
SDC
SECURITY | DISTRIBUTION | CENTER

NEUROsoft

REDYOPS

Powered by Neurosoft S.A.

Red Team Operations

https://www.redyops.com

Red Teaming – "Off the Net"

Infocom Cyprus Conference 2019

The Team

- Members are qualified professionals
- Certified with high profile certifications
- Experienced in the field
- Methodological Processes
- Attacking skills on different areas
- Determined to succeed
- Determined to not been caught

The Target

Where…

- is a “feel” of Security
- true risk must be calculated
- business depends on security (sensitive data)
- penetration tests are not enough
- asymmetric attacks need to be tested
- prevention, detection & response should be assessed

The Goal of the Team

- Specific targets/goals/achievements
- Get in and access sensitive information in any way possible
- Red vs Blue
- Test the organization's detection and response capabilities
- Identify software, physical, hardware and human vulnerabilities
- Realistic attack simulation | | Virtual Exercises
- Evaluate procedures
- Get Proactive Solutions

Approach

Technology

- ✓ Networks, systems, applications
- ✓ Find and exploit vulnerabilities
- ✓ Vulnerability research and 0-day exploits
- ✓ Assess technological security controls

People

- ✓ Staff, departments
- ✓ Advanced Social Engineering attacks
- ✓ Spear Phishing attacks with custom made APT
- ✓ Evaluate readiness and response

Physical

- ✓ Offices, warehouses, buildings
- ✓ Bypass physical security controls
- ✓ Implant physical evidence
- ✓ Find weak entry points to infiltrate a secure building/location
- ✓ Assess physical security procedures

Methodology

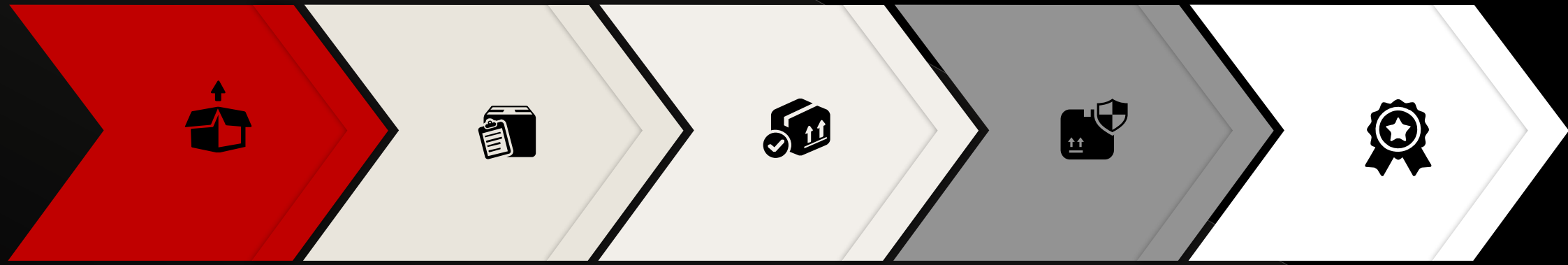
- ✓ Target
- ✓ Scope
- ✓ Duration
- ✓ End Goals
- ✓ Preparation
- ✓ Limitations (RoE)

- ✓ OSINT
- ✓ HUMINT
- ✓ IMINT
- ✓ Dark Web
- ✓ On-Site
- ✓ Results

- ✓ Develop Scenarios
- ✓ Determine Risk
- ✓ Assign Roles
- ✓ Create Test Cases
- ✓ Requirements
- ✓ "Out of Jail"

- ✓ Execute Plan
- ✓ Re-design
- ✓ Daily Report
- ✓ Next Plan

- ✓ Final Report
- ✓ Videos, Photos, Screenshots
- ✓ Recommendations
- ✓ Attack Detection Rules
- ✓ Presentation



Initial Planning

Information Gathering

Final Planning

Attack Execution

Reporting

Real Red Team Case

"The story you are about to hear is true. The names have been removed to protect the innocent"

Initial Planning

- Target
  - Major Bank in Middle East
- Scope
  - Technology (Phishing/Spear)
  - People (Interactive SE & Vishing)
  - Physical (6 Locations)
    - Headquarters
    - IT Department
    - *Branches x 4*
- Duration
  - One month

Initial Planning

External Threat Actor (Team of 5)

