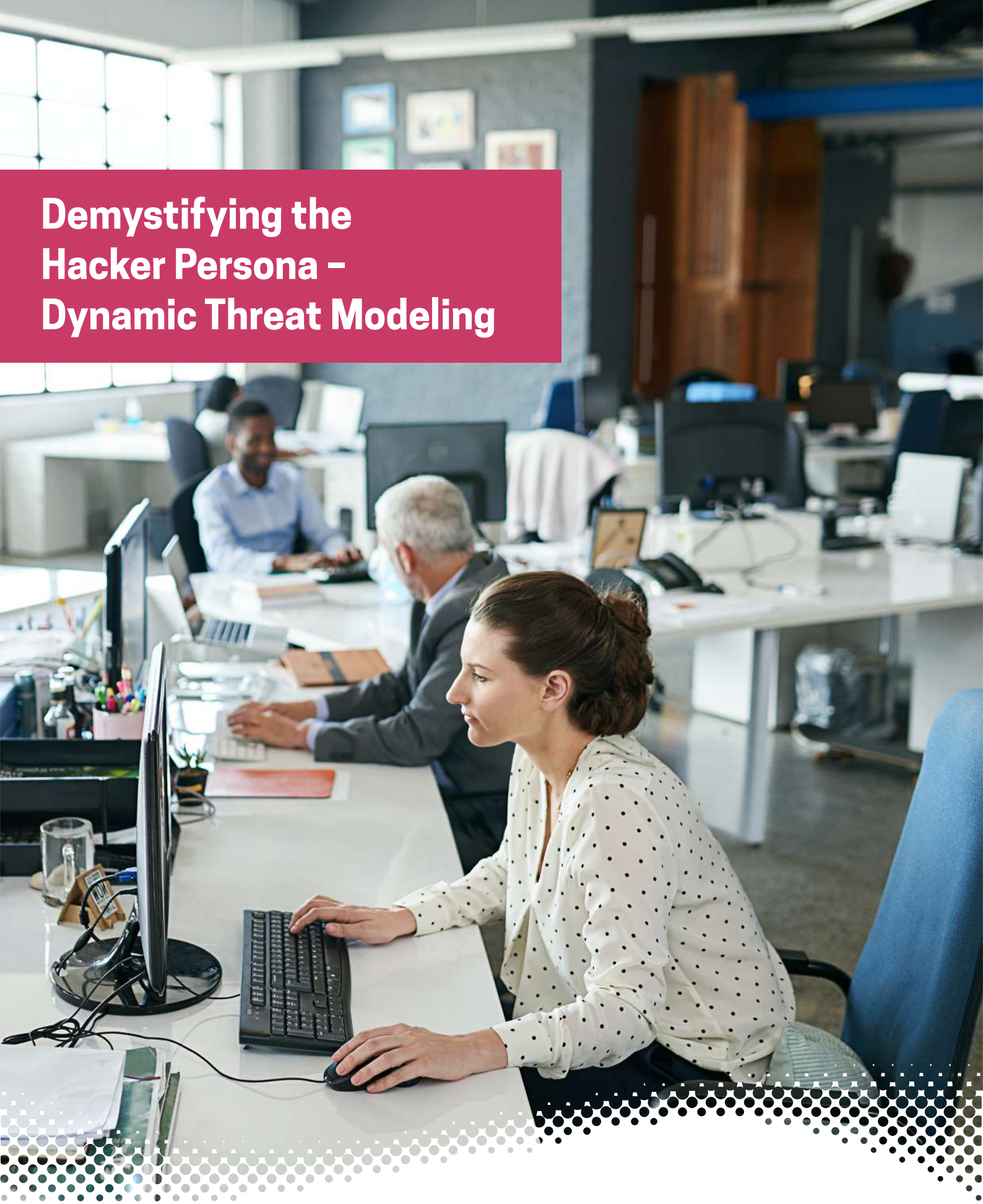
# Demystifying the Hacker Persona – Dynamic Threat Modeling



wipro

## Overview

As markets across the globe continue their digital-first approach toward empowering customers to meet demand at scale, the resulting IT landscape must become increasingly sophisticated and complex to prevail. Although digital transformation promises to drive business initiatives, cybersecurity concerns keep technology leaders up at night. As DevSecOps, cloud transformation themes, and agile initiatives fast-track IT and business, security considerations are often left behind as leaders focus on delivery.

Gartner predicted that "60% of digital business would suffer service failures by 2020 due to inability of security to manage digital risk." Today, threats continue to increase along with the evolution of the technology landscape, and threats can surface from external sources or within an organization, causing overwhelming consequences the organization cannot afford to ignore.

Still, though, many organizations think of security as an operations responsibility or an afterthought. The concept of fostering an end-to-end security culture for development and operations teams seems like a daunting task. However, failing to do so could mean playing catch-up amid the disastrous results caused by aging security vulnerabilities.

How do we integrate development and operations processes that prioritize ongoing security awareness throughout an application's lifecycle? Ensuring security must be a consideration from the beginning stages of development, delivering secure applications without causing friction during the build and deployment processes. In this thought paper, we will summarize an approach for modeling threats by leveraging automated and manual techniques to achieve the same.

## Threat modeling simulates hacker vista

It's imperative to understand your threats in order to build secure systems and applications, all while educating development teams and embedding security culture across an organization. Threat Modeling comes as a device to find answers to simulate hacker persona such as: "How vulnerable we are to different types of cyber-attacks?" "What is the weakest link that an attacker can exploit to reach organization high value assets?" "What can we do to safeguard against these threats in the most effective way?"

