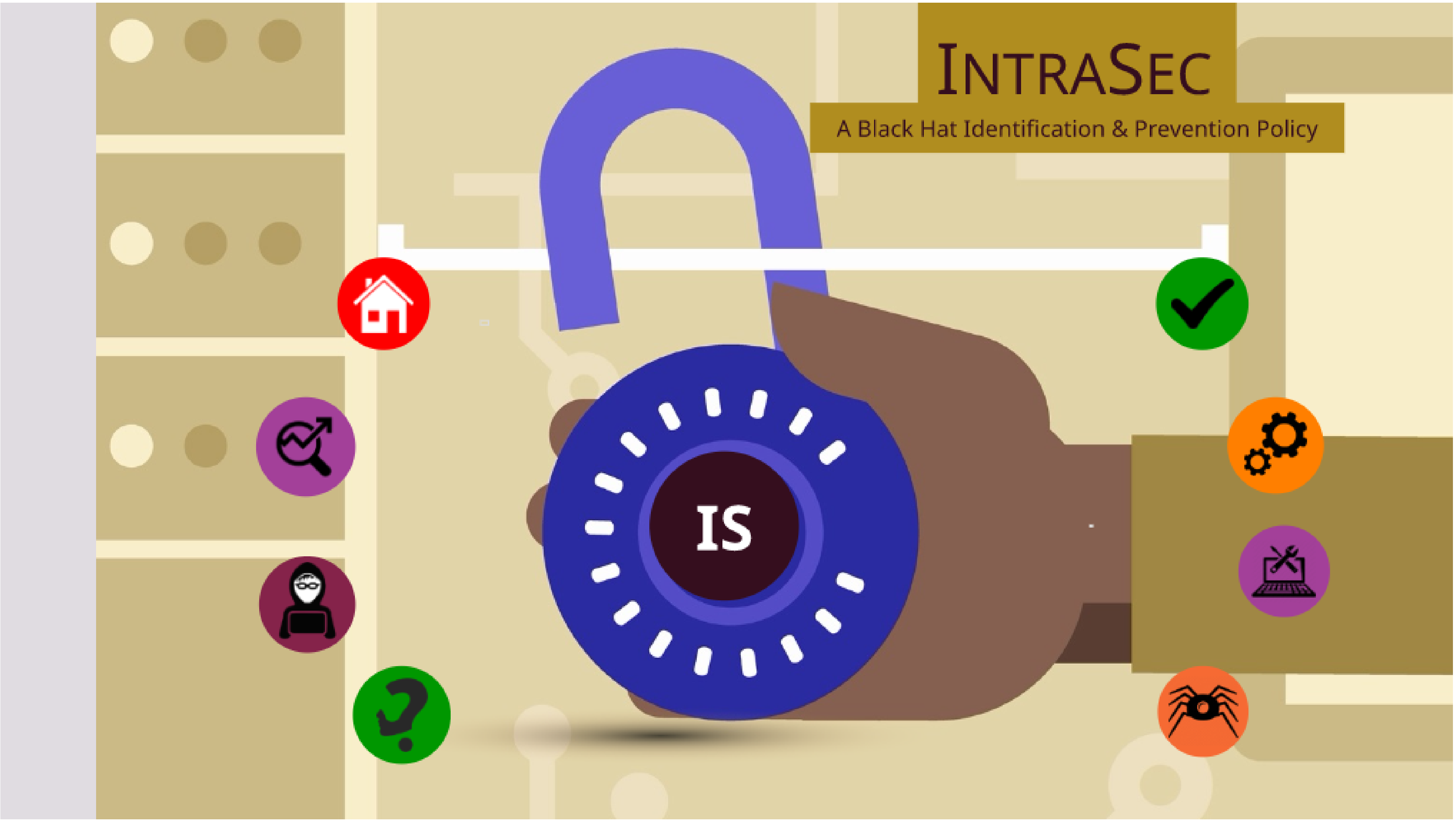
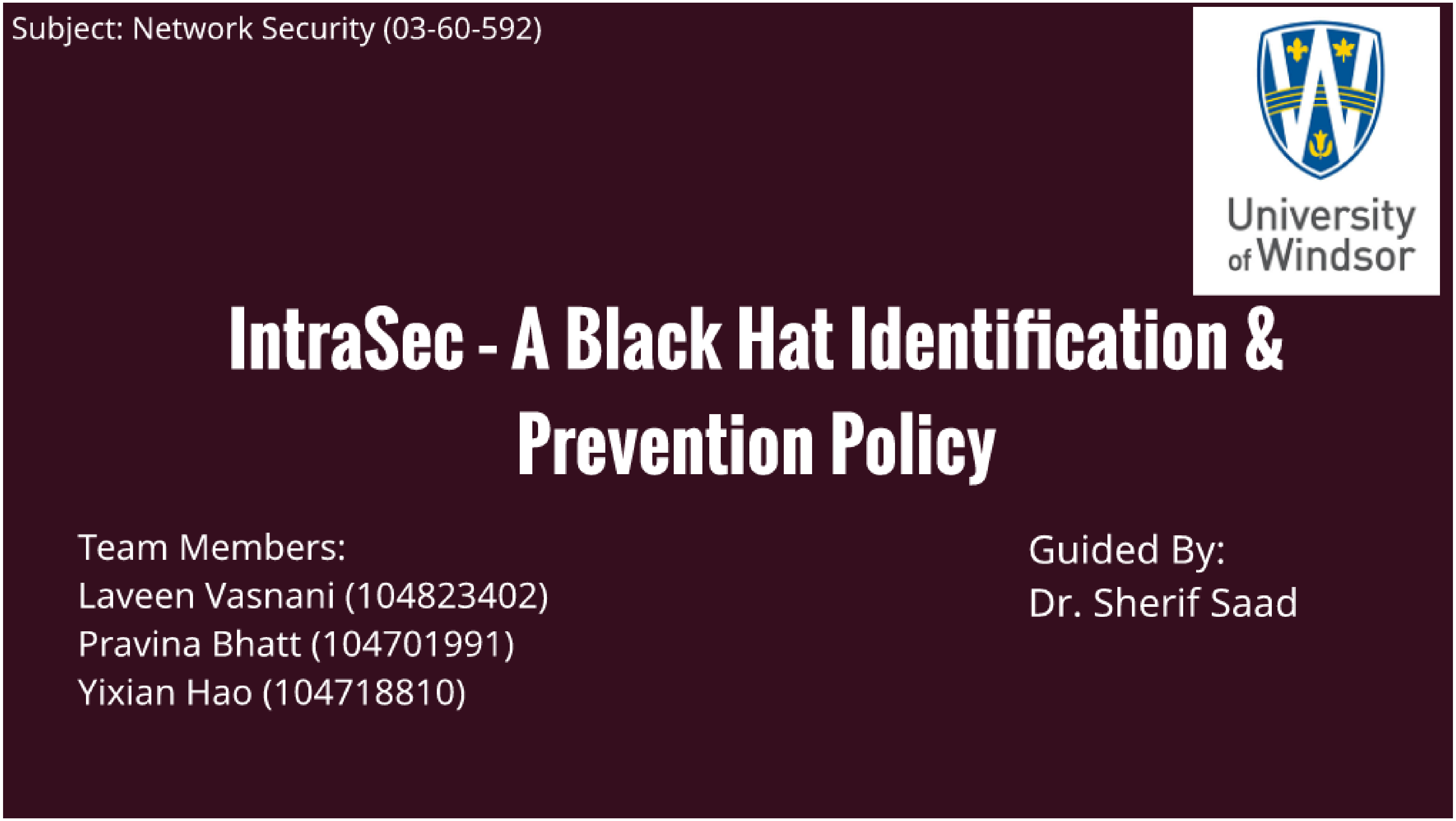


