



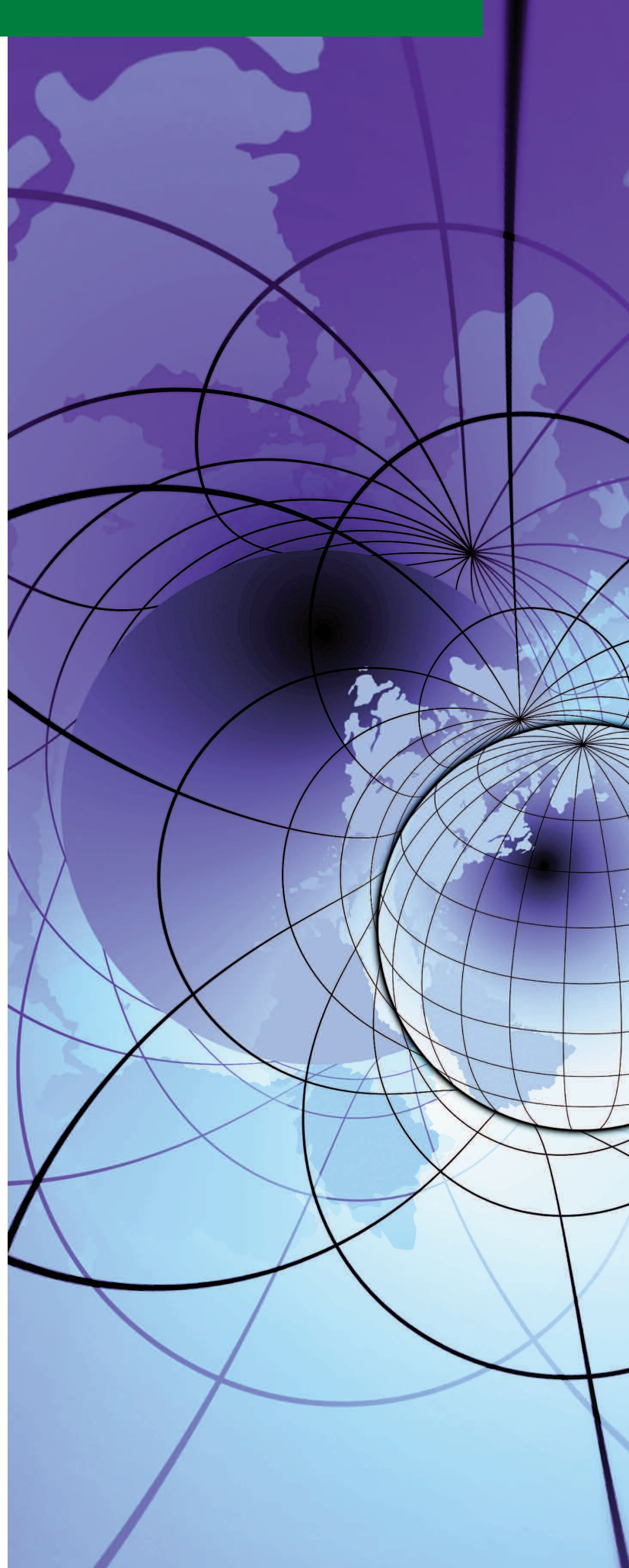
Security Threat Modeling

For many forward-looking organizations, identifying threats helps to develop realistic and meaningful security requirements and countermeasures. This can prove to be particularly useful as—if the security requirements are faulty—the assumption of security for the infrastructure is faulty, and thus risk management cannot be assumed. Proper identification of threats and the appropriate selection of countermeasures help to reduce the ability of attackers to misuse a system. The Patriot Security Threat Modeling service looks at the infrastructure from an adversary's perspective to help identify and anticipate attack scenarios and goals and determine answers to questions about what the system is designed to protect, and from whom.

