Threat Modeling automation, the CyberSage way

Scale up threat modeling with AI, consistent quality

CyberSage conducts security risk analysis for a business feature (e.g, customer login on a web application) and identifies possible security weaknesses introduced by certain design choices, the attack vectors which may exploit such weakness and recommends technical remediation.

Such automation enables software development communities and other information technology disciplines to scale up security risk analysis with threat modeling methodology.

In addition, it enables enterprises to achieve consistency in such analysis by using common profiles, models and rules. The consistency is a common draw-back for security analysis done by a team of analysts, whose skill set and perspectives may vary.

Produce contextualized and accurate threat modeling results

CyberSage produces contextualized threat model of the technology asset tailored for the risk profile of the enterprise.

CyberSage keeps the enterprise and the technology asset’s contextual information such as inherent risk assessments (IRA), threats and existing controls in Threats & Risk Repo. CyberSage also obtains more contextual information from users (if required in inference). Such contextual information are used in the inference to produce tailored threat model aligned with these contextual information.

Enable the Threat modeling to be driven by business value and risk, instead of driven by technological stacks alone.

CyberSage supports the threat modeling methodology, where the threat model is derived from business values and the threats to these values.

Customize threat modeling profiles for enterprise' specific business and risk profile

business and risk profile can be different in each enterprise. It is possible that the out-of-box threat modeling profile needs to adjust to fit the specific scenarios of an enterprise.

CyberSage’s threat modeling engine supports changes in these profiles with rule changes in its rule interface. The rule changes are independent from CyberSage core software and therefore can be done quickly.

The following customizations are supported:

update existing threat modeling profile

Rule changes can be done to make profile fit better?

For instance, one of the out-of-box threat modeling profile is for the business feature which supports users to update their profile (e.g contact information).

need example?

create new threat modeling profile

When the enterprise has unique business features that are not supported by the out-of-box profiles, new profiles can be created with the rule engine and new rules.

Embed security into development life-cycle management

CyberSage enables IT(information technology) teams, such as software development and other IT design/build team to make the threat modeling and remediation part of their development life-cycle. This allows the prevention or remediation of security weakness starts early in the life-cycle, reduces security risks and remediation costs.

CyberSage integrates seamlessly with mainstream IT management tools such as Jira to enable users to manage threat modeling part of their life-cycle.

Secure cloud assets with threat modeling

Automate Threat Modeling of Cloud Infrastructure by integrating threat modeling engine with Cloud infrastructure API and identifies specific Cloud assets and security weakness in their configurations that may facilitate Cyber attacks.

Present the threat model in a visual attack tree

Associate the threats (the objectives of the attackers), the business profile and the applicable attack vectors by building a tree structure graphic representation.

Such knowledge helps users to design and validate remediation plans for these attack vectors.

it facilitates further analysis of security weaknesses that depends on the causing factors which enables the attack vectors.

Automate security issue risk rating and threat impact analysis aligned with enterprise’s business profile

The threat modeling engine uses the risk and business profile (e.g, confidential requirements of an application) as threat modeling input. It also automates the risk rating with ORM (operational risk management) model and incorporate both the impact and likelihood of identified security weakness.

CyberSage incorporate threat and impact analysis of IT assets in security issue risk rating.

Please see details here automate security issue risk rating.

Build for developers to embed security as part of development

Jira Single Sign On and integration

Developers sign in CyberSage using their Jira account with SSO. CyberSage automatically creates Jira work items to track and remediate security weaknesses identified in threat modeling. These seamless integration enables developers to work on security work items as part of their workflow, the same way how they work on business user stories.

And developer only needs a browser to leverage the power of CyberSage.