IntraSec

A Black Hat Identification & Prevention Policy



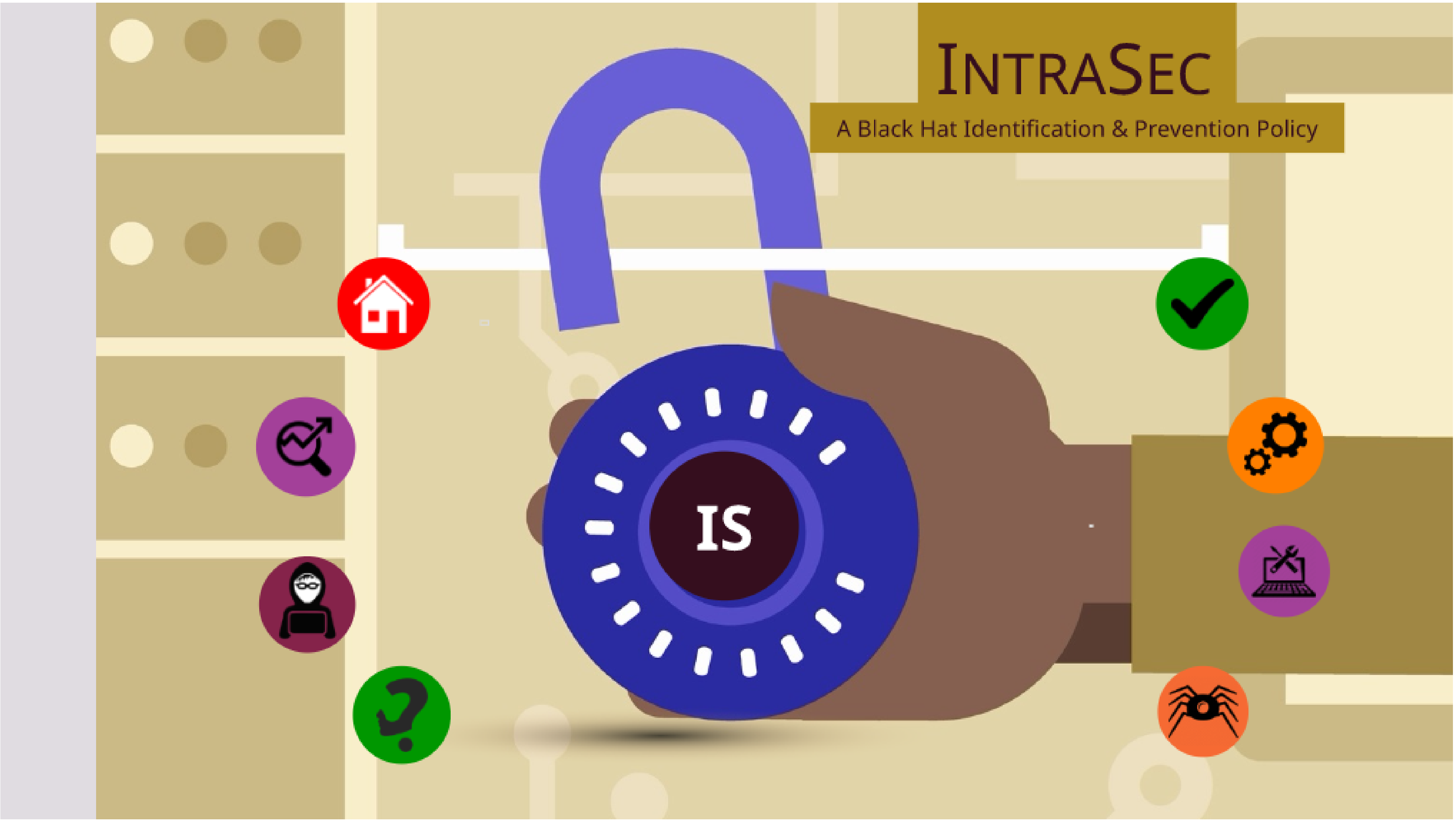
Subject: Network Security (03-60-592)

University of Windsor

IntraSec - A Black Hat Identification & Prevention Policy

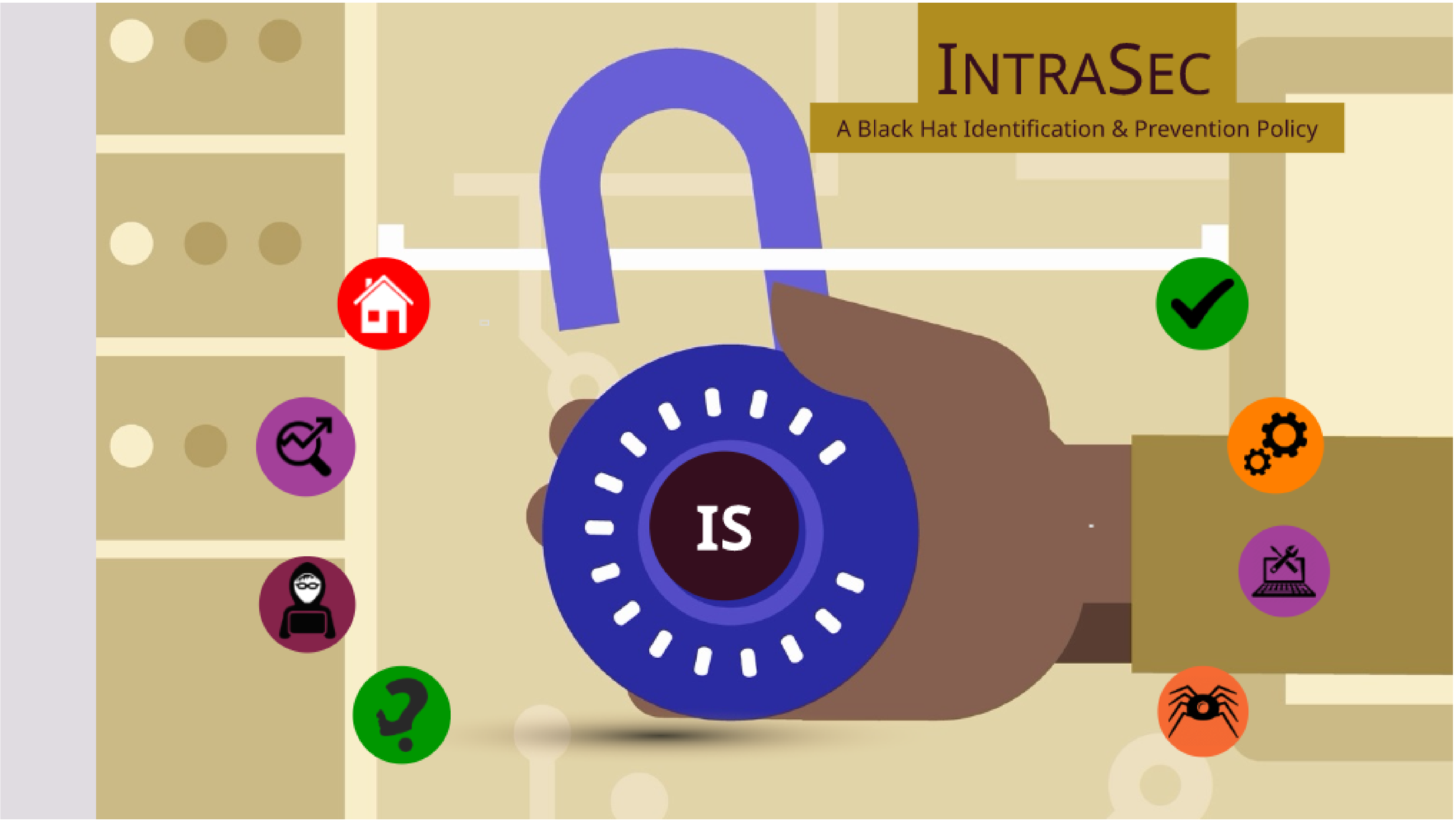
Team Members:
Laveen Vasnani (104823402)
Pravina Bhatt (104701991)
Yixian Hao (104718810)