- Flag 1 (CTR): Bypass Physical Access Controls
- Flag 2 (ACC): Access Sensitive Data & Internal Assets
- Flag 3 (USB): Drop USB (Desks, Meeting Rooms, etc)
- Flag 4 (ATO): Account Take Over
- Flag 5 (LAP): Access Internal Network - plug laptop.
- Flag 6 (REC): Deploy an audio recording device

Challenges/Limitations

Ramadan

Weather Conditions

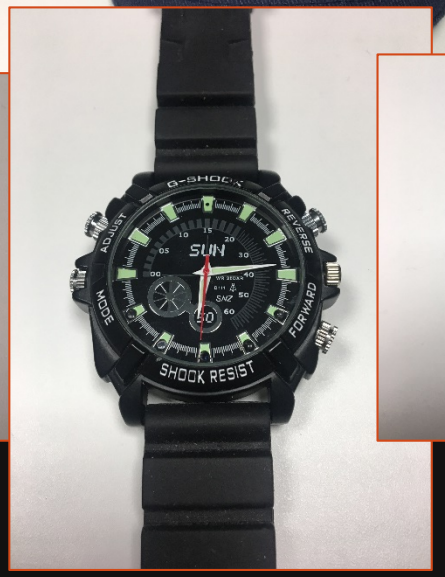
Language , Culture and Localization

Secure Environment, High Risk, Different Policies

Many Flags – Extensive Checks

Preparation

Preparation



Information Gathering

Technical (Passive)

- Google Dorking/Earth/Images
- LinkedIn, Facebook, Twitter, etc.
- Harvester, Maltego, Recon-ng

Non Technical (On-site)

- Long range
- Short range
- Dumpster Diving

Information Gathering

Results

Branches

- High street premises, No Guards
- CCTV and Internal Guards
- Access Control (Major Branch Only)

IT Department

- Patrolling Guards
- Internal Guards and CCTV
- Access Control (Staff ID Card)

Headquarters

- Patrolling Guards
- Internal Guards and CCTV
- Reception (3) and Waiting Area

Final Planning

Location	Target
Branch 1	Easy
Branch 2	Easy
Branch 3	Easy
Major Branch	Normal
IT Building	Hard
Headquarters	Challenging

Final Planning

Develop Scenarios

1. Vishing is the preferred method of account take over (phishing results)
2. Branch Offices seem vulnerable to ad-hoc visitor attacks
3. IT Department will require aggressive techniques or Interactive SE
4. Headquarters will require a “valid” appointment

Final Planning

Location	Scenarios
Branch 1	Bank Opening Account
Branch 2	Bank Opening Account
Branch 3	Bank Opening Account
Major Branch	Bank Opening Account Employee Meeting
IT Building	Security Audit Employee Meeting
Headquarters	Mess Up meeting

Attack Execution

Security Incident Test Case (Vishing)

- Attacker calls Brand Manager
- The caller claims to be from the Security Department of Bank
- Informs the Branch manager for compromised Credentials
- The caller advices the Branch manager to change his password

Attack Execution

Boom!

8 accounts take overs

- Senior Vice-President
- Assistant Vice President
- Branch Managers (x6)

Final Planning

Major Branch Test Case

- Teams member Bill and Julia act as potential customers.
- Ad-hoc opportunities (mainly piggybacking, open doors)
- Laptop, USB and Audio device prepared
- Other team members on hold (phone, messenger)

