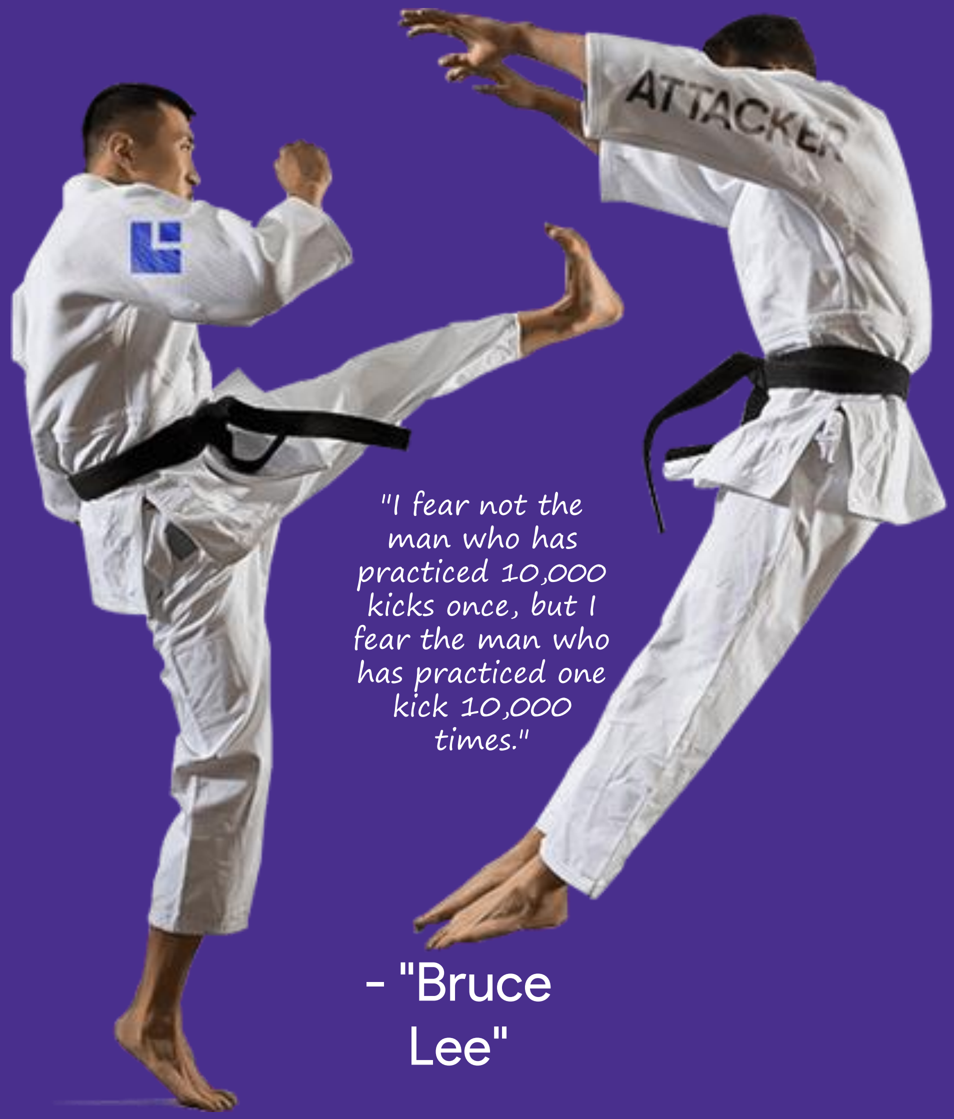
About Infopercept

Infopercept
Secure . Optimize . Strengthen

Infopercept has perfected the Cybersecurity Kick

Infopercept's Vision and core values revolve around making organization more aware and secure through the core values of **Honesty, Transparency and Knowledge,** so as to enable them to make better informed decision about their Security Practices & goals. With our synergistic vision to combine, technical expertise and professional experience we aim to further establish our place as a **one stop shop** for our clients and partners' **cybersecurity** and **accreditation** needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & continuous knowledge in the Cybersecurity domain, latest trends and Security innovations, ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.



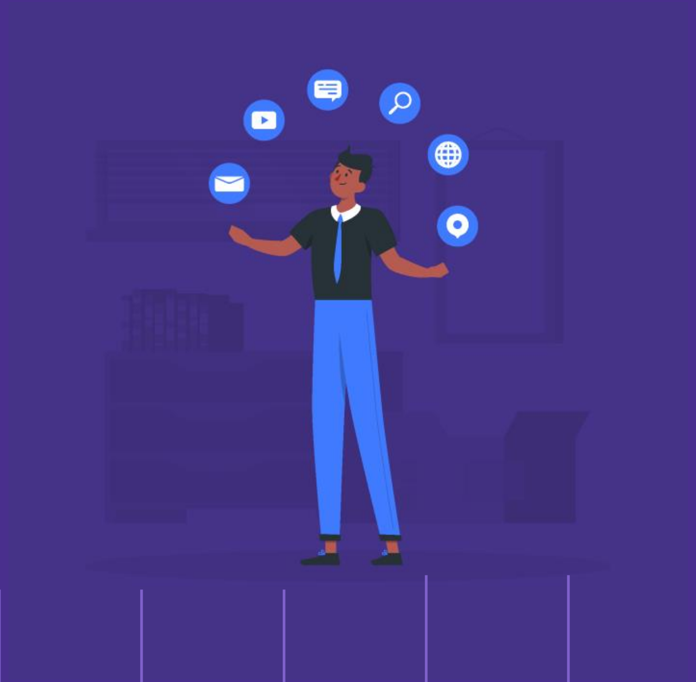
"I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times."