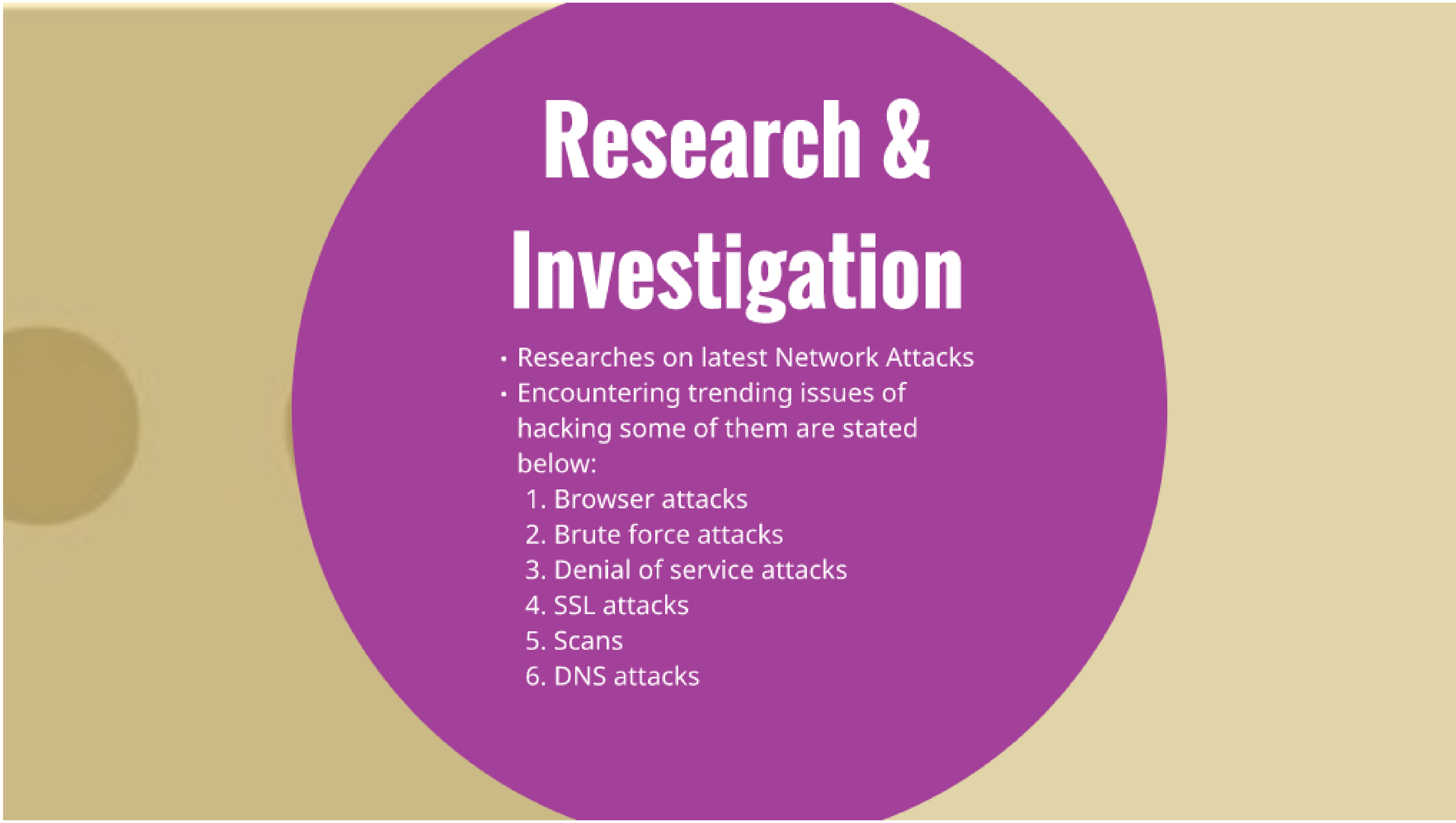
Guided By:
Dr. Sherif Saad


INTRASEC
A Black Hat Identification & Prevention Policy
IS

CONTENT

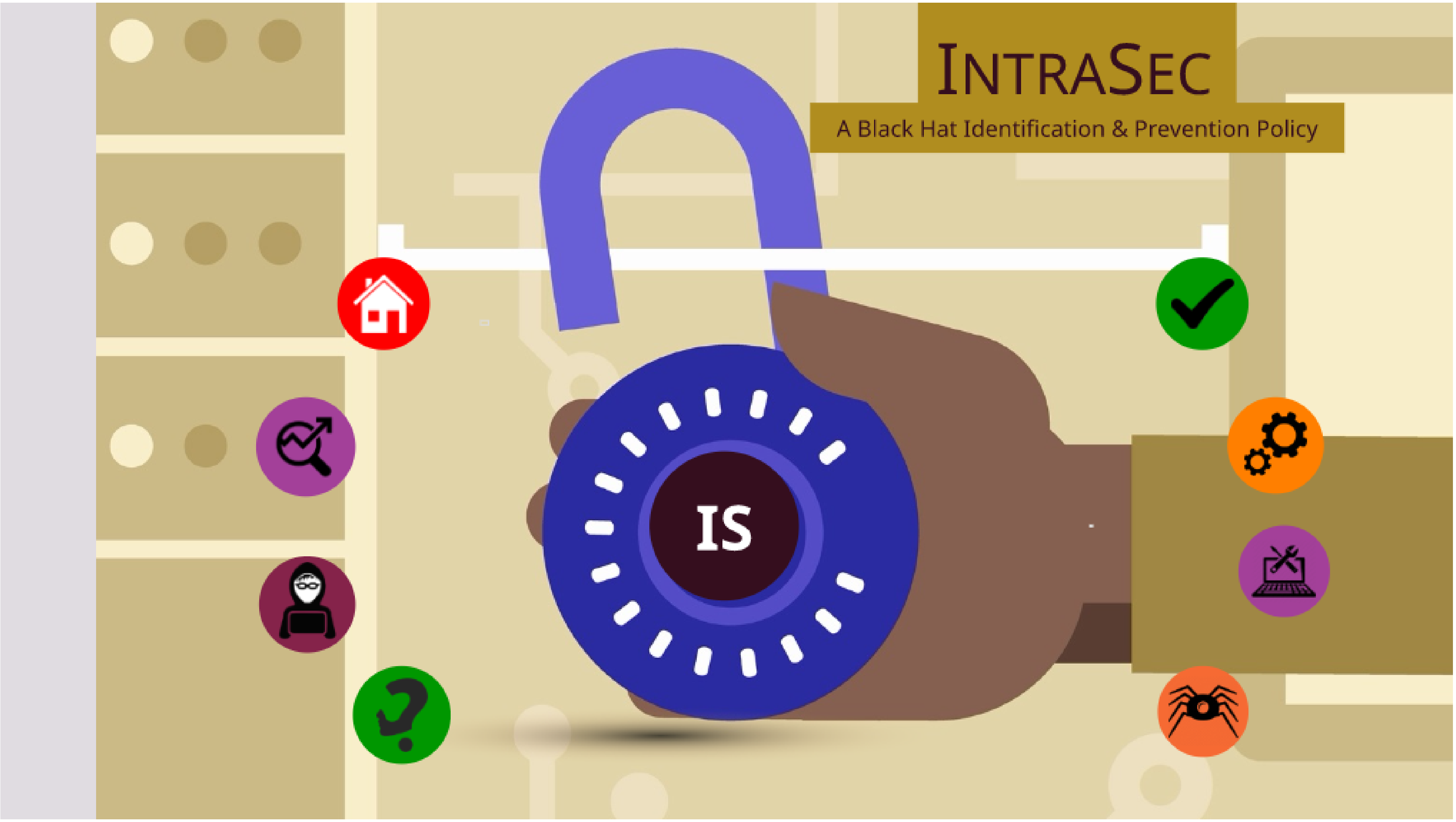
1. Research & Investigation
2. Domain selection
3. Technology mapping
4. Detection & Prevention
5. Network Performance
6. Project Demonstration
7. Questionnaire

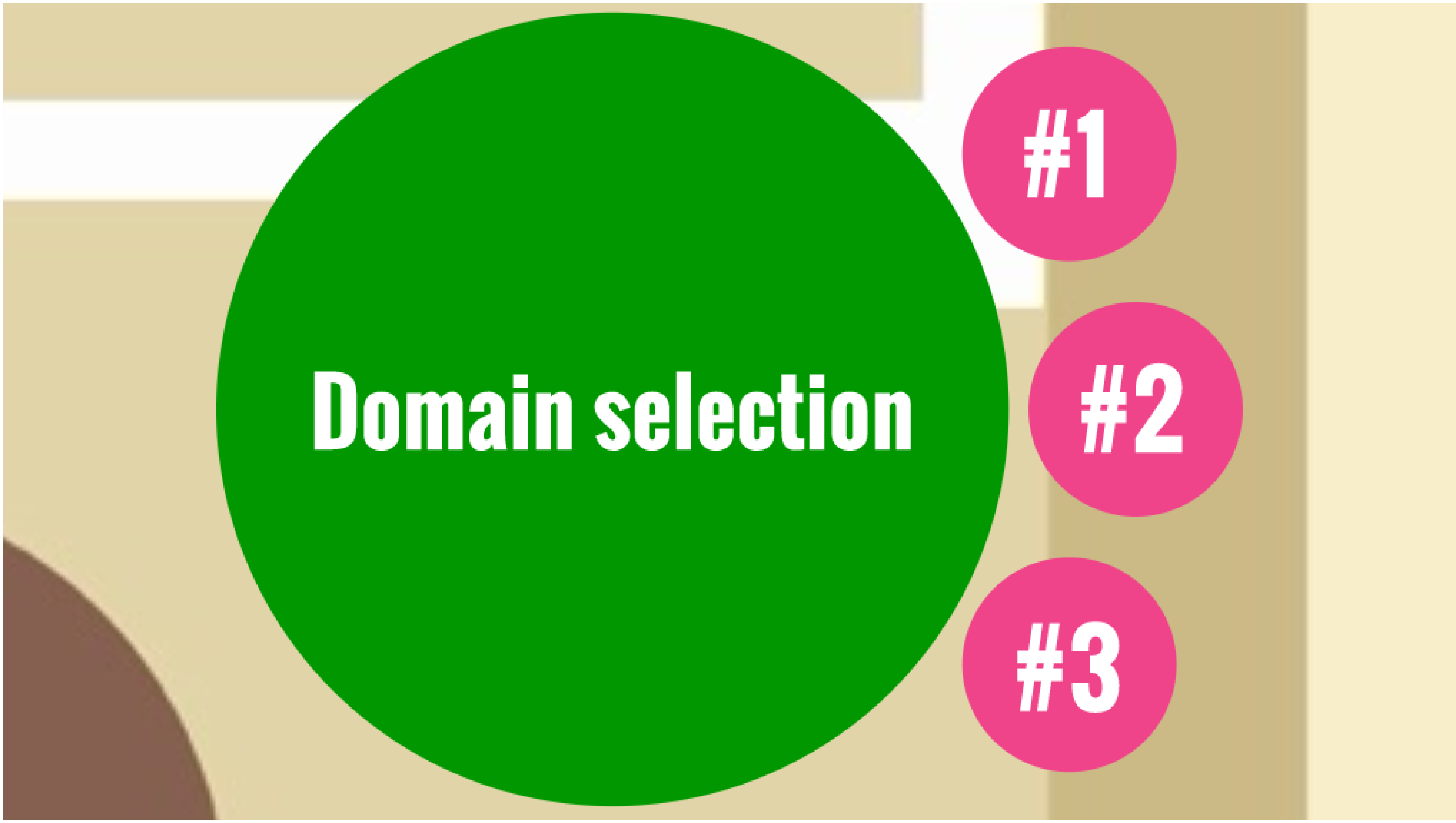

INTRASEC
A Black Hat Identification & Prevention Policy
IS



Research & Investigation

- Researches on latest Network Attacks
- Encountering trending issues of hacking some of them are stated below:
  1. Browser attacks
  2. Brute force attacks
  3. Denial of service attacks
  4. SSL attacks
  5. Scans
  6. DNS attacks


