

Sergey Puzankov

Invisible threat in SS7 networks – attacks based on caller ID spoofing

POSITIVE TECHNOLOGIES

ptsecurity.com

About Positive Technologies

POSITIVE TECHNOLOGIES

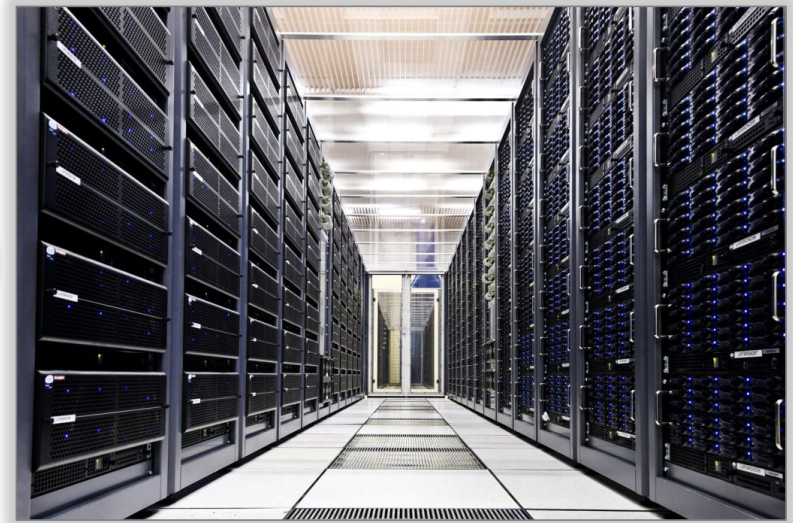
- + 700 people in nine offices across North America, Asia, Africa and Europe and expanding
- + Portfolio securing large organizations and infrastructure providers from targeted attacks through vulnerability detection and management
- + 21% group yearly revenue increase
- + 60 – 70% reinvested back into research, feeding directly through to products
- + Partners include Check Point, Cisco, Microsoft, Google, Oracle, Siemens and IBM
- + 1,000 customers