- "Bruce Lee"

Infopercept

Secure . Optimize . Strengthen

Skill Matrix



PCI DSS QSA

CISSP

CISM

NIST Experts

OSCP

LPT

End Point Security

Cloud Security

ISO 22301 Certified

ISO 20000 Certified

Network Security

ISO 27001 Certified

HIPAA Experts

Application Security

CEH

PMP

Infopercept

Secure . Optimize . Strengthen

Secure

S

Assessment Services

- Technical Analysis
- Process Advisory
- Implementation Services

Optimize

O

Optimization Centres

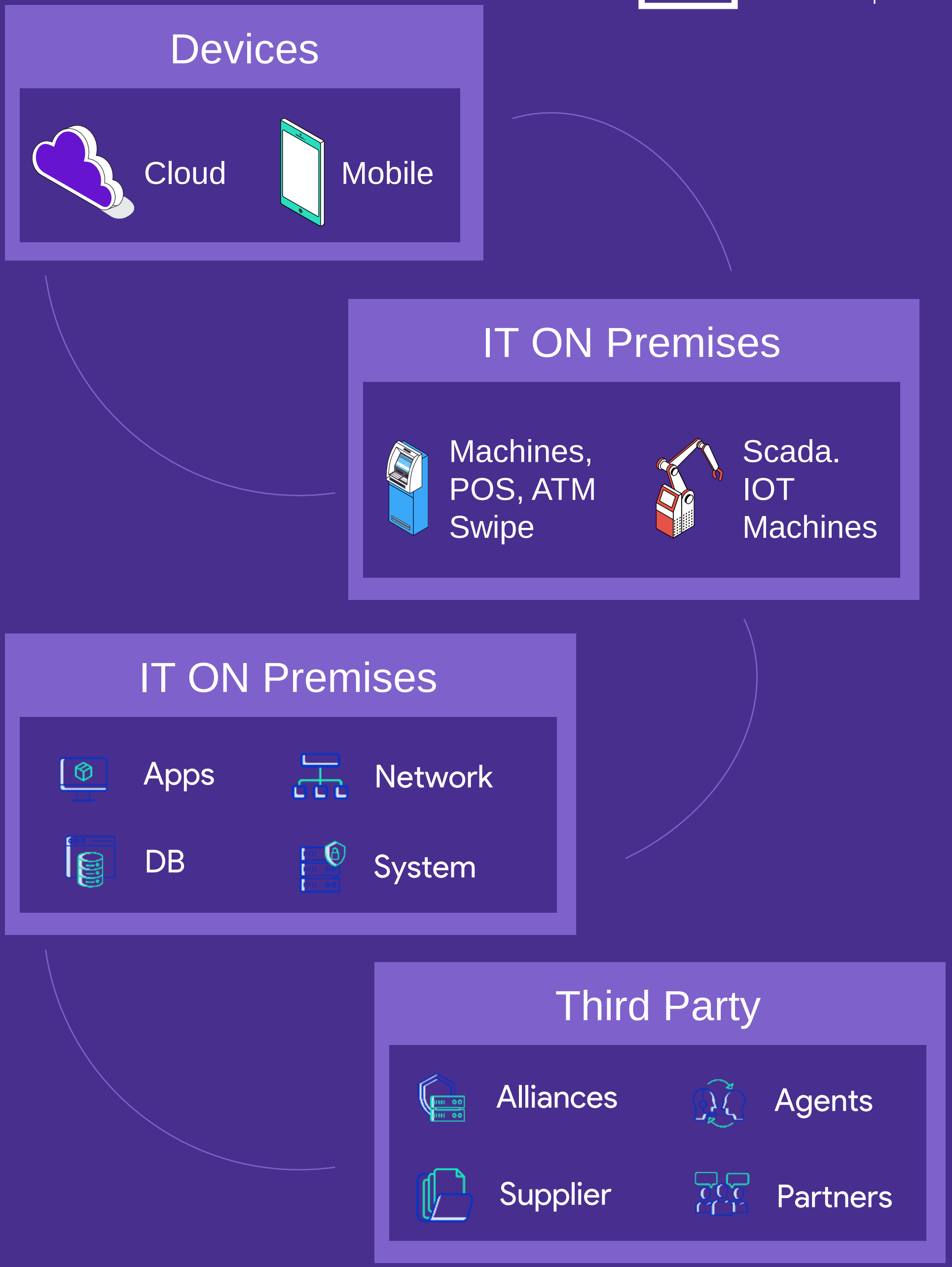
- Security Optimization Center
- Technology Optimization Center
- Compliance Optimization Center