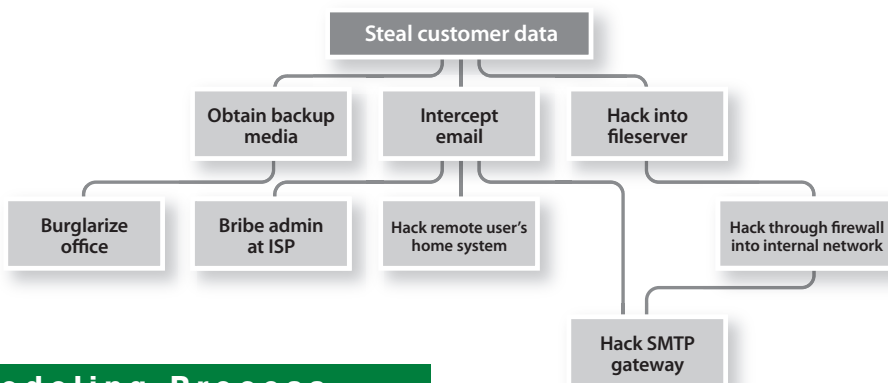
Any type of system can benefit from threat modeling. Our Threat Modeling service consists of the following three high-level steps: characterizing the system, identifying assets and access points, and identifying threats. We're able to aggregate SEIM, network anomaly detection, and network behavioral analysis data to model threat scenarios and determine attack likelihoods. We are then able to predict what attacks may occur, from where, and what particular outcomes may result. We employ various tools and processes to measure scenarios and outcomes, for example:

- **Spoofing:** When using someone else's credentials to gain access to otherwise inaccessible assets
- **Tampering:** When one changes data to mount an attack
- **Repudiation:** Which occurs when a user denies performing an action, but the target of the action has no way to prove otherwise
- **Information Disclosure:** The disclosure of information to a user who does not have permission to see it
- **Denial of Service:** Reducing system/network availability
- **Elevation of Privilege:** Occurs when an unprivileged user gains privileged status

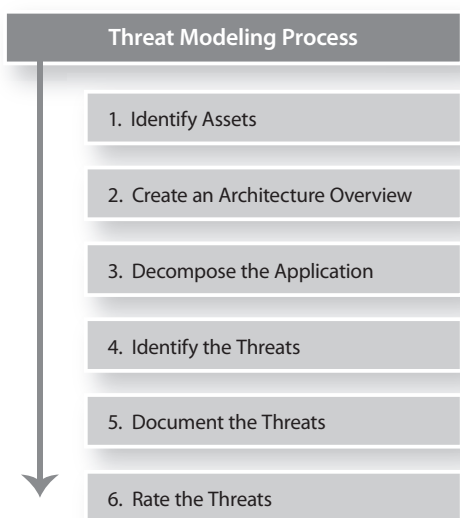
The Patriot Security Threat Modeling service leverages the most current analytical tools to determine (a) the level of threats that exist, and (b) the extent of countermeasures that need to be put into place.



Attack Tree



Threat Modeling Process



Enterprise Lifecycle Security Specialists

Founded in 1996, Patriot Technologies is a privately owned, small business headquartered in Frederick, MD serving government and commercial organizations worldwide. To learn more about how Patriot's Professional Services can benefit your enterprise, call **301-695-7500** or visit **www.patriot-tech.com**.

GSA# GS-35F-4363D
 We Accept IMPAC Visa Card
 USDA BPA#AG-3142-B-08-0018
 ESI SmartBUY# FA8771-07-A-0307 (Check Point)
 NIH SmartBUY BPA# HHSN 263999900685B
 BPA# W91QUZ-06-A-0005 (Websense)
 SAIR SmartBUY BPA# GSQ0009AE0013 (BigFix)
 Consulting and Technical Services (CATS) Contract
 MD CATS Contract# 050R5800338

Other vehicles available: Encore II, Firstsource, ITES-2H, ITES-2S, NETCENTS, SEWP, Tiger, Treasury Commercial Vehicle (TCV), GSA Stars, Networx, SDVOB and 8a partnerships, Arete Government Solutions, Leasing options

CAGE Code: 07FD4
 DUNS: 933945248
 Federal ID# 52-1957100



GSA Agent and Teaming Programs Available



Phone **301.695.7500**

Fax **301.695.4711**

01/12