SIGTRAN is a Time Machine

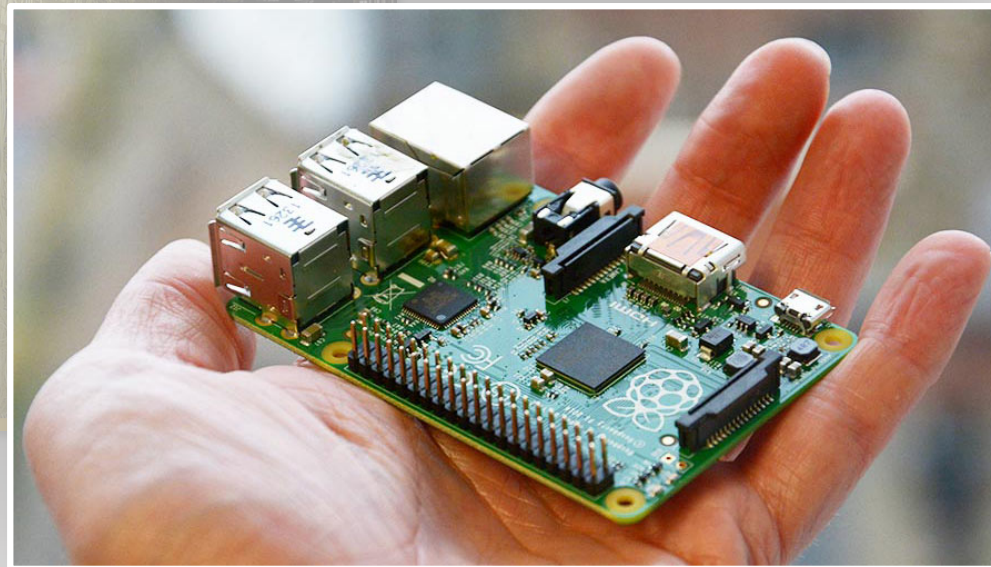
POSITIVE TECHNOLOGIES

Through SIGTRAN back to 1970's



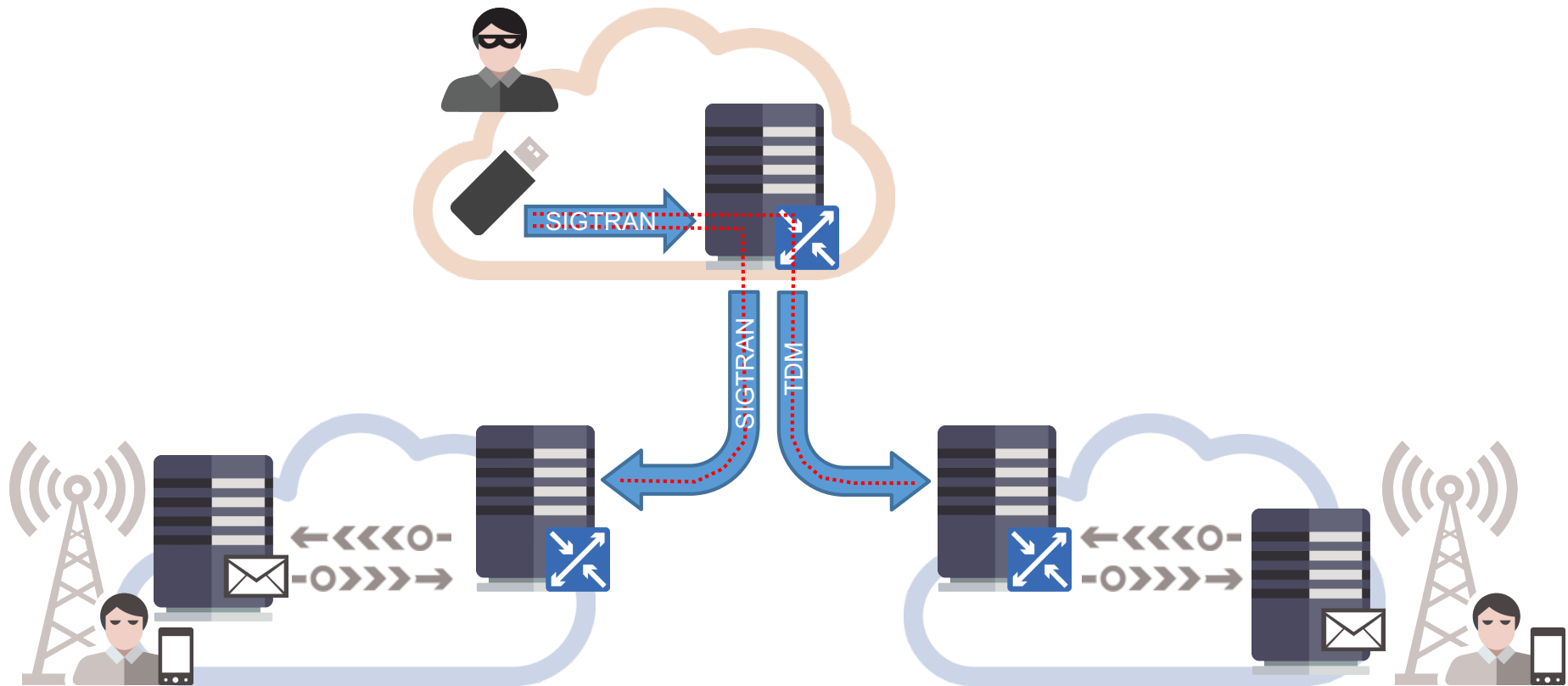
Micro Computer as an SS7 Node

POSITIVE TECHNOLOGIES



SIGTRAN – TDM

POSITIVE TECHNOLOGIES





Fraud and Security Group

IR.82 SS7 Security Network Implementation Guidelines