Using this process, defenders can take a systematic approach to analyzing what defenses need to be included, given the nature of a system, the probable attacker's profile, likely attack vectors, and an organization's risk profile. It empowers companies to take a proactive and effective role in managing their own cybersecurity.

Threat modeling early in a development cycle promotes early detection and the alleviation of security risks, enabling economies of scale. Moreover, threat modeling fosters a culture that actively thinks about security requirements, leading to proactive architectural decisions that reduce threat lifecycles.

Considering these benefits, it's natural to wonder why more organizations aren't adopting threat modeling more readily. The adoption of threat modeling can pose challenges and discourage application owners/stakeholders, causing them to shy away from adoption and implementation cycles. In turn, this situation presents a DevSecOps paradox: "**How can we identify design-level flaws on a continuous basis during development and operations phases?**"

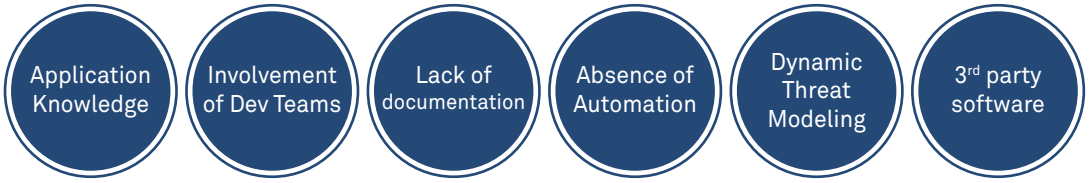



Figure 1: Application Threat Modeling Challenges

## Dynamic threat modeling

This approach is an automated modeling method that captures application insights, employing runtime application discovery, deep application forensics, and dynamic threat model generation. Automated threat modeling eliminates major challenges encountered during the threat modeling process, positioning stakeholder modelling activities as gate checks within the DevSecOps play.

**Dynamic threat modeling can be achieved with the following process:**

### Continuous Discovery Discovery

**Automated** discovery uncapping complex applications at process level and fingerprinting of application communications

### Continuous Build Build

**Automated** generation of application forensics in well structure format

### Continuous Modeling Model

**Building** detailed, granular thread model data planet, discoverting security requirement & test cases

### Continuous Mitigation Mitigation

**Easily mitigate** integration with all popular DevSecOps tools

Figure 2: Making Automated Threat Modeling a Reality

This process expedites threat contextualization and reporting exercises, rewarding security/development teams with background knowledge on application architecture, process IDs, protocols, database and API calls, session details, and more. As a result attack tree mapping can be built with a homegrown/domain-agnostic threat library or security architecture framework, and risk ratings can be converted into protection recommendations.

The well formatted structure generated during a continuous build phase can be pushed into threat modeling tools to generate an automated model, expediting instant security controls and requirement creation. The prescribed dynamic modelling approach works well in the context of legacy, cloud native, and digital landscapes with no exception to the adopted software delivery methodology (i.e. waterfall, agile, etc.). Dynamic threat modeling delivers significant benefits to the following roles within the SDLC.

### Executive Level

- Fosters the culture of communications
- Facilitates compliance/ investment decision using a risk based approach
- Improves compliance and risk reporting for C-suite

### Application Owner

- Improves visibility of flaws using Threat Contextualizaiton
- Entails prioritized list of unilikely to improbable, to not likely security risk
- Expedites decision making during development and operations phase

### Developer

- Understand multi faceted 3 tier application flows with ease
- Enhances security awareness to the developer
- Entails applications meet security triage (CIA) goals.

### Solution/Security Architect

- Offers a systematic approach to modelling known/unkown attack vectors.
- Empowers risk based approach determining security controls.
- Enables embed security DNA across Application lifecycle.

Figure 3: Significance of Threat Modeling across Various Players within an SDLC

## Conclusion

Threat modeling can serve as the bedrock for integrating security culture in the workplace, resulting in development, security, and operation teams working in tandem in a DevSecOps-empowered culture. In turn, this practice can ensure transparent governance within development and operations processes, leading to high-quality and secure applications.

On the development front, threat modeling promotes early detection, reducing threat cycles and enabling economies of scale. Moreover, the threat modeling engagement process enhances security views for various stakeholders within a Software Development Lifecycle.

Threat modeling must be the first step for any organization, versus adopting a “silver bullet” approach that oftentimes results in planting problem-specific tools -- and later discovering new problems in the overall application landscape. As markets continue adopting DevSecOps, organizations have no choice but to implement and embrace threat modeling -- starting with fostering a security culture across the organization in order to succeed.

## About the authors


### Allam Vinodh Kumar

**Practice Partner, Cybersecurity & Risk Services Wipro Ltd.**


A globally recognized Cybersecurity Assurance Evangelist, Vinodh A has more than 20 years of experience building, developing, and securing web-based software systems. As a Practice Partner for Cybersecurity & Risk Services at Wipro Limited, his technology teams launch and expand critical application security initiatives and build secure applications and infrastructures, integrating security throughout the development process.

### Arun Pillai

Arun Pillai is a Security Architect who champions DevSecOps for Security Assurance Service within Wipro's Cybersecurity and Risk Services (CRS) division. He has over 14 years of experience with a specialization in security and is responsible for evangelizing DevSecOps across Wipro. He has worked on and managed projects involving Security Architecture, Secure SDLC, Threat Modelling, Secure Coding, Penetration Testing, and Security Consulting. Arun is an ISC2 Certified Information Systems Security Professional (CISSP) and ISACA Certified in Risk and Information Systems Control (CRISC). Arun holds a Master's degree in Information Technology from Sikkim Manipal University of Science & Technology and is a TOGAF-certified Enterprise Architect for The OpenGroup.

**Wipro Limited**
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
**wipro.com**

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**

IND/TBS/MAY-DEC 2020