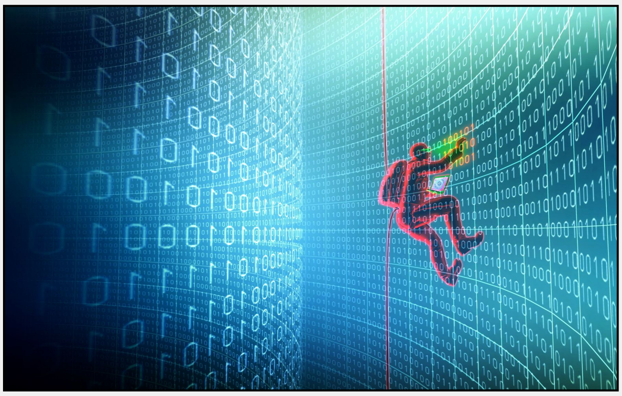
Hippogriff LLC - Threat Modeling Fast Look

Be compliant. Be prepared. Stay ahead of increasing security challenges. Remain functional. Maintain customer confidence. Demonstrate marketplace competence. Establish a full field of view to allow for more efficient network penetration tests.



Threat Modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. In this context, a threat is a potential or actual adverse event that may be malicious (such as a denial-of-service attack) or incidental (such as the failure of a storage device), and that can compromise the assets of an enterprise.

Threat Vector Tiers

- Perimeter Defenses
- Network Enumeration
- Authentication
- Local System Security
- File-Level Security
- Direct Threat Security

Areas of Focus

- Network Device Security
- Web Security
- Operating System Security
- Internal Network Security
- Workstation and Endpoint Security
- Media Storage and Decommissioning
- Third Party Risk Management
- Perimeter Security
- Application Security
- Physical Security
- Database Security
- Internet of Things Security
- Digital Espionage Countermeasures
- Human Domain Behavioral Profiling

State of Compromise

- Detect/Discover
- Triage/Contain
- Respond/Remediate

Security Lifecycle

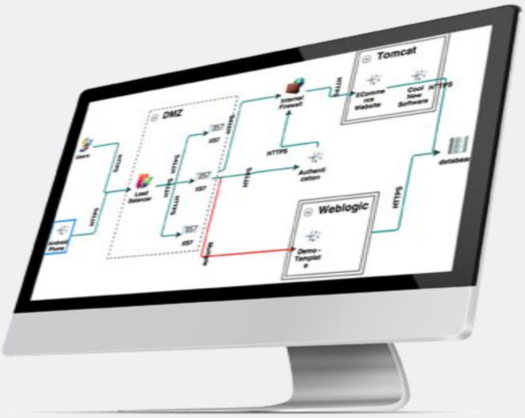
- Correlate/Enhance
- Prevent
- Detect

“In every respectable organization there are some sort of policies and procedures. Those need to be identified for compliance purposes. In reality, almost one-fourth of the defensive capabilities corporations have in place fail to meet the minimum security standards. In the opinion of Art Gilliland, a senior vice president of security products unit of Hewlett-Packard, “[t]he reason for that is that they were often pushing to meet a policy – checkboxing for compliance.”

Amassing detailed information about real cyber incidents (e.g., URLs to malicious links, phishing email header and content, and uncovered hostile Command and Control (C2) infrastructure of domain names and IP addresses) is the first step. The focus should fall on targeted threats existing in reality, and scope settings need to filter out those perceived as such but not real, which can merely distract your attention from other ongoing security affairs.

An IT analyst must have unrestricted access to data in order to transform it into intelligence. Sources of information are, for example, intrusion incidents, detection system logs, firewall logs, the reverse engineering of malware, open source Internet searches, honeypots, digital forensic analysis, etc. Of course, one source simply cannot provide all of the information needed for a thorough threat analysis, and the analyst should incorporate multiple data wells seamlessly. Once all corporate policies and procedures are collected, they should be examined to show whether they match the compliance level in the organization. Consequently, logically processing vast amounts of data and thinking critically are qualities that will form a good cyber analysis.”

- Dimitar Kostadinov, InfoSec Institute, July ‘14



The key to Threat Modeling is to determine where the most effort should be applied to keep a system secure. This is a variable that changes as new factors develop and become known, applications are added, removed, or upgraded, and user requirements evolve. Threat Modeling is an iterative process that consists of defining enterprise assets, identifying what each application does with respect to these assets, creating a security profile for each application, identifying potential threats, prioritizing potential threats, and documenting adverse events and the actions taken in each case.

Computer Technology Protection Services

1-866.273.4831
inquiry@hippogriff.tech
Hippogriff.TECH • Hippogriff.IO