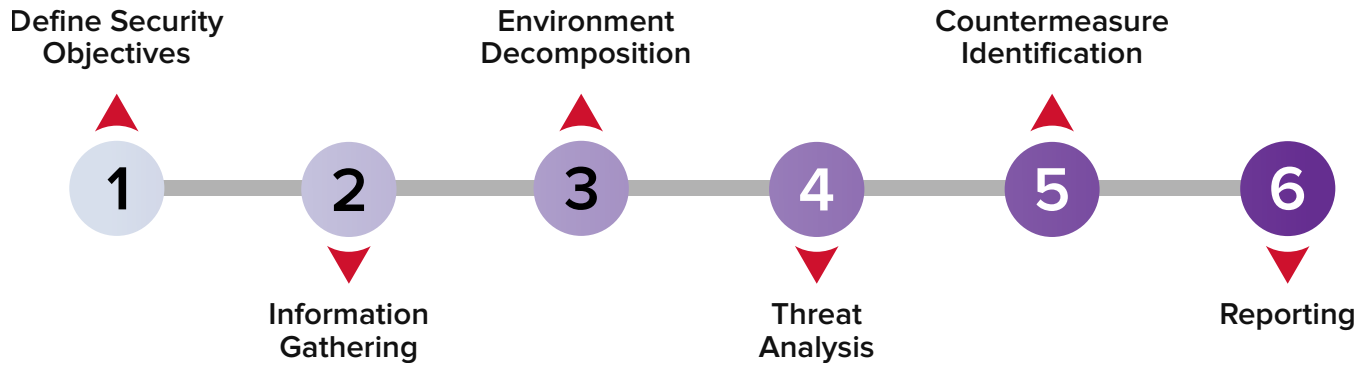
NETSPI™

Threat Modeling

Identify potential threats and gain actionable information to enable strategic security decision-making.

NetSPI's Threat Modeling service takes a holistic approach to identifying potential threats to your company's systems and applications. Leveraging a proprietary methodology developed from over 20 years of hands-on penetration testing experience, we provide a detailed technical analysis of your environment. During each engagement you will gain a comprehensive set of deliverables that enable stakeholders to make strategic decisions based on prioritized vulnerabilities, enumerated attack scenarios, and customized remediation recommendations.

NetSPI's 6-Step Threat Modeling Process:



1. **Define Security Objectives:** Establish specific security objectives and prioritize in alignment with your company's overall mission and risk tolerance.
2. **Information Gathering:** Collect documents and conduct interviews with stakeholders such as developers, project managers, and business owners to understand the architecture and context.
3. **Environment Decomposition:** Diagram the deployment models, enumerating the components and information flows in each environment and delineating trust zones.
4. **Threat Analysis:** Define attack scenarios based on assets, environment, and business risks leveraging our comprehensive threat library, and enumerating and prioritizing threats.
5. **Countermeasure Identification:** Enumerate existing threat mitigation controls and assess residual risk.
6. **Reporting:** Build threat traceability matrix mapping current threats to components, assets, controls, and trust zones. Unmitigated threats are then summarized with supplementary information.

NETSPI™

Collaboration

We know there is no one-size-fits-all approach to threat modeling, so we work with you and your team to build a custom approach to each engagement.

Customization

We incorporate your preferred processes to target unique business risks, goals, and regulations, providing information that empowers security decision making.

Consistency

We use a combination of threat modeling methodologies developed by NetSPI and other widely adopted methodologies (STRIDE, PASTA, etc.) to provide top-quality and in each engagement.

NetSPI Exclusive Human Impact

- **Real-Time Reporting –** Get notified of vulnerabilities in platform as they are found.
- **Remediation Guidance –** Vulnerabilities are delivered with remediation instructions and consultant support.
- **Project Management and Communication –** Effortlessly assign responsibilities, track remediation status, communicate with teams, and more.
- **Track and Trend Data –** Analyze findings and discover trends over time.

To learn more about NetSPI's Threat Modeling Service, or any of our other offerings, visit www.netspi.com or contact us.

Platform Driven, Human Delivered

ASM | BAS | RESOLVE

Attack Surface Management • Breach and Attack Simulation • Penetration Testing as a Service
Application Pentesting • Cloud Pentesting • Network Pentesting • AI/ML Pentesting • IoT Pentesting
Blockchain Pentesting • SaaS Security Assessment • Secure Code Review • Cybersecurity Maturity
Threat Modeling • Red Team Operations • Social Engineering • Strategic Advisory

About NetSPI:

NetSPI is the global leader in offensive security, delivering the most comprehensive suite of penetration testing, attack surface management, and breach and attack simulation solutions. Through a combination of technology innovation and human ingenuity NetSPI helps organizations discover, prioritize, and remediate security vulnerabilities. Its global cybersecurity experts are committed to securing the world's most prominent organizations, including nine of the top 10 U.S. banks, four of the top five leading cloud providers, four of the five largest healthcare companies, three FAANG companies, seven of the top 10 U.S. retailers & e-commerce companies, and many of the Fortune 500. NetSPI is headquartered in Minneapolis, MN, with offices across the U.S., Canada, the UK, and India.