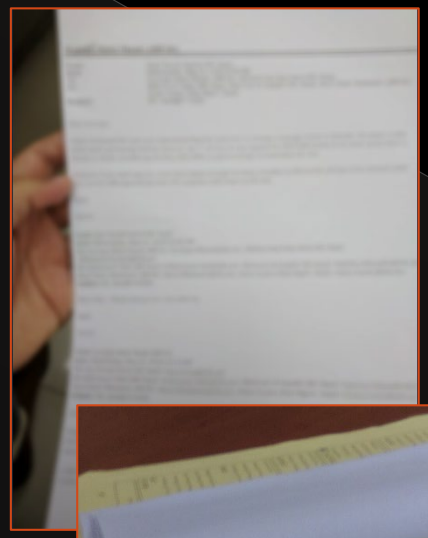
Attack Execution

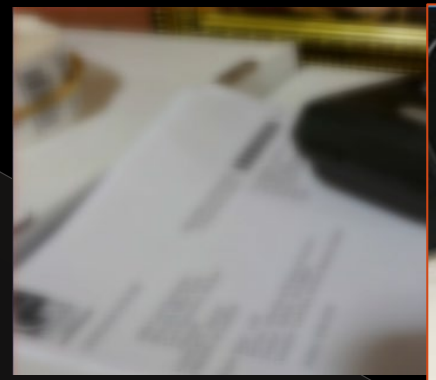
Major Branch Execution

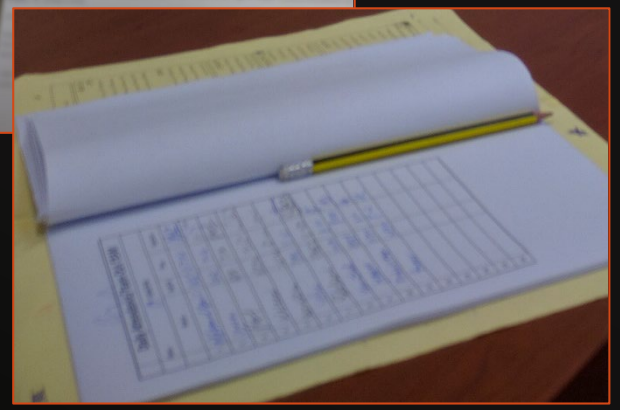
- Bill and Julia are walking around and asking questions
- Bill is being asked by Guards and Police!
- 2 Hours and no success
- An opportunity (3rd party company, A4 papers)
- Bill and Julia performed piggybacking (CTR)
  - actually got inside together with the Company
- While in:
  - accessed unattended assets (ACC), accessed internal documents (ACC)

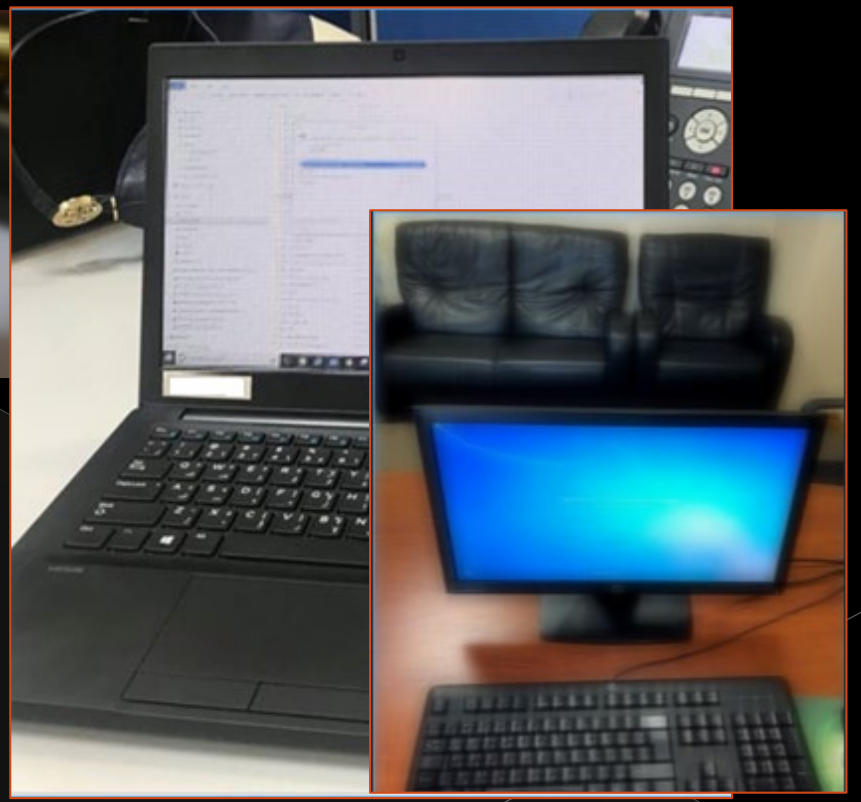
Attack Execution

Boom!









Final Planning

IT Department Test Case

- Team member “Bill” poses as an “External Security Auditor”.
- Related Documentation is prepared (Audit Procedure, Fake authorization, etc.)
- Team member “Alex” to enter the Rest Room as ad-hoc visitor
  - Also monitors the process of “External Security Auditor”
- Other team members on hold (phone, messenger)

Attack Execution

IT Department Scenario Execution (1)

- Bill along with Alex and other employees head to the elevator.
- Alex is already “talking” on the phone.
- Bill is heading straight up for a piggybacking.
- Guard stops Bill.
- Bill is explaining the guard about the security audit.
- Guard asks for a verification.
- Bill gives the “fake” authorization email.
- Guard asks Bill to escort him to the Security Officer (Surprise!)
- Things are getting complicated but team stayed calm!