Strengthen

S

Assessment Services

- Security Automation



Devices

Cloud

Mobile

IT ON Premises

Machines, POS, ATM Swipe

Scada. IOT Machines

IT ON Premises

Apps

Network

DB

System

Third Party

Alliances

Agents

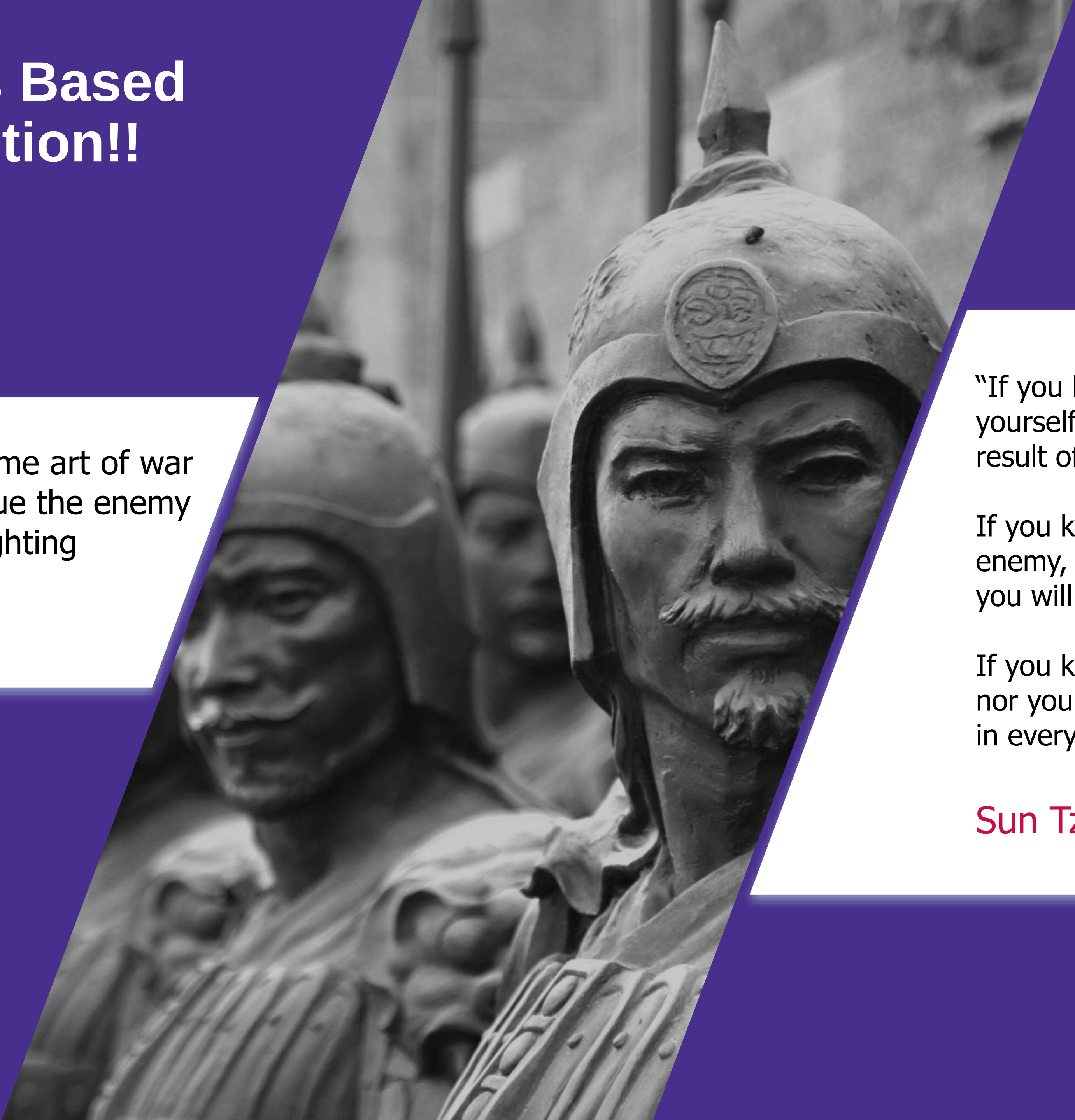
Supplier

Partners

All War is Based on Deception!!

