

# RULES OF ENGAGEMENT FOR **RED-TEAM**





## EXECUTIVE SUMMARY

### **Cyber Security is an Exponential Problem**

Red team assessments help you understand your organization's detection and investigative capabilities. Not setting the right rules and expectations when starting a Red team or Penetration Testing exercise may lead to less-than-great outcomes.

This document is an example of the rules of engagement between the Komodo Consulting Team and the Customer Teams for the Red team and Pentest exercises which will help you understand the rules of engagement for Red team exercise.

# FRAMEWORK

- **Contacts**

	Name	Email	Phone

- **Timeline**

- Activity Start Date:
- Activity End-Date:
- A red-team activity usually takes about 60 days start to end.

- **Locations**

- Komodo Offices
- Customer Europe Site
- Customer US Site

- **Status Updates**

Weekly conference will take place on Mondays &, Thursdays  
OR specify the days you want the status updates

Critical findings will be notified on a daily basis.

- **Testing Time Frame**

- During Business Hours?
- After Business Hours? E.g. Israeli GMT+2 daytime hours  
(PST night time)



On Weekends?

Doesn't Matter

- Our assumptions are that 90% of testing will be performed on Israeli daytime hours

- **Stealth/Shunning**

Testing should be performed in stealth mode

- Note that this limits the pentesters capabilities but reflects a closer to 'real life' attack simulation.


- **Permission To Test**

The Customer hereby acknowledges that Komodo's team will perform penetration testing on systems in scope (see IP range and domain lists below).

Testing may lead to system instability and all due care will be given by the tester to not crash systems in the process. However, because testing can lead to instability, and the connection between testing and system instability is sometimes loosely coupled and wrongly connected, The Customer shall not hold the tester liable for any system instability or crashes.

- **Legal Approval**

The Customer hereby approves that testing the systems in scope is approved to be legal in the state they are performed.



## PROJECT SPECIFIC

- **LIST IP RANGE AND DOMAINS IN SCOPE**

Here follows is the list of IP ranges identified by Komodo at the preliminary information gathering stage. These IP addresses will define the scope for the project. Each range is attached with its Physical GEO location.

IP/Domain	GEO	Zone

- **LEVERAGE**

In the case that a system is penetrated, how should the testing team proceed? (Check all that apply)

Perform a local vulnerability assessment on the compromised machine?

Attempt to gain the highest privileges (root on UNIX machines, SYSTEM or Administrator on Windows machines) on the compromised machine?

Attempt to proceed with the attack towards internal reachable servers

Stop and notify

- **Available Testing Environment (Check All That Apply)**

- Production Environment

- Staging Environment

- Test Environment

- Development Environment

- **EFFECTIVENESS OF DEFENSE**

- Can be defined as required

- **EXCEPTIONS**

- Modules to exclude, e.g. Mainframe server is not part of the scope.

- 1.

- 2.

- 3.

- Tests to exclude, e.g. Do not run RCE exploits in production.

- 1.

- 2.

- 3.

- Tools to exclude

- 1.

- 2.

- 3.





## ABOUT US

---

- Cyber Security Consulting since 2011
- Founded by leading consulting experts with decades of experience
- Team consists of:
  - Seasoned security specialists with worldwide information security experience
  - Military intelligence experts
- Provide services across multiple verticals – banking, insurance, hi-tech, automotive, energy, communication, critical infrastructures, healthcare, and international mega-brands