FS.07 SS7 and SIGTRAN Network Security

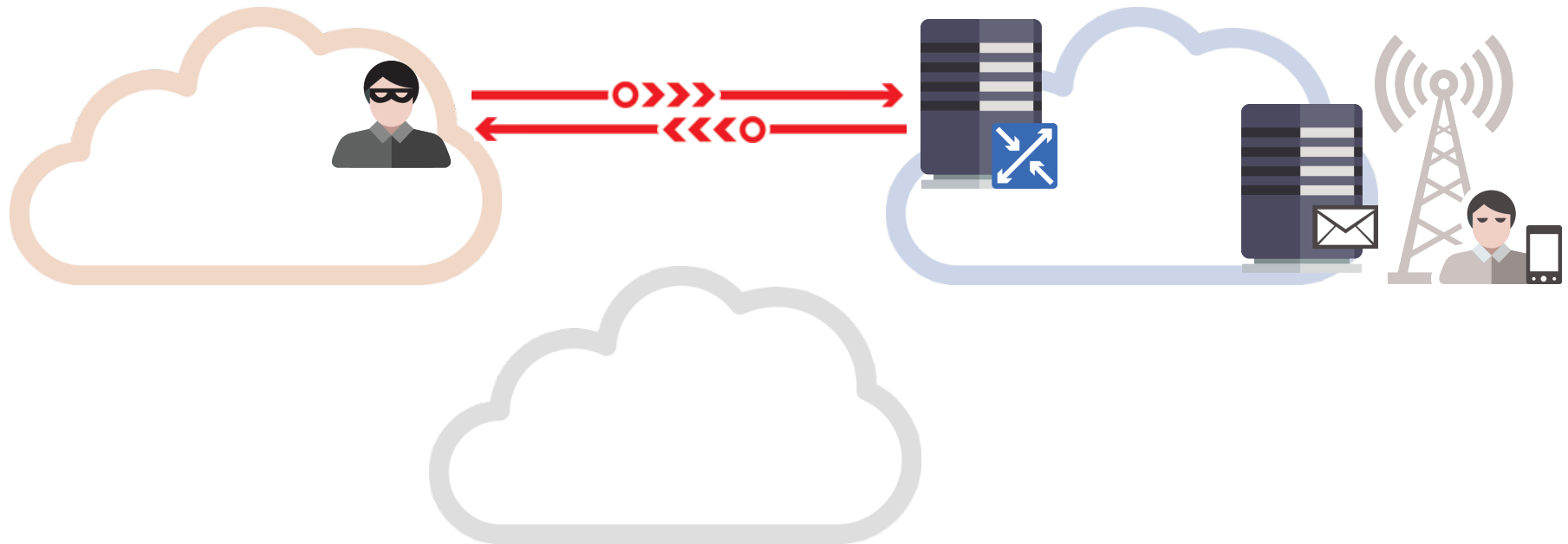
FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines

FS.19 Diameter Interconnect Security

FS.20 GPRS Tunnelling Protocol (GTP) Security

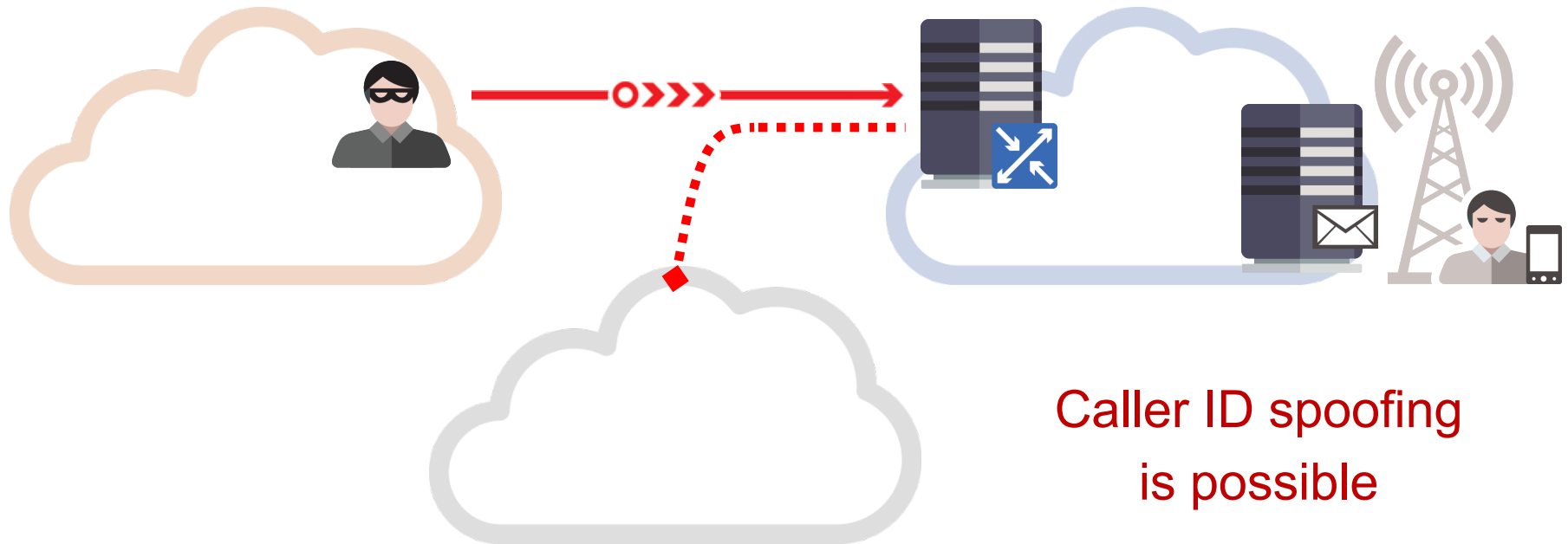
FS.21 Interconnect Signalling Security Recommendations