INTRASEC
A Black Hat Identification & Prevention Policy
IS

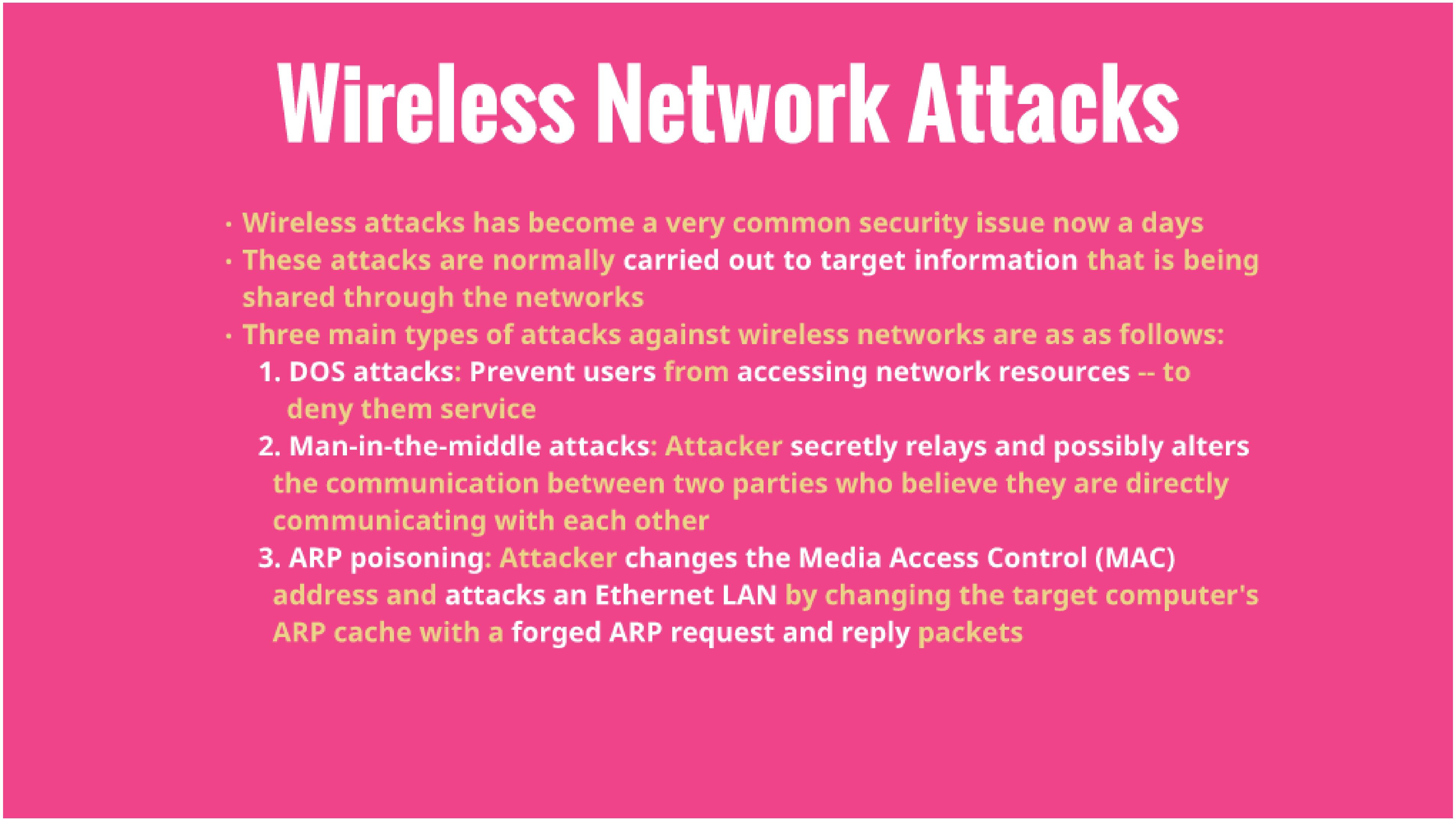


Domain selection

#1

#2

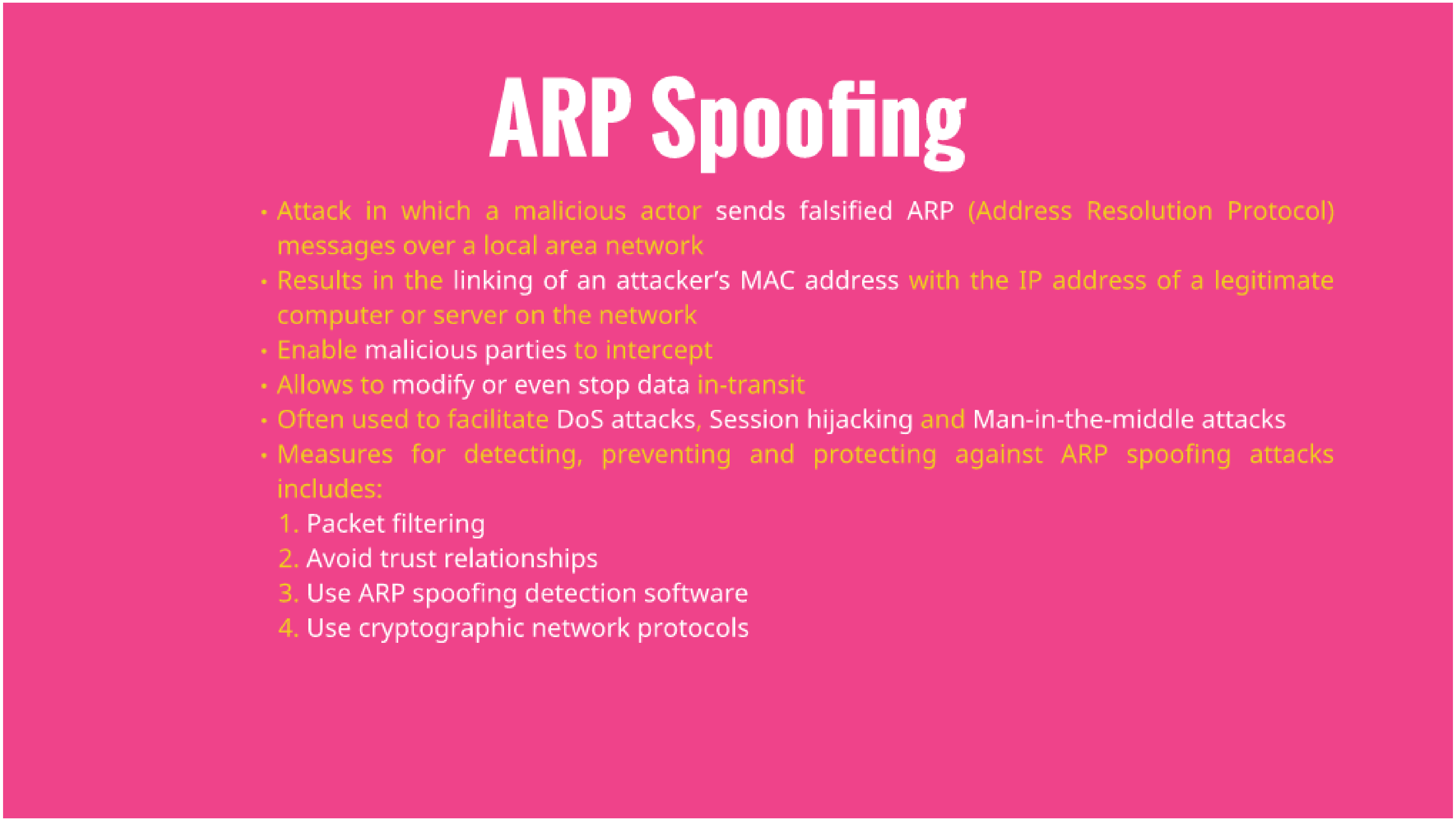
#3



Wireless Network Attacks

- Wireless attacks has become a very common security issue now a days
- These attacks are normally carried out to target information that is being shared through the networks
- Three main types of attacks against wireless networks are as as follows:

  1. DOS attacks: Prevent users from accessing network resources -- to deny them service
  2. Man-in-the-middle attacks: Attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other
  3. ARP poisoning: Attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets

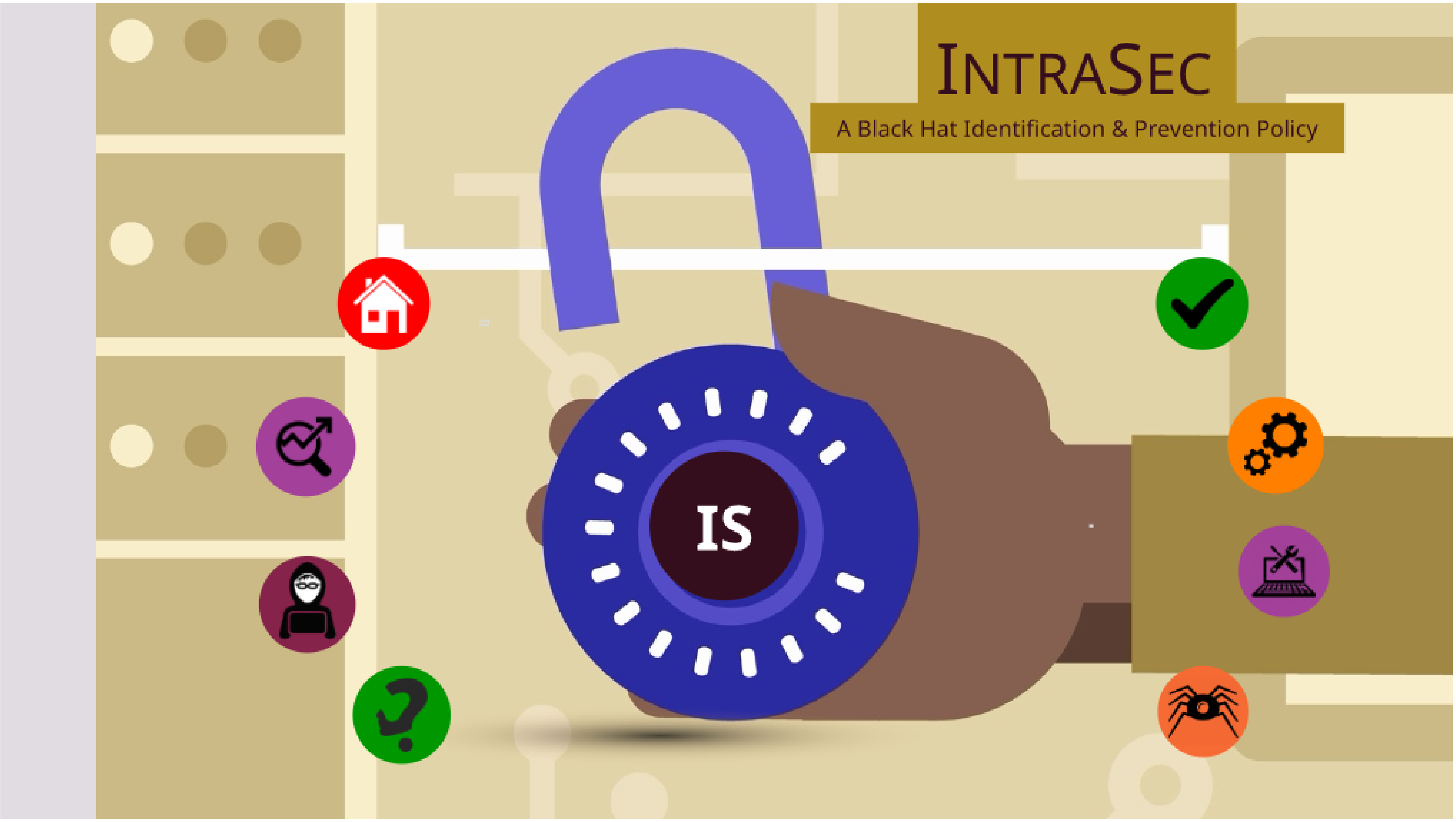


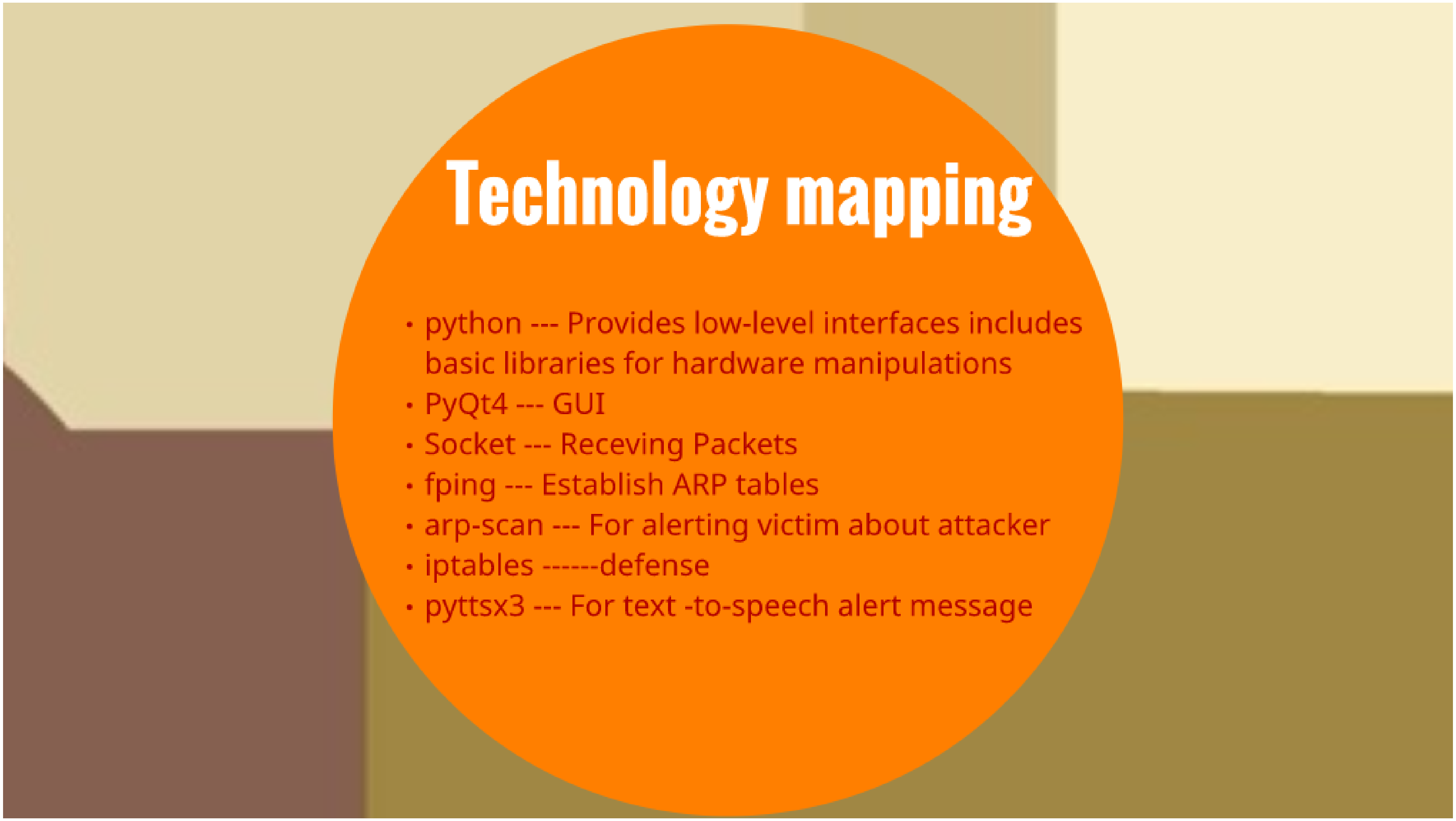
ARP Spoofing

- Attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network
- Results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network
- Enable malicious parties to intercept
- Allows to modify or even stop data in-transit
- Often used to facilitate DoS attacks, Session hijacking and Man-in-the-middle attacks
- Measures for detecting, preventing and protecting against ARP spoofing attacks includes:
  1. Packet filtering
  2. Avoid trust relationships
  3. Use ARP spoofing detection software
  4. Use cryptographic network protocols

Internet Security

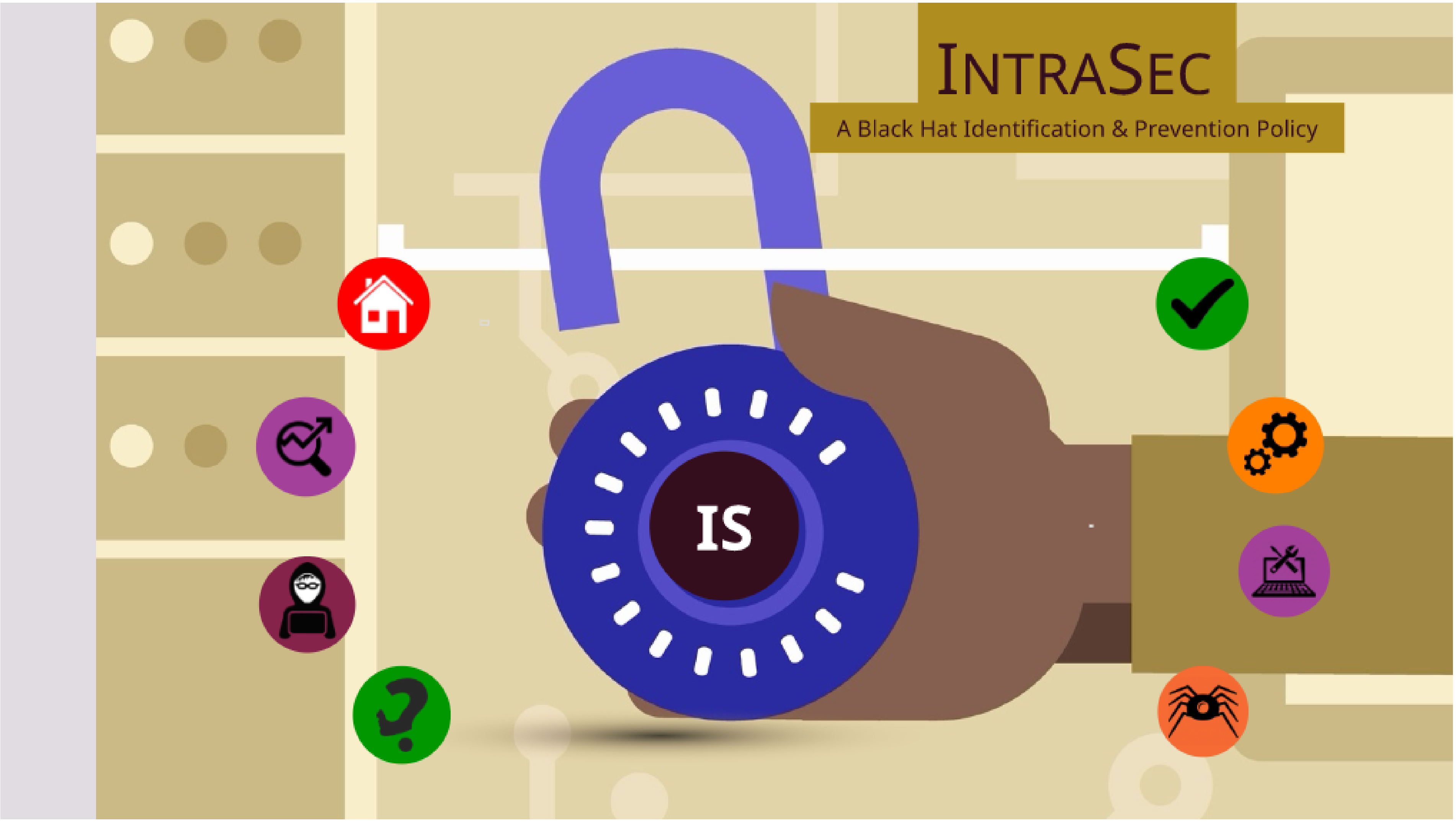
- Objective is to establish rules and measures to use against attacks over the Internet
- Encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol
- Relies on specific resources and standards for protecting data
- Includes various kinds of encryption such as Pretty Good Privacy (PGP)
- Other aspects of a secure Web setup includes firewalls, which block unwanted traffic
- Anti-malware, anti-spyware and anti-virus programs can also help to provide security over internet