Infopercept

Secure . Optimize . Strengthen



The supreme art of war is to subdue the enemy without fighting

Sun Tzu

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

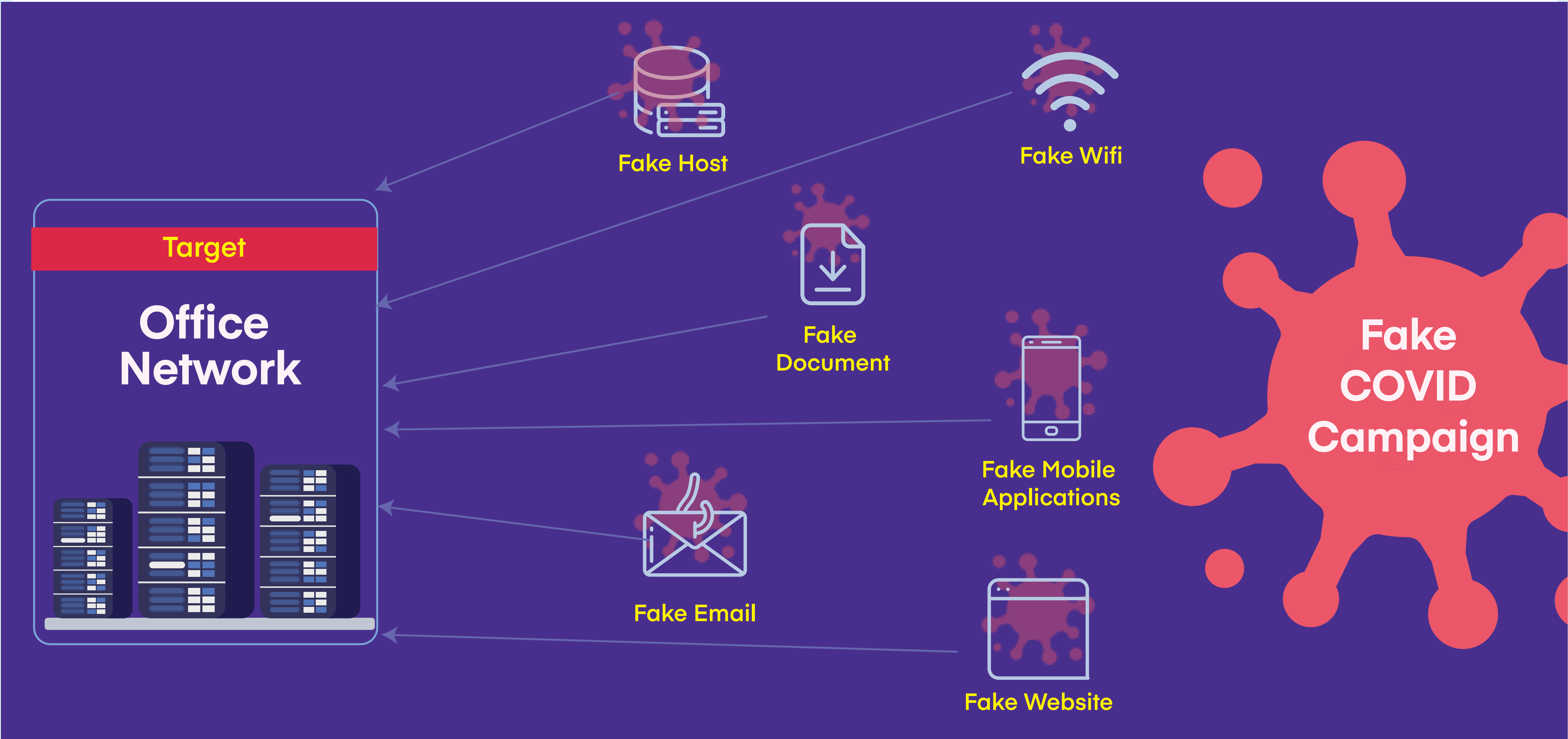
If you know neither the enemy nor yourself, you will succumb in every battle

Sun Tzu – Art Of War

Level 03

Cyber Covid (Malware) Strategy – Unknown Unknown Situation

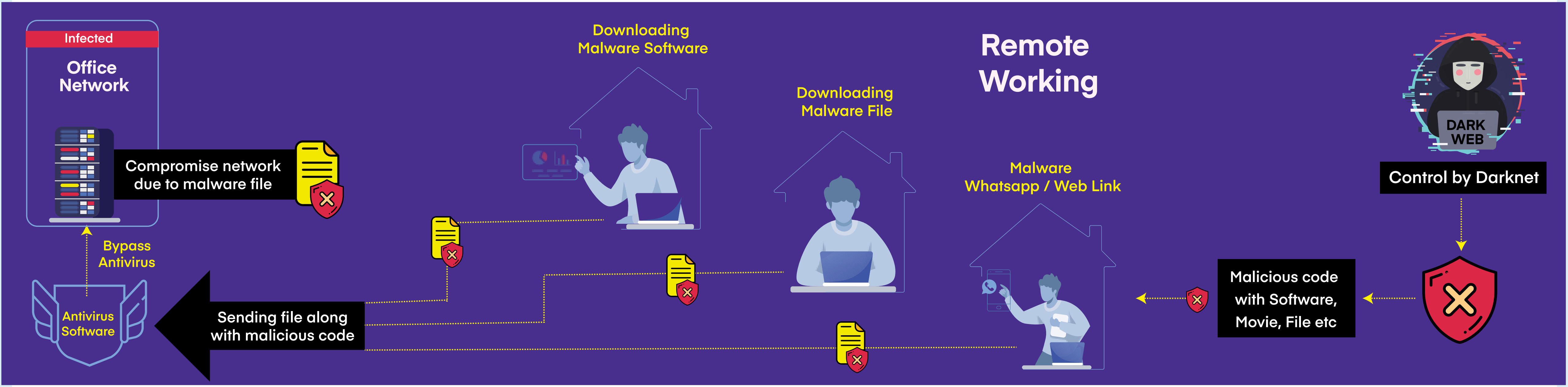
Infopercept
Secure . Optimize . Strengthen



Level 04

Unknown Unknown Situation for Business Leaders

Infopercept
Secure . Optimize . Strengthen



Infected
Office Network
Compromise network due to malware file
Bypass Antivirus
Antivirus Software
Sending file along with malicious code
Downloading Malware Software
Downloading Malware File
Remote Working
Malware Whatsapp / Web Link
DARK WEB
Control by Darknet
Malicious code with Software, Movie, File etc

CEO Concerns Intellectual Properties

1. Formulas,
2. Pricing
3. Business Secrets
4. Go-To-Market Strategy
5. Innovation etc.

Companies are ready with

1. Compliance
2. Best practice
3. secure remote user access with MFA
4. Anti-Virus?

CIO and CISO are worried about

1. Advance Attacks on endpoints
2. Existing endpoint solutions not enough
3. What will happen when this compromised system will come back to network

