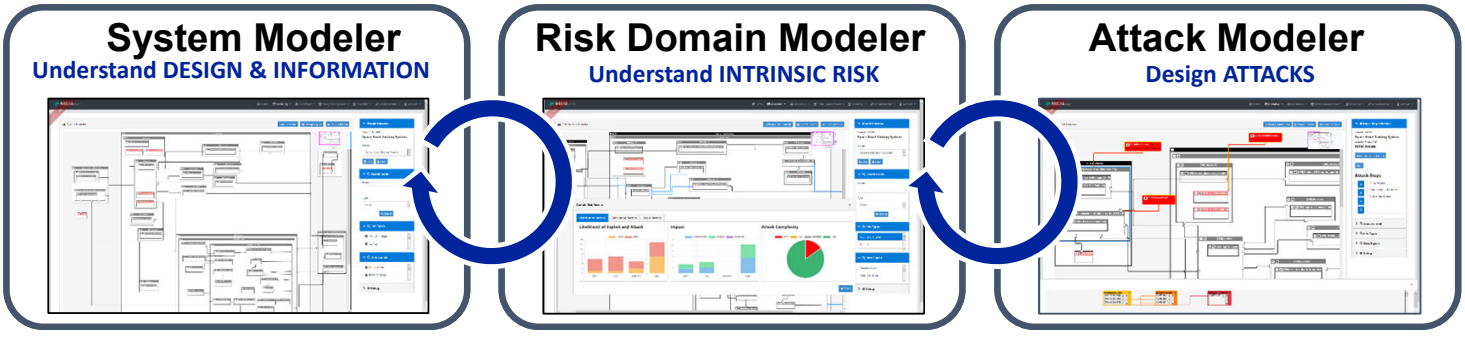
Go Beyond Cybersecurity with Model-Based Analysis of Intrinsic Risk and Threat-Based Analysis

Model-Based Engineering for Automated Risk Management (MBEAR) is a model-based approach to cybersecurity risk mitigation that goes beyond the compliance and regulatory based cybersecurity approaches with intrinsic risk and threat-based analysis. This approach provides an evidence-based risk management solution early in the system lifecycle, does not require an available running system, while at the same time reducing the cost and skills required to achieve cyber resilience at scale.

MBEAR establishes analysis techniques for evaluating a system's intrinsic cyber risk based on the system design, user-tailored risk views, and the discovery and modeling of viable cyber attacks. MBEAR is model-driven, which means that MBEAR provides role-based views that supports the modeling and capture of information required for advanced cyber resilience. MBEAR can import system models from Cameo System Modeler or you can use MBEAR's user friendly modeling interface.

MBEAR is designed so that end-users are using built-for-purpose interfaces meeting requirements for specific role-based activities. This approach reduces training requirements when compared to the complexity of general modeling tools by offering specific cybersecurity automation and interfaces that streamlines complex or tedious tasks. MBEAR's key features include:

- Model-Based Approach with Early Risk Mitigation
- Import System Model from Cameo Systems Modeler
- Automatic Discovery of Potential Vulnerabilities, Weaknesses, and Common Attack Patterns
- Build-for-Purpose Role-Base Risk Views and Metrics
- Workflow for Streamlining Risk Management Framework (RMF) Activities
- Attack Path Modeling Based on Auto-Discovered
- Design-Based Intrinsic Risk Views
- Data-Driven Template-Base Report Generation



System Modeler

An intuitive graphical modeler specifically designed for Systems Engineers acquiring and curating system structural and behavioral details relevant to cybersecurity analysis while minimizing the need for modeling training. With the System Modeler you gain:

- Understanding of system composition and function
- Understanding of the system attack surface and opportunities
- Support analysis of information flows and potential impact
- Intuitive graphical system design view (diagram)

Attack Modeler

An attack and threat modeler specifically designed for threat modelers to capture specific attack paths aligned to system elements and expressed as MITRE ATT&CK® taxonomy. The Attack Modeler provides:

- Curation and understanding of valid attacks against the system of interest using intrinsic system design vulnerabilities and weaknesses
- Machine-enabled analysis and understanding of the discrete attack steps that make up the attack path
- Correlation of attack steps to system elements