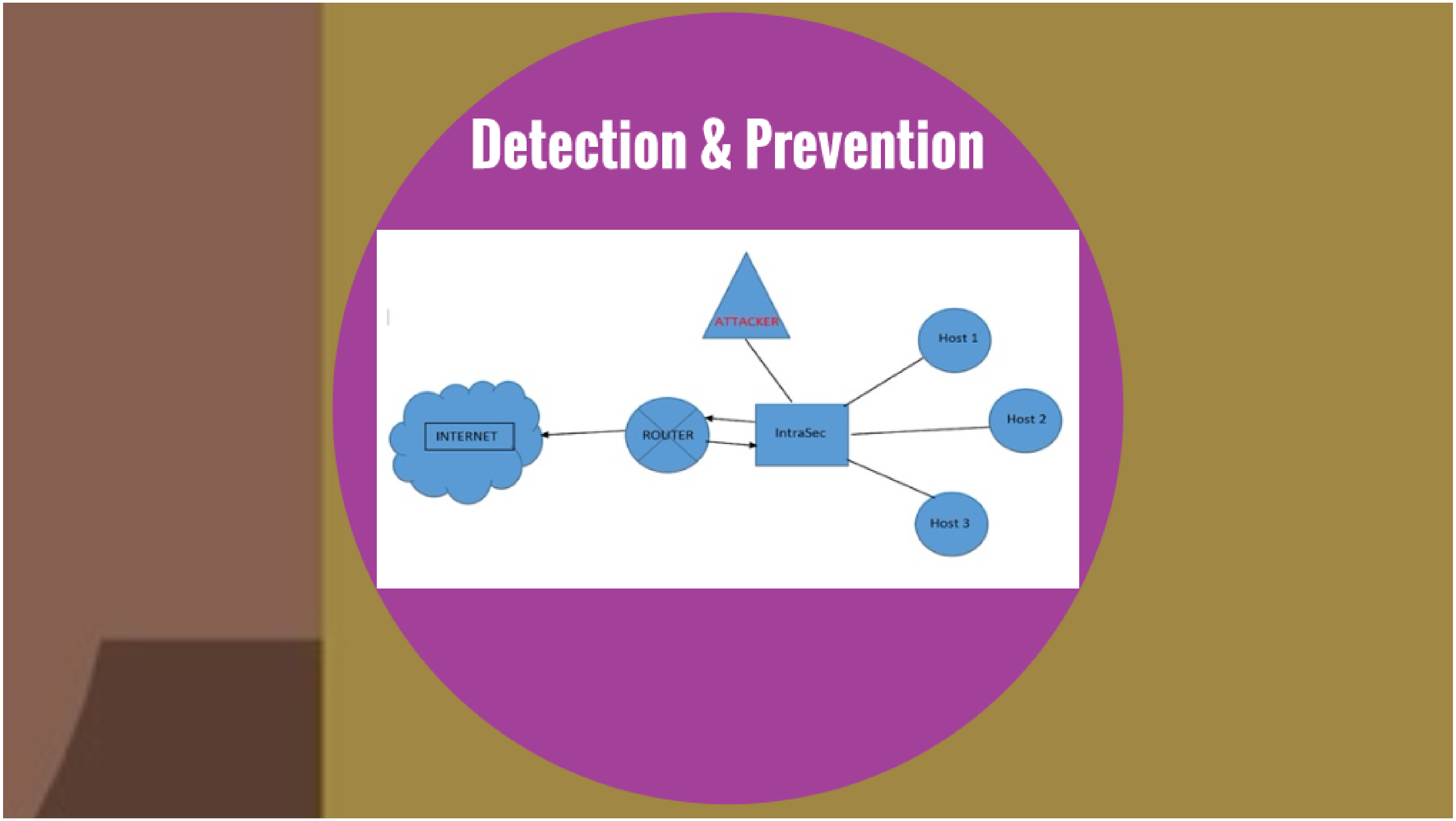

INTRASEC
A Black Hat Identification & Prevention Policy
IS



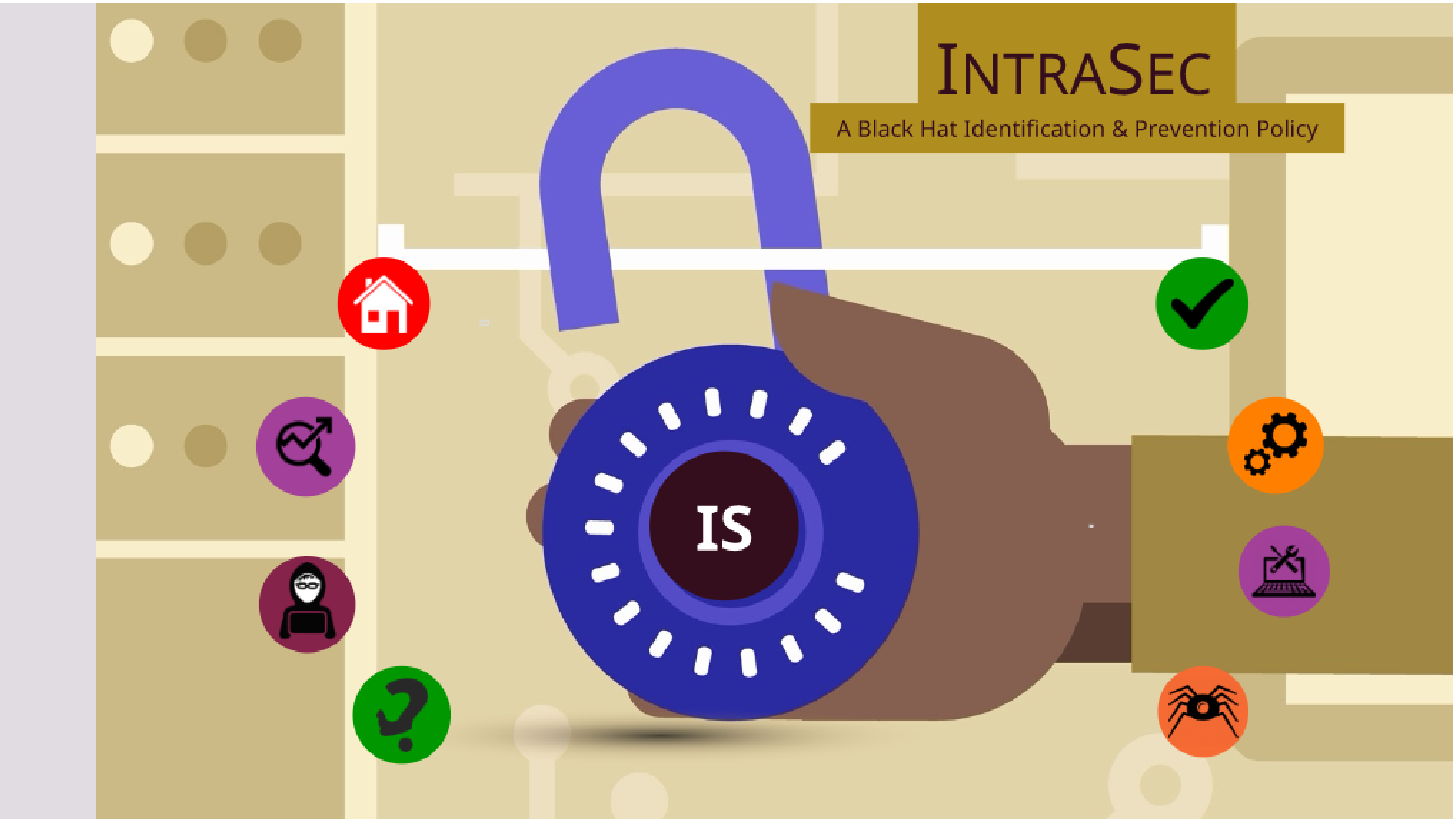
Technology mapping

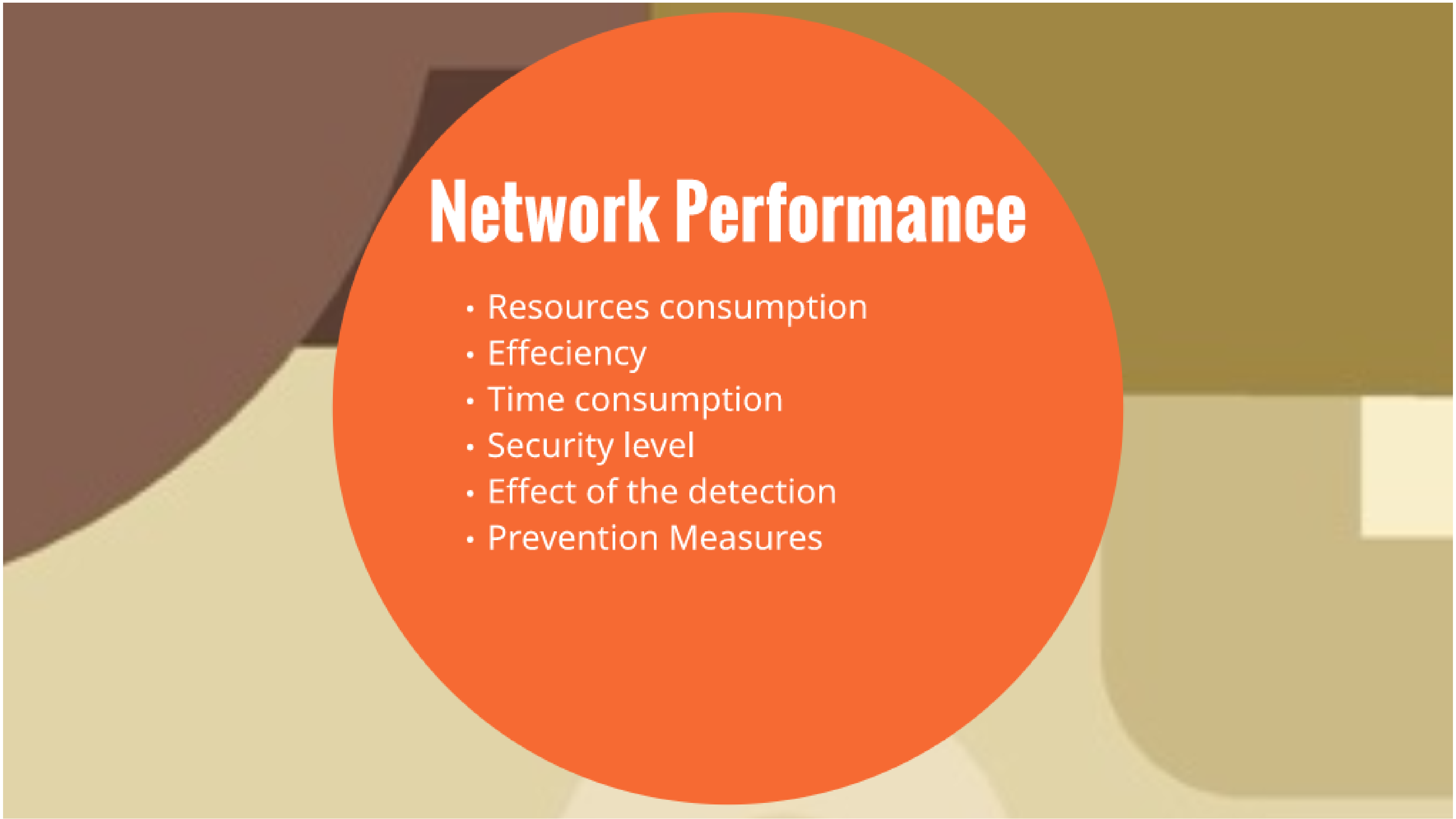
- python --- Provides low-level interfaces includes basic libraries for hardware manipulations
- PyQt4 --- GUI
- Socket --- Receving Packets
- fping --- Establish ARP tables
- arp-scan --- For alerting victim about attacker
- iptables ------defense
- pyttsx3 --- For text -to-speech alert message