Level 05

Infopercept Proposed Strategy to fight at end points

Infopercept

Secure . Optimize . Strengthen

Scenario 1

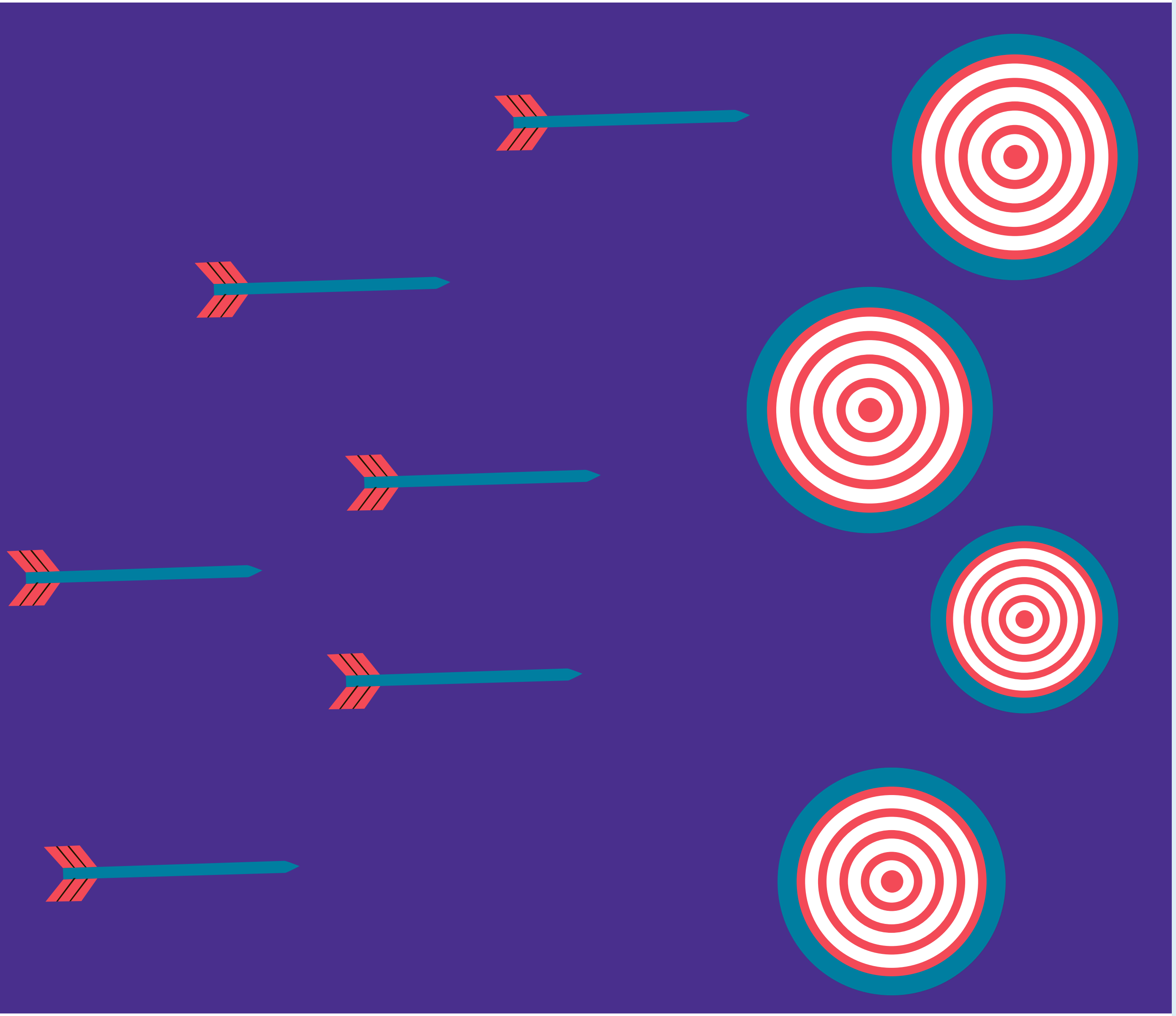
Attacker builds knowledge
about the environment

Scenario 2

In a **changing environment**,
the attacker needs much more
skill, effort and resources to hit