Answer is required



- Identity request (e.g. IMSI)
- Location request
- Network information request

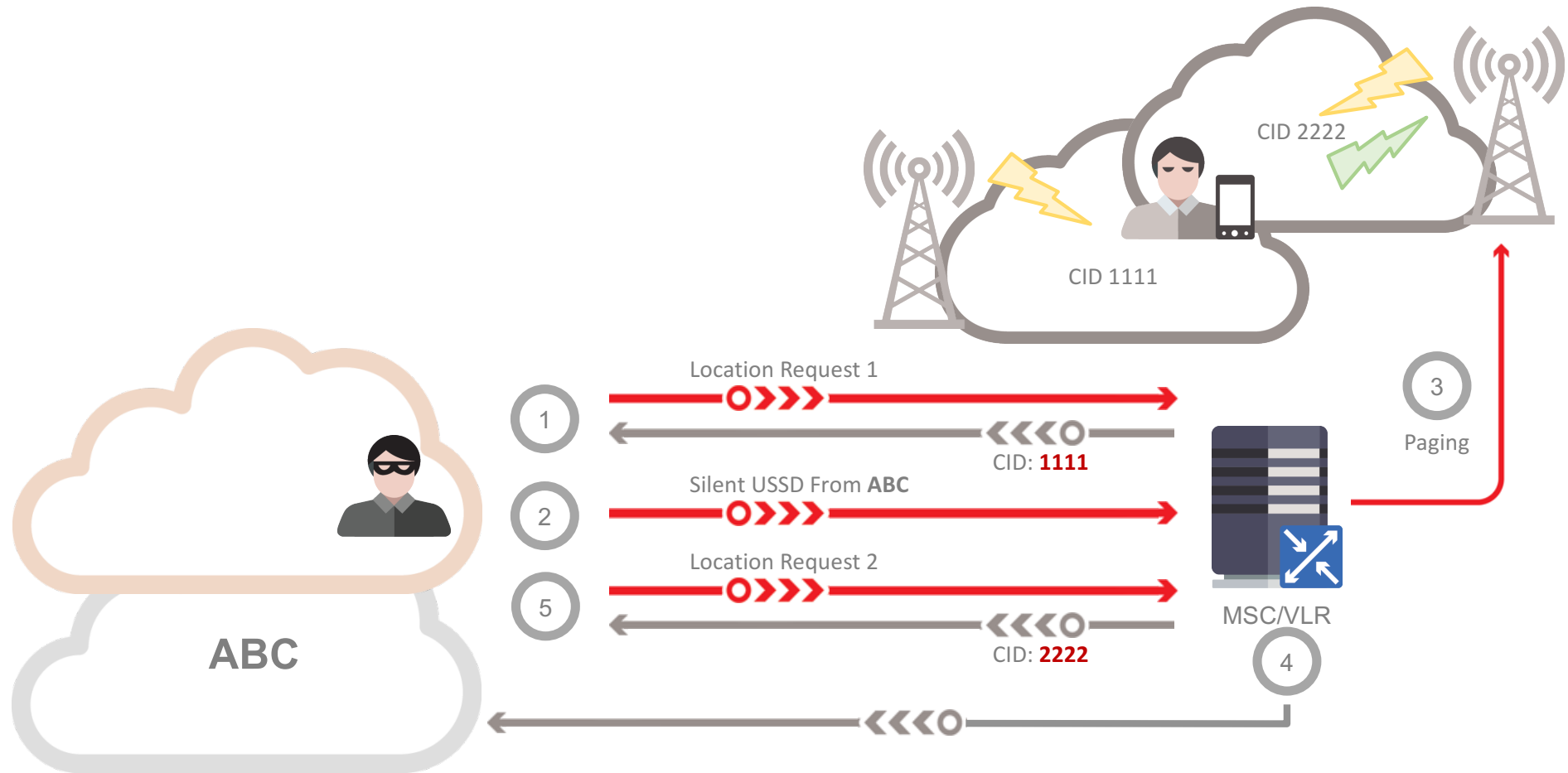
Answer is not required