INTRASEC
A Black Hat Identification & Prevention Policy
IS



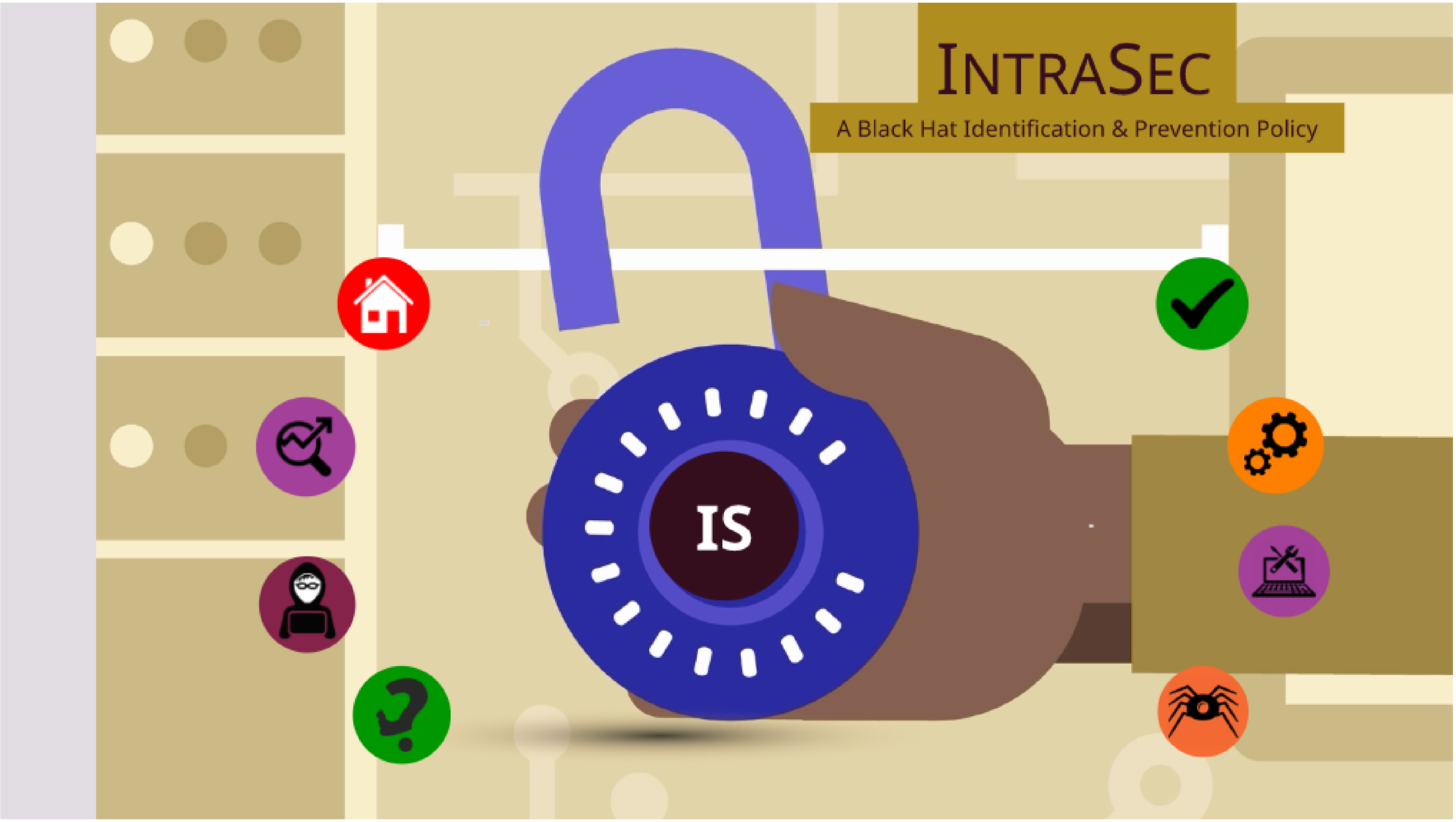
Detection & Prevention


INTRASEC
A Black Hat Identification & Prevention Policy
IS

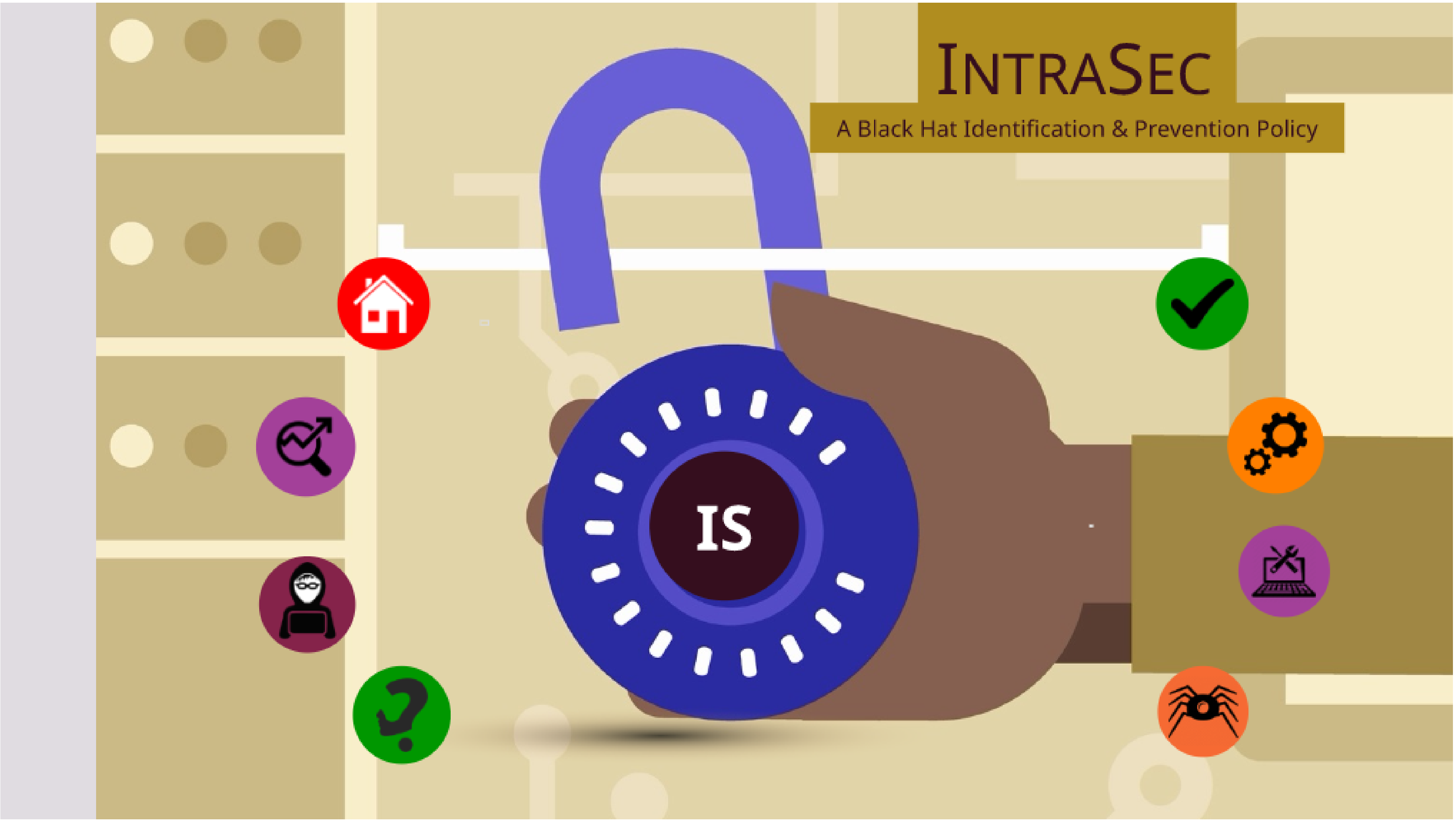


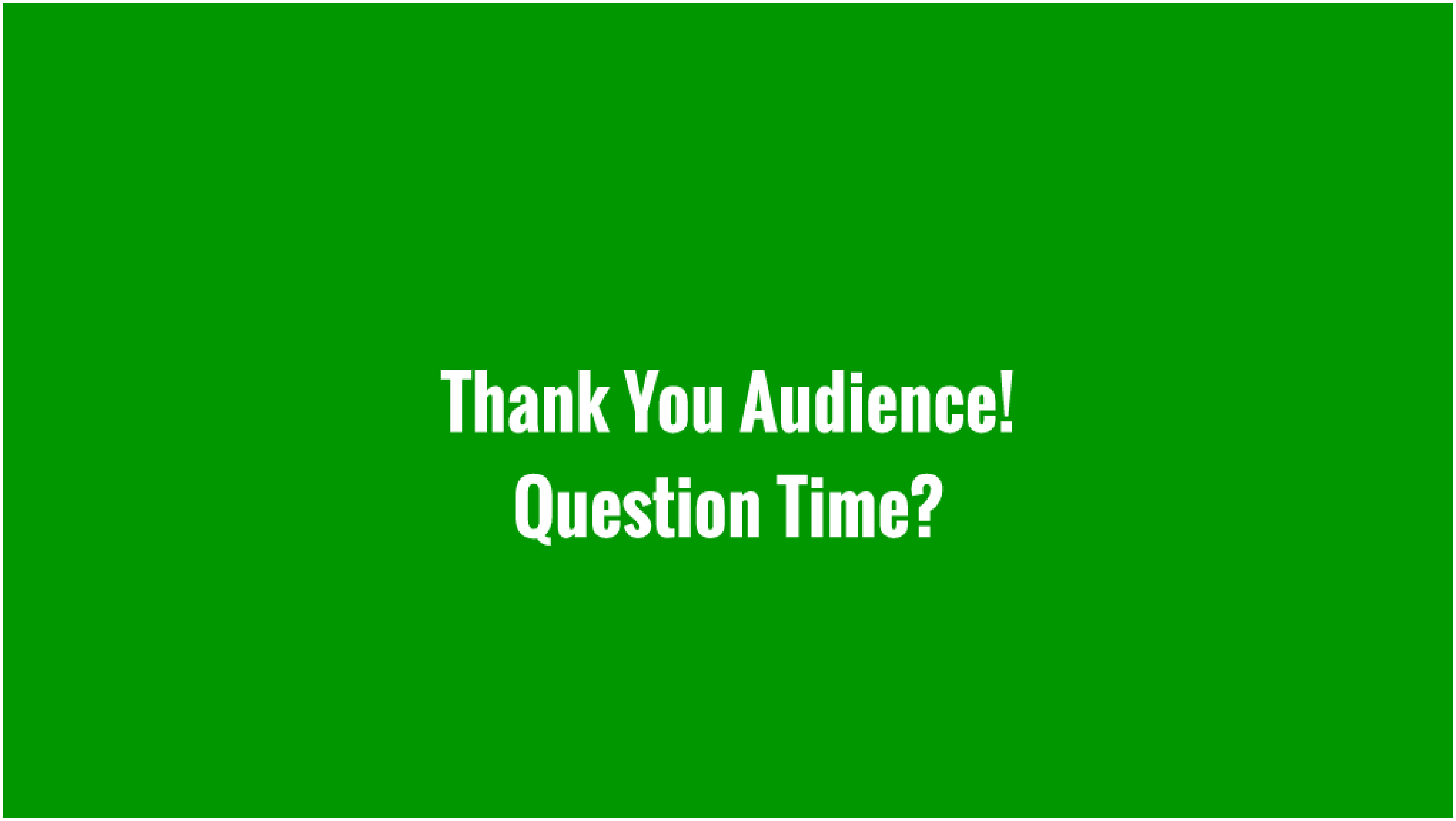
Network Performance

- Resources consumption
- Effeciency
- Time consumption
