# Cybersecurity Specialization: Threat Modeling

**Durée: 2 Jours** **Réf de cours: GK840103** **Méthodes d'apprentissage: Classe à distance**

## Résumé:

**Understand and apply threat modeling techniques to enhance cybersecurity.**
**Cybersecurity Specialization:** Threat Modeling dives into the critical practice of threat modeling, a key component in modern cybersecurity strategies. Participants will learn to identify, analyze, and mitigate potential security threats in complex systems. The course covers various threat modeling frameworks such as STRIDE, PASTA, and VAST, and their application in different contexts, including microservices, containerized architectures, and IoT systems. By integrating threat intelligence and advanced risk assessment techniques, students will gain the skills to develop robust threat models that enhance security operations and DevSecOps pipelines.
Throughout the course, attendees will engage in hands-on exercises using tools like OWASP Threat Dragon and Microsoft Threat Modeling Tool to create and evaluate threat models. They will also explore the role of threat intelligence in dynamic environments and learn to automate threat modeling processes within CI/CD pipelines. By the end of the course, participants will be equipped to design and implement effective threat models for various scenarios, ensuring comprehensive security coverage for their organizations.
This course is ideal for professionals looking to deepen their understanding of threat modeling and its practical applications in real-world environments. Join us to enhance your cybersecurity skills and stay ahead of emerging threats.

## Public visé:

The ideal learner will have at least 1 year of experience in their job role and understand Cybersecurity Principles. Security Engineers, IT Architects, System Administrators, Software Developers, Cloud Engineers, DevOps Engineers etc.

## Objectifs pédagogiques:

- Describe the concepts of Security as Code and DevSecOps.
- Explain the characteristics of advanced persistent threats, social engineering, supply chain attacks, and insider threats.
- Compare and contrast different threat modeling frameworks like STRIDE, PASTA, and VAST, and their applicability in complex contexts.
- Analyze and evaluate different threat modeling techniques and tools for modeling microservices and containerized architectures, hybrid, multi-cloud, and edge computing environments, and IoT systems.
- Summarize and interpret the role of threat intelligence in dynamic environments and the ways to integrate it into threat models and security operations.
- Create attack trees and threat models for distributed systems using open-source tools like OWASP Threat Dragon and Microsoft Threat Modeling Tool.
- Adapt multiple frameworks to a sample complex system and develop a threat model for a multi-cloud architecture or IoT ecosystem.
- Implement advanced risk assessment techniques for a complex system, map threat models to security controls, and develop a threat model for a microservices-based app.
- Evaluate the effectiveness of different threat modeling tools and techniques to enhance static and dynamic code analysis and tool compatibility and limitations.
- Analyze and compare the characteristics of different attack chains, such as APTs and ransomware, and develop threat models for specific attack vectors.
- Assess the strengths and weaknesses of group-based threat modeling activities and provide constructive feedback to peers.
- Design a threat model for Zero Trust policies, integrate it with SOAR tools, and automate threat modeling in a DevSecOps pipeline.
- Develop adaptable and reusable threat models in Agile using modular approaches and reusable templates for microservices.
- Build and align a threat model with a sample application SDLC and create an iterative feedback loop for security improvement.
- Critique and analyze the success stories and lessons learned from case studies of CI/CD integrations in large organizations.
- Evaluate the appropriateness of different threat modeling frameworks, techniques, and tools in different complex contexts, and propose solutions to mitigate identified security threats.

## Pré-requis:

- Basic Knowledge of IT Infrastructure and Systems
- Experience with Risk Management or Vulnerability Assessments (Optional but beneficial)
- Familiarity with Security Tools (Optional)

## Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- 9701 - Cybersecurity Foundations
- G013 - Formation CompTIA Security+

## Contenu:

Introduction to Advanced Threat Modeling

Review of STRIDE, PASTA, and VAST in complex contexts

Integrating threat modeling with attack trees, attack vectors, and data flow analysis

Threat modeling for large-scale distributed systems

Combining multiple frameworks for a holistic approach

Threat modeling for hybrid, multi-cloud, and edge computing environments

Advanced techniques for modeling microservices and containerized architectures (e.g., Kubernetes, Docker)

Modeling for IoT systems: securing device communication and protocols

The role of threat intelligence in dynamic environments

Using Open-Source and Commercial Threat Intelligence Feeds

Integration of threat intelligence into threat models and security operations

Automating threat intelligence collection for continuous threat modeling updates

Quantitative vs. Qualitative Risk Assessment

Advanced risk prioritization: Bayesian networks, Monte Carlo simulations, and decision trees

Using threat modeling results to drive prioritization of security controls

Real-time risk assessment tools and technologies

Key principles and strategies of Zero Trust

Threat modeling for Zero Trust: securing identity, authentication, and access controls

Integrating threat modeling with Security Automation and Orchestration (SOAR)

Automating threat modeling in a DevSecOps pipeline

Security as Code: Embedding Threat Modeling into Automated Workflows

Integrating Threat Modeling Tools with DevSecOps Pipelines (e.g., Jenkins, GitLab)

Continuous Threat Detection and Monitoring Using Automated Threat Models

Case Studies of CI/CD Integrations in Large Organizations

Lessons learned and best practices

Threat Modeling in Agile and Scrum Teams

Modeling Security Risks in Rapidly Changing Architectures and Microservices

Techniques for Creating Adaptable and Reusable Threat Models in Agile

Collaboration Between Developers, Security, and Operations Teams

Best Practices for Embedding Threat Modeling at Each Phase of the SDLC

Threat Modeling Tools and Techniques to Enhance Static and Dynamic Code Analysis

Continuous Feedback Loops: Incorporating Findings into Subsequent Development Phases

Advanced Persistent Threats (APTs): Threat Modeling for Long-term, Sophisticated Attacks

Social Engineering, Supply Chain Attacks, and Insider Threats Modeling

Modeling for Advanced Malware and Ransomware Threats

Simulating Complex Attack Chains with Attack Trees and Kill Chains

Group-based Threat Modeling: Collaborative Analysis of a Multi-layered Enterprise System

Presentations and Peer Reviews of Group Models

## Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement