securiCAD Vanguard

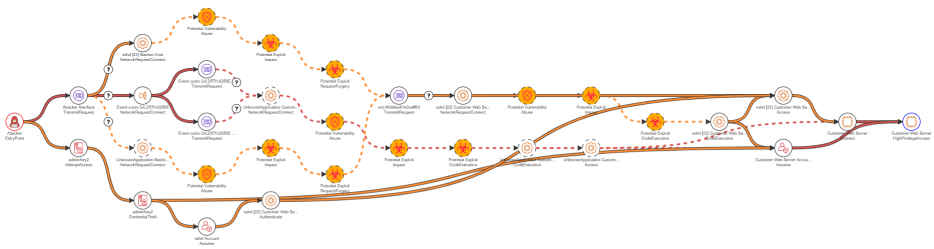
ATTACK SIMULATION-BASED SECURITY ANALYSIS FOR AWS

securiCAD Vanguard is fully automated and non-disruptive. The attack simulations are conducted on virtual models that are automatically generated and will not interact with the actual environment in any way.

securiCAD Vanguard leverages the vast amount of data available in AWS to automate threat modeling of cloud environments and bring unprecedented insight with cutting edge attack simulations. securiCAD Vanguard allows developers and cloud security architects to get an overview of the cyber security characteristics of their AWS environment.

Attack simulations and automated threat modeling will enable you to automatically simulate attacks on a virtual model of your AWS environment. By providing securiCAD Vanguard with read access to standard AWS APIs, a model of your environment is automatically built and visualized.

By simulating attacks on the model, securiCAD Vanguard will assess your AWS configuration, existing vulnerabilities and misconfigurations. AWS concepts, services and their configurations are represented in the virtual model.



Find the most critical paths from the attacker's entry point to your high value assets and the chokepoints (key assets) in your architecture that the attacker is expected to exploit to reach the high value assets.

» KEY BENEFITS

AWS Integration
Specifically developed and fully integrated with Amazon Web Services

Non-disruptive
Attack simulations are conducted on digital twins

Automated
Fully automated model generation, visualization and attack simulations

Secure
No installation or privileged access needed. Required data is collected through read access to standard AWS APIs

No data is saved
No sensitive data is saved, read our data policy here

» WHAT IT DOES

Prevent breaches by analyzing your AWS configuration, allowing you to detect misconfigurations, potential lateral movements and to prioritize vulnerabilities

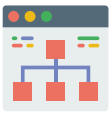
Generate and visualize a digital twin of your AWS environment and run attack simulations, to get reports with the most likely attack paths, weak spots and risk exposure

Secure and on-demand analysis of AWS configurations including IAM, VPC, EC2, S3, Inspector and more.

KEY FEATURES

1:1 Mapping
AWS concepts, services and their configurations are represented in the virtual models

Chokepoints
Find chokepoints (or key assets) in your architecture that the attacker exploits to reach high value assets



Attack Scenarios
Choose between different attack scenarios and threat profiles

Vulnerability Scanners
Import data from vulnerability scanners to asses and prioritize current software vulnerabilities

Critical Paths
Find the most critical paths from the attacker's entry point to your high value assets

Model Visualizations
A virtual model of your AWS environment is automatically generated and visualized

Structural Vulnerabilities
Find the structural weaknesses in your architecture

AWS Marketplace
securiCAD Vanguard is now available as a SaaS in AWS Marketplace.

About foreseeti
foreseeti, Europe's leading provider of Automated Threat Modeling and Attack Simulation solutions, is a Swedish technology company headquartered in Stockholm. Our flagship products, the securiCAD solutions, empower IT decision makers with insight to the cyber risk exposure and resilience of their IT architectures, uncovering critical paths to high value assets and weak spots in the architecture so that proactive actions can be taken where they really matter.

For more information about foreseeti and our products, visit:

www.foreseeti.com

aws partner network
Select
Technology
Partner