- Security level
- Effect of the detection
- Prevention Measures


INTRASEC
A Black Hat Identification & Prevention Policy
IS

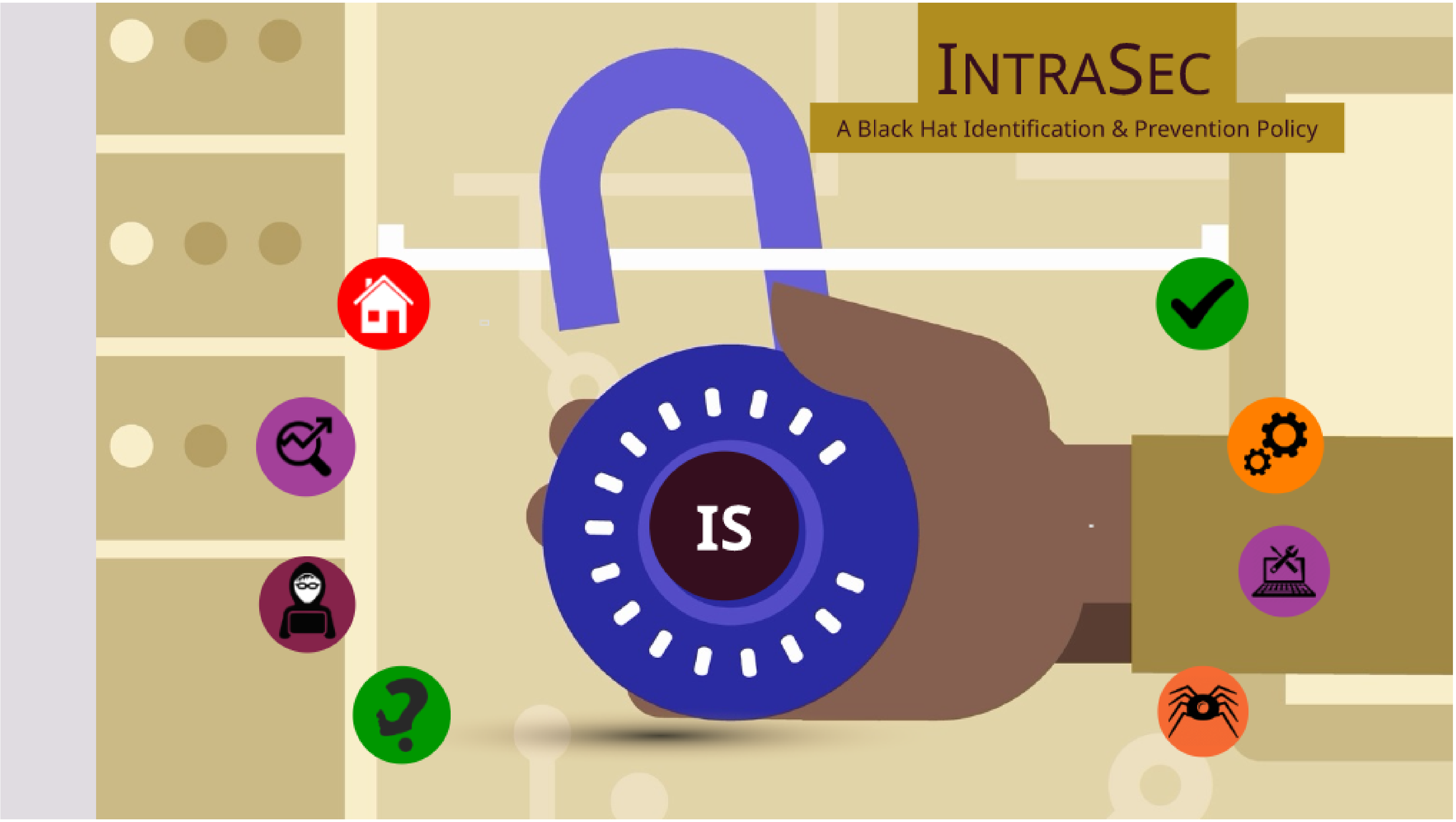
Project Demonstration


INTRASEC
A Black Hat Identification & Prevention Policy
IS



Thank You Audience!

Question Time?


INTRASEC
A Black Hat Identification & Prevention Policy
IS