Attack Execution

IT Department Scenario Execution (2)

- Guard and Bill is heading to the Security Officer
- Alex (who is still talking)

  Noticed that Guard left the remote door keys unattended!

  Calls immediately Jim.
- Jim managed to come on time!

  Alex opens the door for Jim **(CTR)**

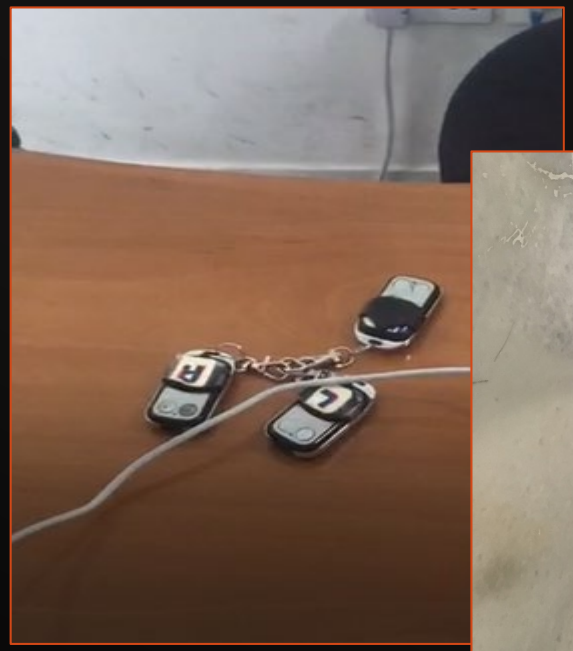
  Jim now is an insider.
- While in:

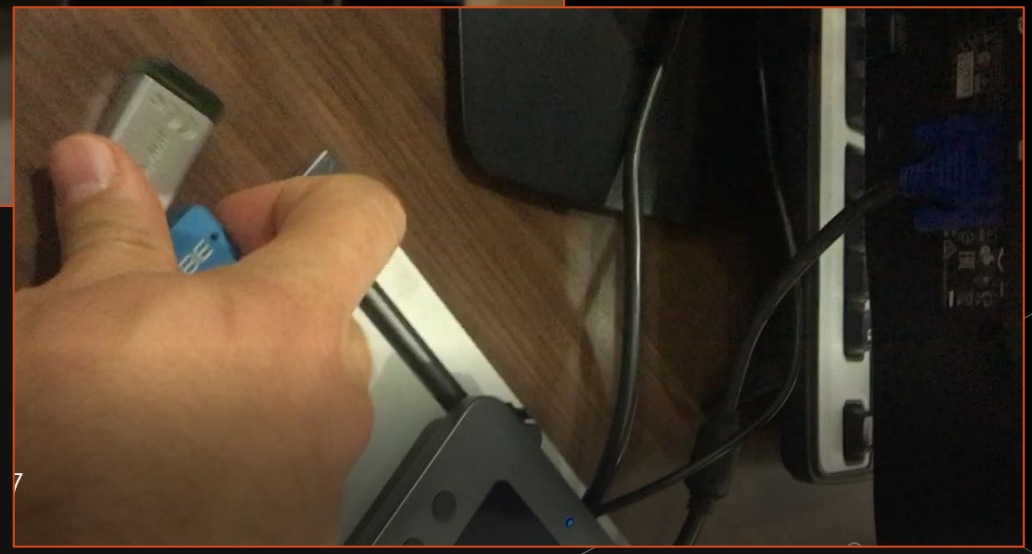
  Dropped USB on offices (Meeting Room unfortunately was occupied!) **(USB)**

  REMOTE ACCESS WAS ACHIEVED!

Attack Execution

Boom!





Final Planning

Headquarters Test Case

Team member “Jim” is calling reception to inform about the mess-up.

Team member “Alex” is coming as a business man.

Informs about the meeting and asks to wait until Manager arrives.