# VALUES

---





# SERVICES

We Help Our Clients Identify Their Weaknesses

## Infrastructure and Application Security



PENETRATION TESTING



RED-TEAM



APPLICATION SECURITY



CLOUD SECURITY

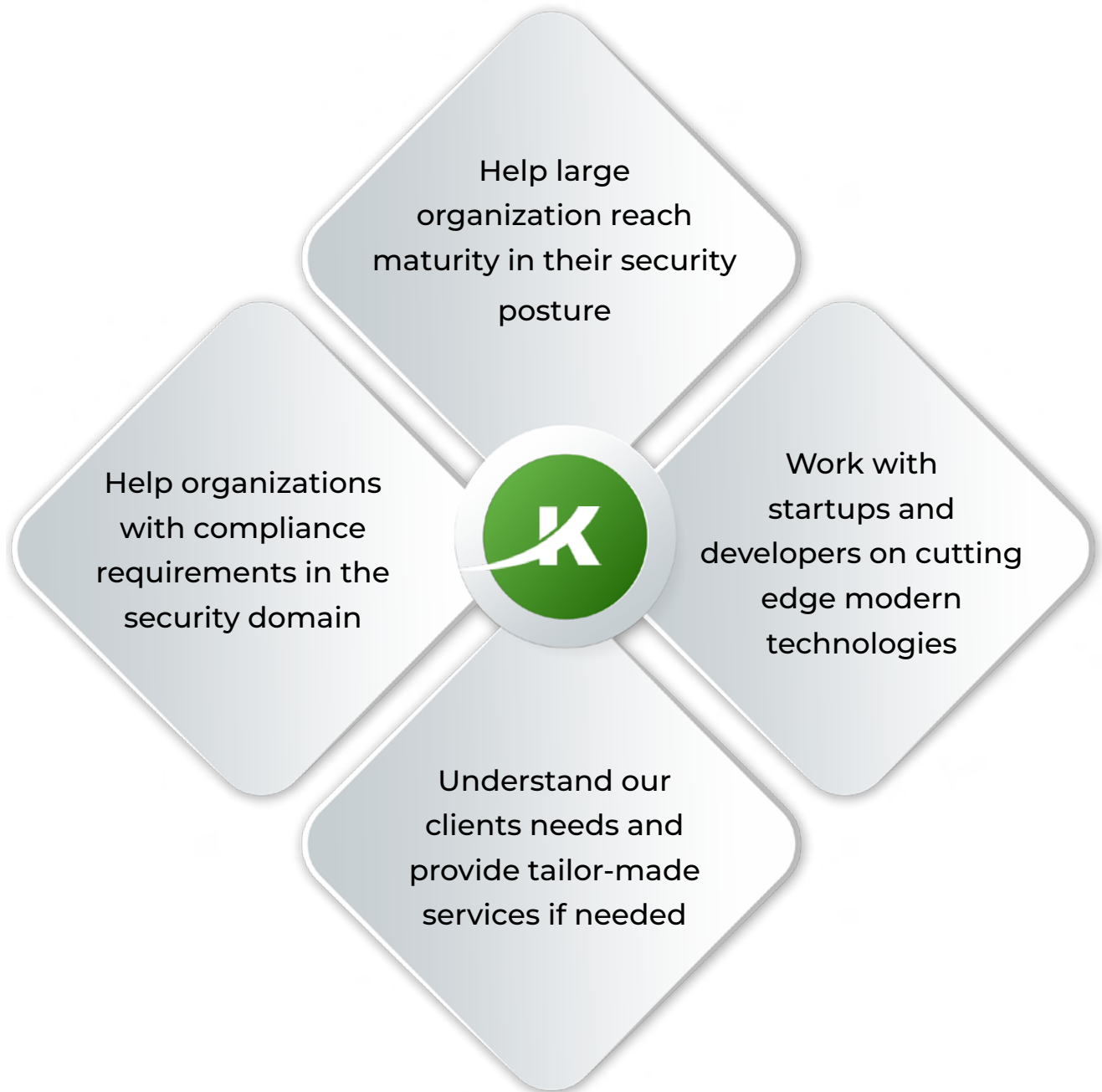


SECURITY DUE DILIGENCE



INCIDENT RESPONSE/FORENSICS

## OUR EXPERTISE



# OUR CLIENTS

We are Trusted by the World's Best Companies

## Finance / Insurance / Fintech



## Hitech / Cyber Security / Startups



## Global Brands



## Automotive



## Government



## WHAT OUR CLIENTS SAY

---



### **Komodo provides us with peace of mind**

As an organisation constantly targeted by malicious attacks, Komodo provides us with peace of mind both by securing our applications before they go into production and by acting as our incident response team at the most critical moments when we need them.

Amnon Cohen, CIO, Safecharge



### **First-class application and cyber security services**

We've been working with Komodo, our trusted advisers on application security and penetration testing, for over six years now. They consistently provide us with invaluable insights, briefings, and value. I wholeheartedly recommend them to any company in need of first-class application and cyber security services.

Amir Levi, CTO, Harel Insurance



### **Komodo presents valuable insights and advice**

Work with Komodo Consulting has always been a streamlined, efficient process. Results are always to the point and right on time, accompanied by valuable insights and advice.

Eldan Ben-Haim, CTO, Trusteer (IBM)



# ARE YOUR SYSTEMS SECURE?

Most companies take nearly 6 months to detect a data breach, even major ones.

Are your IT systems strong enough to withstand an attack and/or detect a data breach?

We help you identify critical vulnerabilities, map security vulnerabilities and suggest effective countermeasures.

**Enhance Your Security with  
Actionable Customized Recommendations**

[REQUEST FREE CONSULTATION](#)

OR

**Talk to Our Representative  
to Learn More**

USA: +1 800 409-0472 | UK: +44 20 8089 5205 | ISR: +972 9 955 5565

**Komodo Consulting**

Ramat-Gan Hamerkaz, Israel

[info@komodosec.com](mailto:info@komodosec.com)

[www.komodosec.com](http://www.komodosec.com)