Scenario 3

With practice and skill,
can achieve accuracy in a
standard/static environment

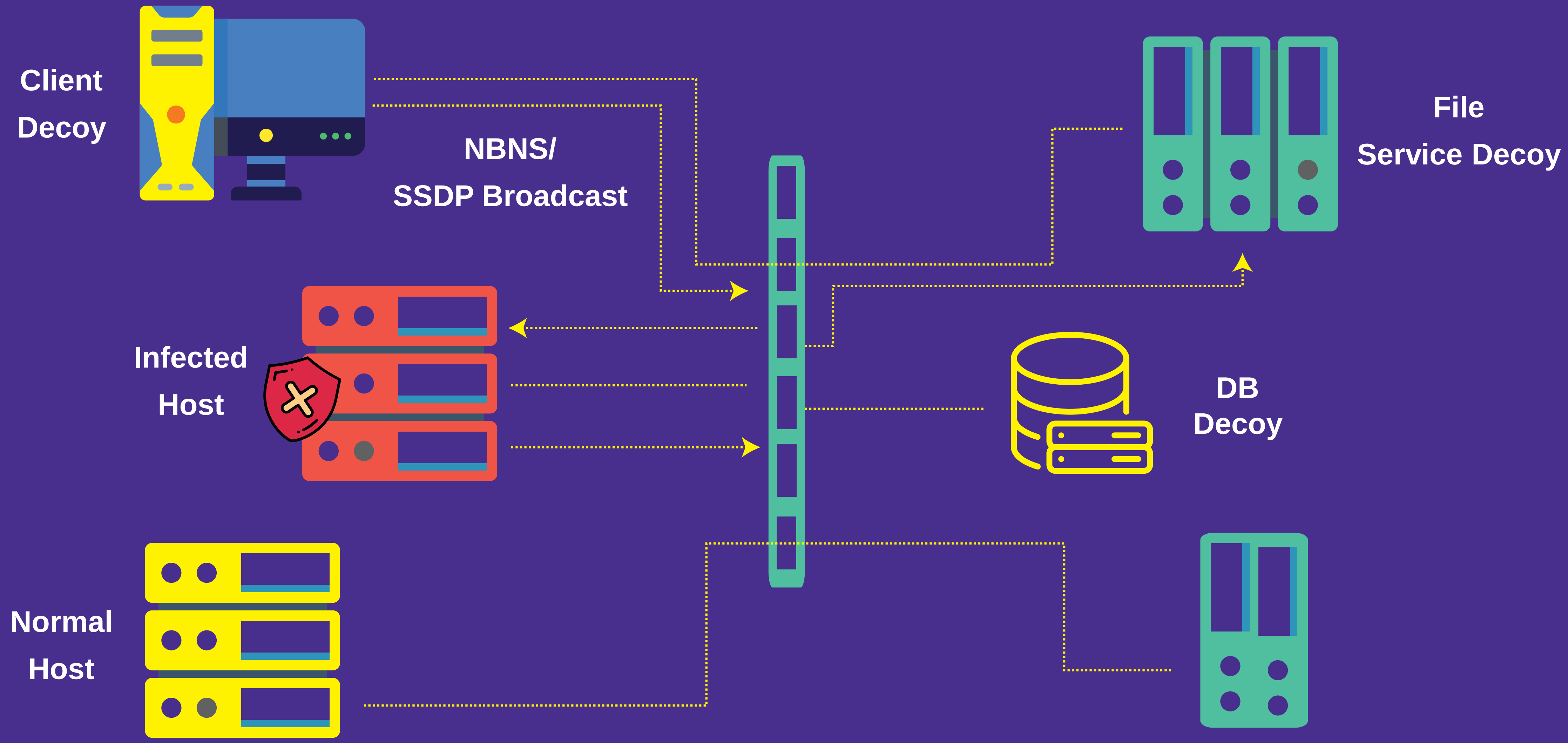


Level 06

Infopercept Proposed Strategy On Network

Infopercept

Secure . Optimize . Strengthen



Level 07

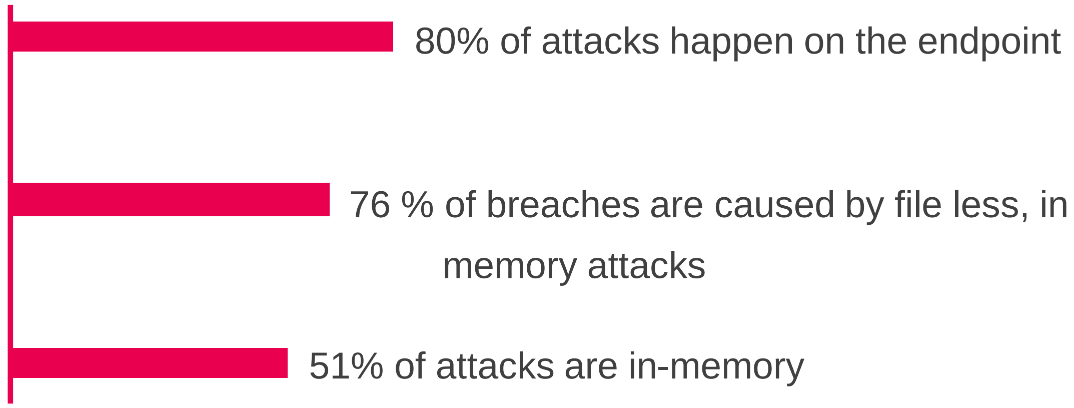
Advanced Threats Exist In-Memory

Infopercept
Secure . Optimize . Strengthen

Recent Example

- LockerGoga ransomware cost Norsk Hydro $45 million so far and gains dropped 82%
- Lake City and Riviera Beach, Florida together paid attackers over $1 million following ransomware attacks
- POS malware stole millions of customer payment details from restaurant chains Buca de Beppo, Planet Hollywood and other Earl Enterprise companies

The 2017 State of Endpoint Security Risk, Ponemon Institute, October 2017



80% of attacks happen on the endpoint

76 % of breaches are caused by file less, in memory attacks

51% of attacks are in-memory

EXISTING SOLUTIONS rely on **PRIOR KNOWLEDGE** and are **DEFENSELESS** against **unknown, evasive threats**.