Attack Execution

Headquarters Execution (1)

- Alex is arriving at reception and informs about the appointment
- Reception is willing to call Branch Manager
- Alex has already the contact in his mobile (already called him)
- Reception calls back
- Jim confirms the appointment
- Reception is offering the waiting area (**insist for a meeting room**)

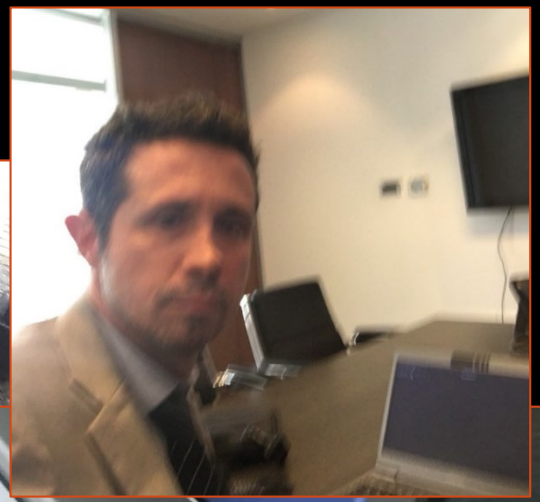
Attack Execution

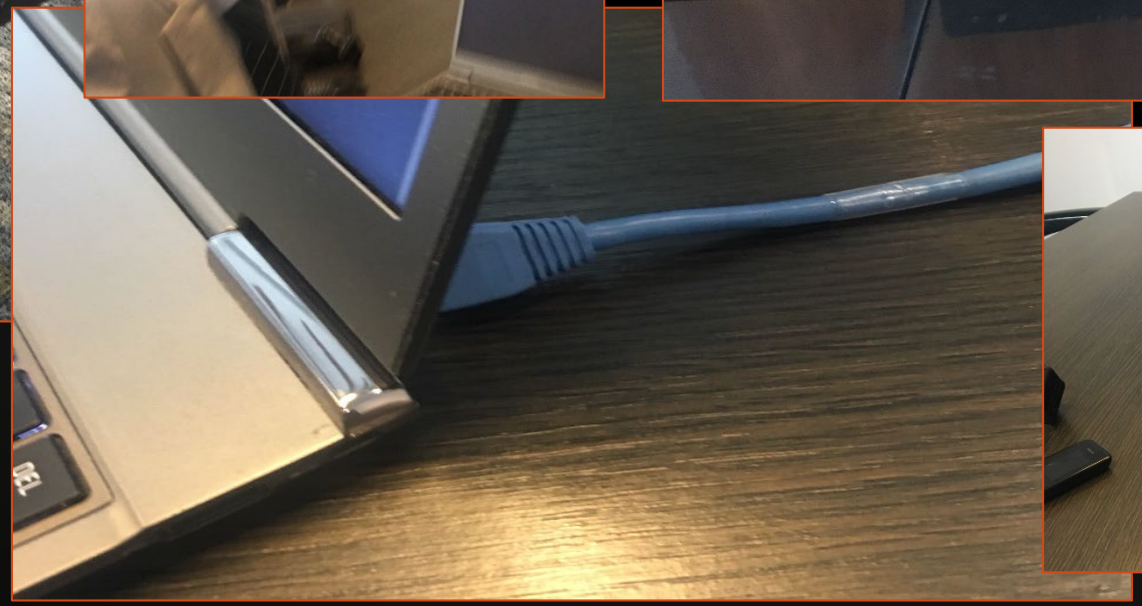
Headquarters Execution (2)

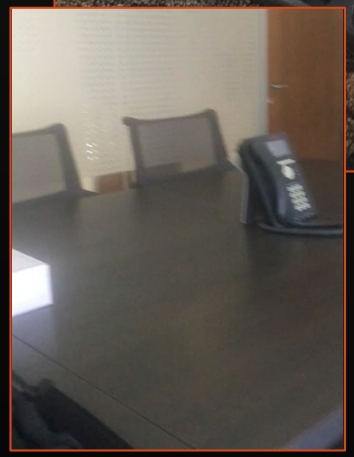
- Alex is talking to guard that everything is handled already
- Guard offers to escort to upper floors
- Alex kindly answers he is willing to take stairs
- While waiting at meeting room also asked about having a coffee ;-)
- While in: (45 minutes)
  Plugs Laptop, Recording Device to different meeting Rooms
- Alex leaves the building unnoticed!!