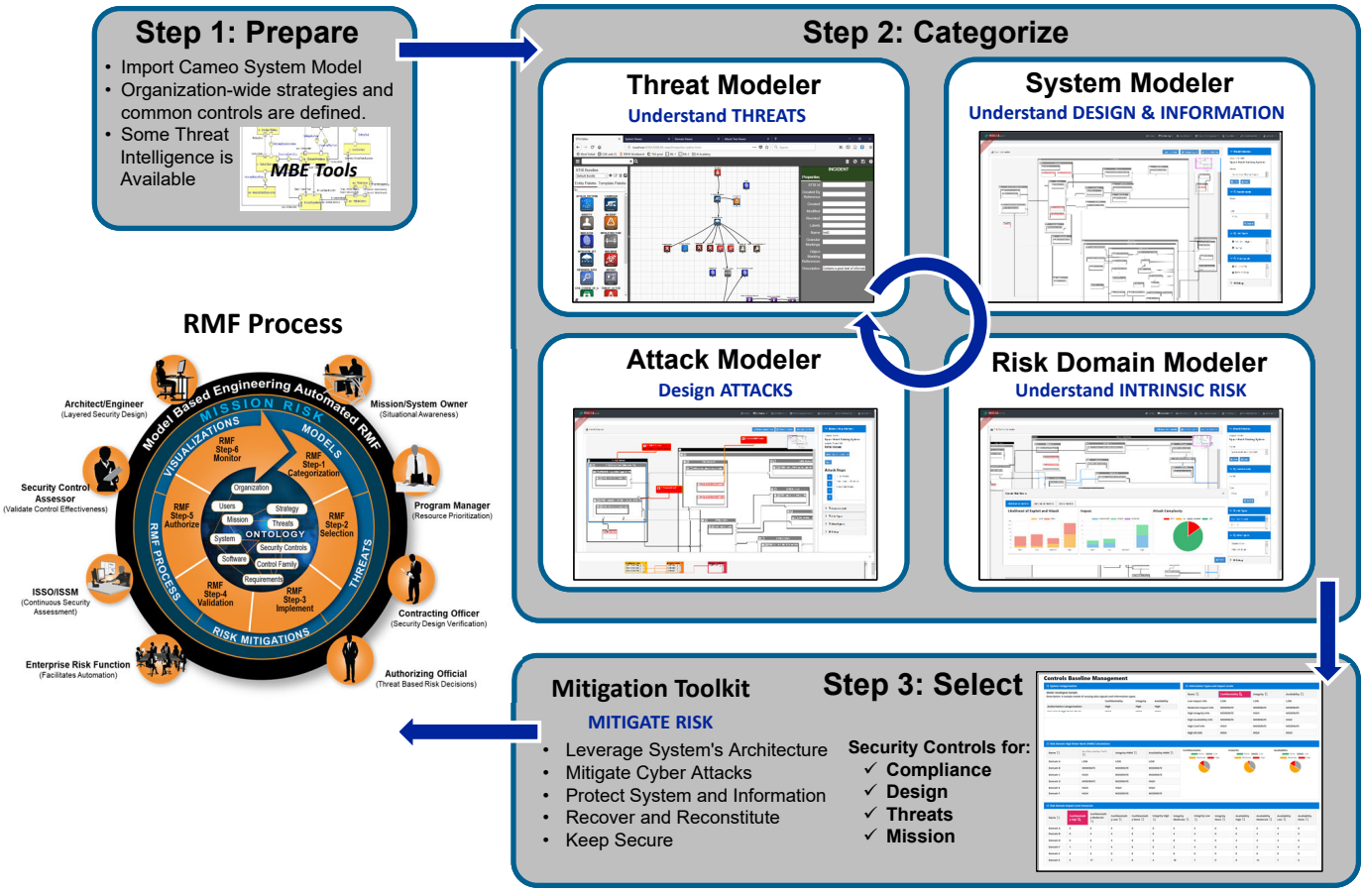
Risk-Domain Modeler

A novel built-for-purpose graphical modeler specifically designed for the entire team to understand the traceability of system design, threat, and security attributes for cybersecurity risk analysis. The Risk-Domain Modeler establishes a risk view that provides impact traceability and evidenced-based situational understanding of:

- System elements, stakeholders, and authorization boundaries
- System design risk and requirement alignment
- System design intrinsic risk
  - Potential weaknesses, vulnerabilities, and attack patterns
  - Likelihood of exploitation or attacks
  - Impact Assessment and mitigation strategies

Mitigation Toolkit

A toolkit and workflow for cybersecurity professionals streamlining the RMF process. This toolkit calculates information impact level high watermarks, supports system categorization, security controls selection, allocation, tailoring, supplement, and more.



For more information, please contact:
Northrop Grumman Mission Systems Rusty Toth
Phone: 703-949-2335
roger.toth@ngc.com

northropgrumman.com

NORTHROP GRUMMAN