Level 08

Moving Target Defense Implementation

Prevention

Prevents zero-days, targeted and unknown attacks, with no prior knowledge

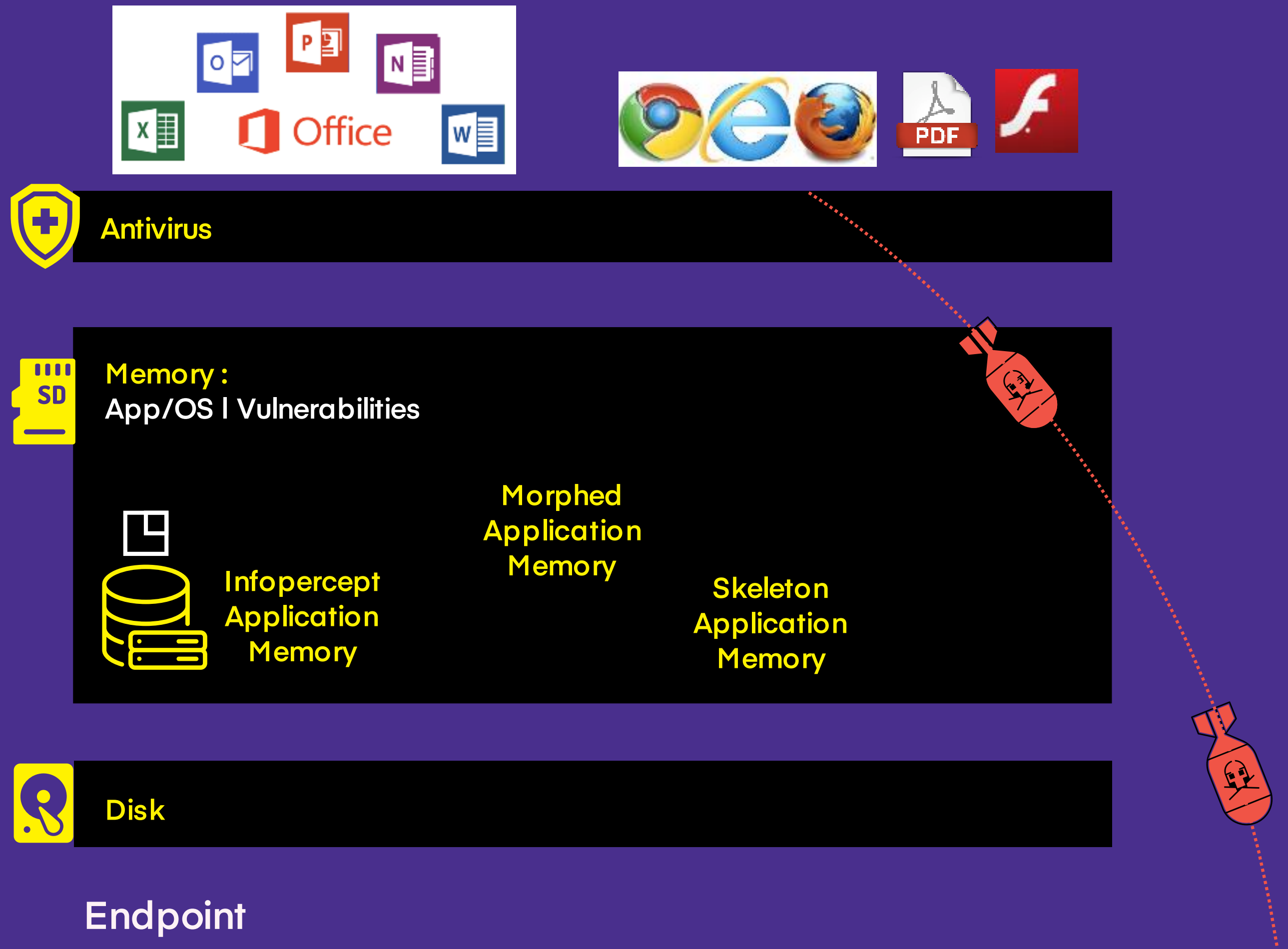
Deterministic

Eliminates false positives

Resilience

Randomization of each process

- Moving Target



Antivirus

Memory :
App/OS I Vulnerabilities

Infopercept Application Memory

Morphed Application Memory

Skeleton Application Memory

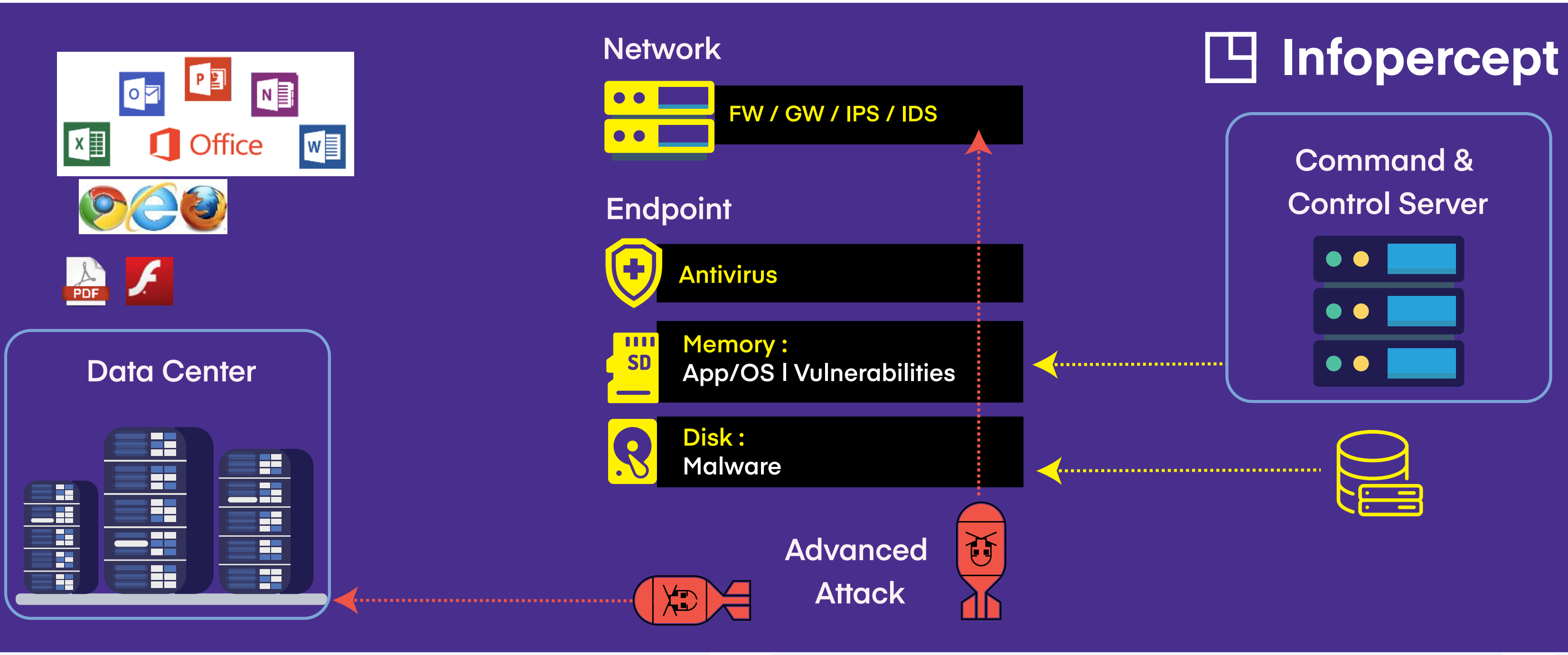
Disk

Endpoint

Level 09

Memory A Mission Critical Battlefield

Infopercept
Secure . Optimize . Strengthen



Denial-of-attack stops attacks at initial penetration stage, before malware downloaded from C2C or if malware already persistent and tries to evade

Most of advanced attacks uses memory resources and vulnerabilities in applications and operating systems

Memory is used at one or multiple stages in the attack kill chain in order to penetrate or evade from traditional Prevention and Detection systems

Traditional security products focus on executables and inefficient memory scanning thus fail to prevent advanced memory based attacks

Level 01

Current Cyber-Defense Landscape

Infopercept
Secure . Optimize . Strengthen

	USE CASE	SHORTCOMINGS
Signature / Whitelist	Implemented at both network and endpoint	Requires constant updates
Sandbox	Devices placed at the perimeter to emulate files in a contained environment and assess risk	Sandbox aware malware can easily evade sandbox detection by delaying mechanism
Artificial Intelligence	Machine Learning/Deep Learning work on principle of training set deployed on the cloud.	IOA needs to be downloaded to the host to prevent if connectivity to cloud is not present. - League of signature based solution plus false positive - also adds burden to users
Behavior Monitoring	Looks for behavior anomalies of processes to make a decision	Based on known behaviors only