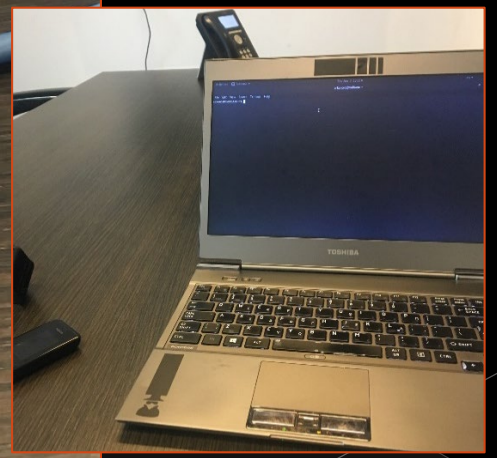
Attack Execution

Boom!









Reporting

Results (some..)

- **Weak Points**
  - Weak Authorization Process (No Identification Process)
  - Insufficient Staff Training (Piggybacking, Vishing, Unattended assets, etc.)
  - Blind/Weak Spots (Cameras, Open Doors, etc.)
  - Unsupervised guests at Branch Offices
  - Lack of proper monitoring
- **Strong Points**
  - External Media Protection
  - Incident Report Procedure
  - CCTV in place

Conclusions

Red Team

- Threat Analysis
- Simulate real attacks
- Check defenses and controls
- Do not overlook off-the-net attacks!

Contact us

Zisis Ziogas
Offering Manager
Cyber Security Solutions and Services
Neurosoft s.a

Email: **z.ziogas@neurosoft.gr**

WE IMPROVISE. WE ADAPT. WE DELIVER.

NEUROSOFT

Greece
466 Irakliou Ave. & Kiprou
141 22 Iraklio, Athens
Greece

Cyprus
2 Sophouli Street
The Chanteclair House,
1096, Nicosia
Cyprus

U.K
5th floor 1 Connaught Place
W22ET London
United Kingdom

U.A.E
Dubai Silicon Oasis,
Headquarters
PO Box 341568 Dubai,
United Arab Emirates

PROUD CREATORS OF PROXIMA+ | CONFIRM | ILLICIUM | ANGEL | REDYOPS

PROVISION ISR®

Now you can see!

Ronen Cohen
Regional Sales Director
Provision-ISR

www.provision-isr.com

Location. d

ISRAELI KNOW-HOW AND RELIABILITY

About

PROVISION-ISR

PROVISION-ISR is an Israeli multinational company founded in 2007 to meet the demands for high quality products in the medium segment of the CCTV market.

Israel has experienced the threat of terrorism for decades, and out of necessity, has come to excel in the homeland security arena.
Many Israeli security manufacturers hail from a variety of specialties including:
emergency management, cyber-security, intelligence, critical infrastructure protection, smart cities etc.

.

Worldwide

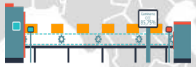
ORGANIZATION

Logistic Warehouse
(Panama)

Logistic Warehouse
(The Netherlands)

R&D, Support, Marketing, Sales
(Israel)

Production Units
(China)



Logistic Warehouse
(China)

Global Distribution

NETWORK

We serve **more than 40 countries** on **5 continents** with official exclusive distributors.

What We Provide

- ✓FULL **CAMERA** PRODUCT RANGE.
- ✓BEST OF BREED **DVRs /NVRs**.
- ✓COMPLETE RANGE OF **ACCESSORIES**.

- We constantly upgrade the products while keeping in mind issues of **COST** and **QUALITY.**

NEEDS ASSESSMENT

What make us different

Brand

PHILOSOPHY

Betting against the choices of other manufacturers, Provision-ISR says **“NO” to e-commerce**, enhancing the irreplaceable service guaranteed by our sales network. Our professional ethics leads us to **respect and protect all the actors of the supply chain:** from the big distributor to the small installer.

What make us different

One-Stop-Shop

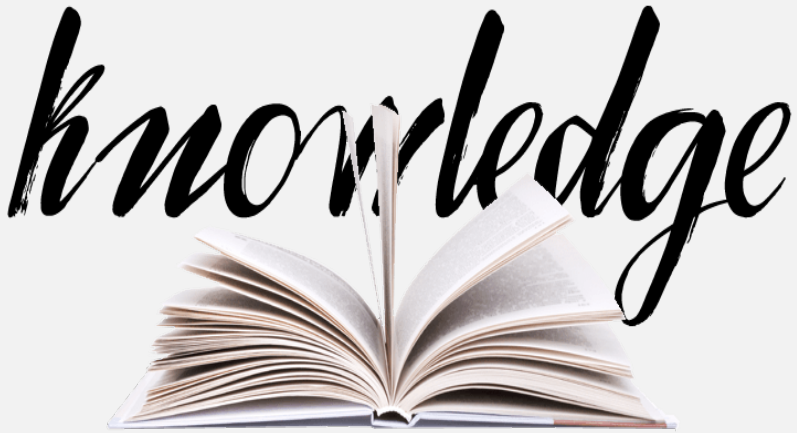
FORMULA

Provision-ISR understands the need for **tested and reliable CCTV accessories**. We have managed to create a full range of accessories matching all types of installation. Today we proudly represent a One-Stop-Shop for all CCTV product needs.

CCTV KNOWLEDGE!

“Knowledge is power. Information is liberating. Education is the premise of progress, in every society.”

Kofi Annan (Former Ghanaian Diplomat)



In today’s CCTV market, where products and technologies change every few months, knowledge is the keyword, and we believe that delivering the information all the way from the manufacturer thru the entire chain all the way to the installer is our responsibility.

Provision-ISR’s technical specialists, release a new How-to-tutorial every time a new solution is launched into the market.

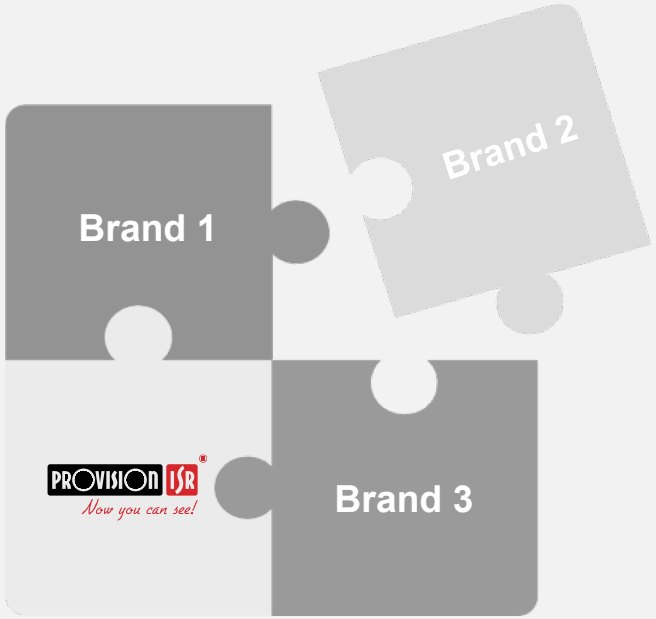
Technical webinars are periodically organized to update Provision-ISR customers about product upgrades or new features.

Last but not least, Provision-ISR roadshows, seminars, training sessions and workshops take place all over the world to support distributors, sub distributors and installers.

FULL COMPATIBILITY WITH OTHER BRANDS DEVICES

“I want to break free.”

Queen (British rock band)



We believe that the installer shouldn’t be forced to choose between brands or technologies.

What does it mean?

Provision-ISR solutions have been designed to be compatible with the ones of other brands. Our HD cameras allow the installer to select the output and they are well-matched with any recorder machine available in the market

- TVI
- CVI
- AHD
- ANALOG

Our HYBRID DVRs allow the installer to connect each and every channel to the technology he wants!

- Each channel automatically recognize the connected device.

SIMPLE AND INTUITIVE SOFTWARE AND APPLICATIONS

“Simplicity is the ultimate sophistication.”

Leonardo da Vinci
(Renaissance painter, scientist, inventor, and polymath)

According to Provision-ISR philosophy “advanced” shouldn’t be a synonymous with “complicated”.

This is why our Israeli engineers aim at developing advanced software solutions keeping the user interface simple and intuitive.

Do you need an example?
Today, thanks to the APP Provision CAM2, you can easily manage you face database with your smartphone!

FACE RECOGNITION:
MANAGE YOUR FACE DATABASE BY THE APP

Beeing a Provision-ISR Partner

“You must have a professional and strong partner to win the market.”

Ari Pick
(Provision-ISR CEO)

PROVISION ISR®
Now you can see!

SDC
SECURITY | DISTRIBUTION | CENTER

Thank you