Level 02

The Current Anti-APT Technologies

	ADDITIONAL LIMITATIONS
Signature / Whitelist	Only known attacks can be prevented.
Sandbox	**Time:** On average sandboxes require 5 mins to analyze a file and most have a cut-out time of 20 mins, after which file is released termed as benign. This is enough time for a patient zero infection to occur in the environment.
Artificial Intelligence	Works on principle of prior knowledge. The training set needs to be configured by humans to understand the pattern. If the malware strain is not identified by the training set then it is marked as clean, resulting in infection in network. If IOA downloaded locally does not identify the malware, then it needs to be sent to cloud and await results, bringing to prominence Time factor
Behavior Monitoring	Programmed to detect certain anomalies which means it works on principle of prior knowledge. If malware evades the detection mechanism, then it bypasses the solution.

Level 10

Benefits of Infopercept Approach

Endpoints

- Prevention of in-memory zero days or file-less attacks
- Application Virtual Patching against in-memory attacks for commonly used applications
- Protection from Mimikatz Credential Stealing attacks
- Enhanced Lateral movement attack prevention by WMI coverage
- Prevention of Shell Code Injections

Servers

- Enhanced Lateral movement attack prevention by WMI coverage
- Prevention of Shell Code Injections
- Protection from Mimikatz Credential Stealing attacks
- Application Virtual Patching capabilities against in-memory attacks on default applications installed on server’s(ex browsers, adobe etc)

Network

- Identify Compromise System
- Identify Horizontal Movement
- Real-time Threat Intelligence specific to environment
- Less False Positive

Infopercept

THANK YOU

Email
jaydeepr@infopercept.com

phone
+91 9033955155

website
www.infopercept.com