- Service disruption (DoS)
- Data injection
- Service manipulation

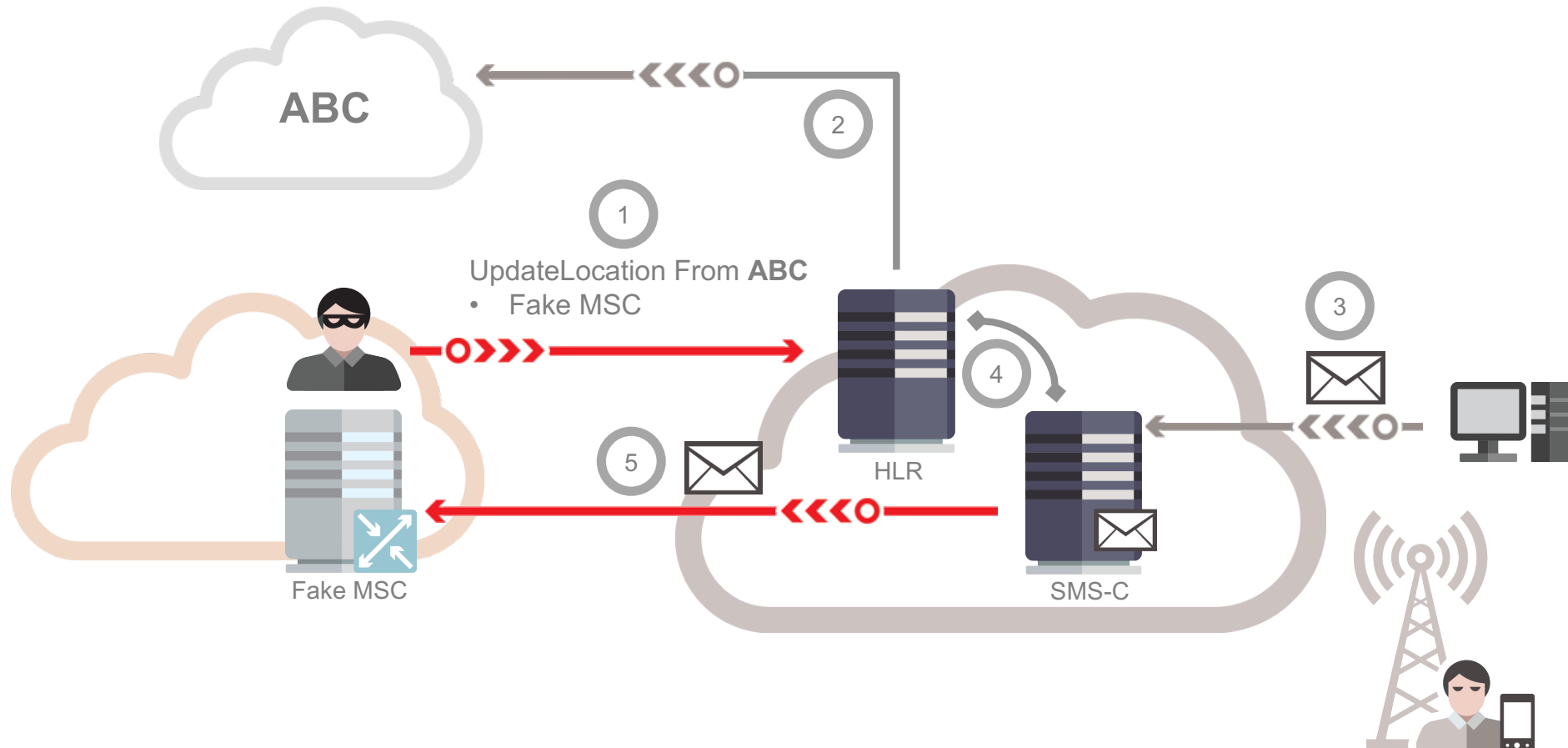
Caller ID Spoofing at Position Refinement Attack

POSITIVE TECHNOLOGIES



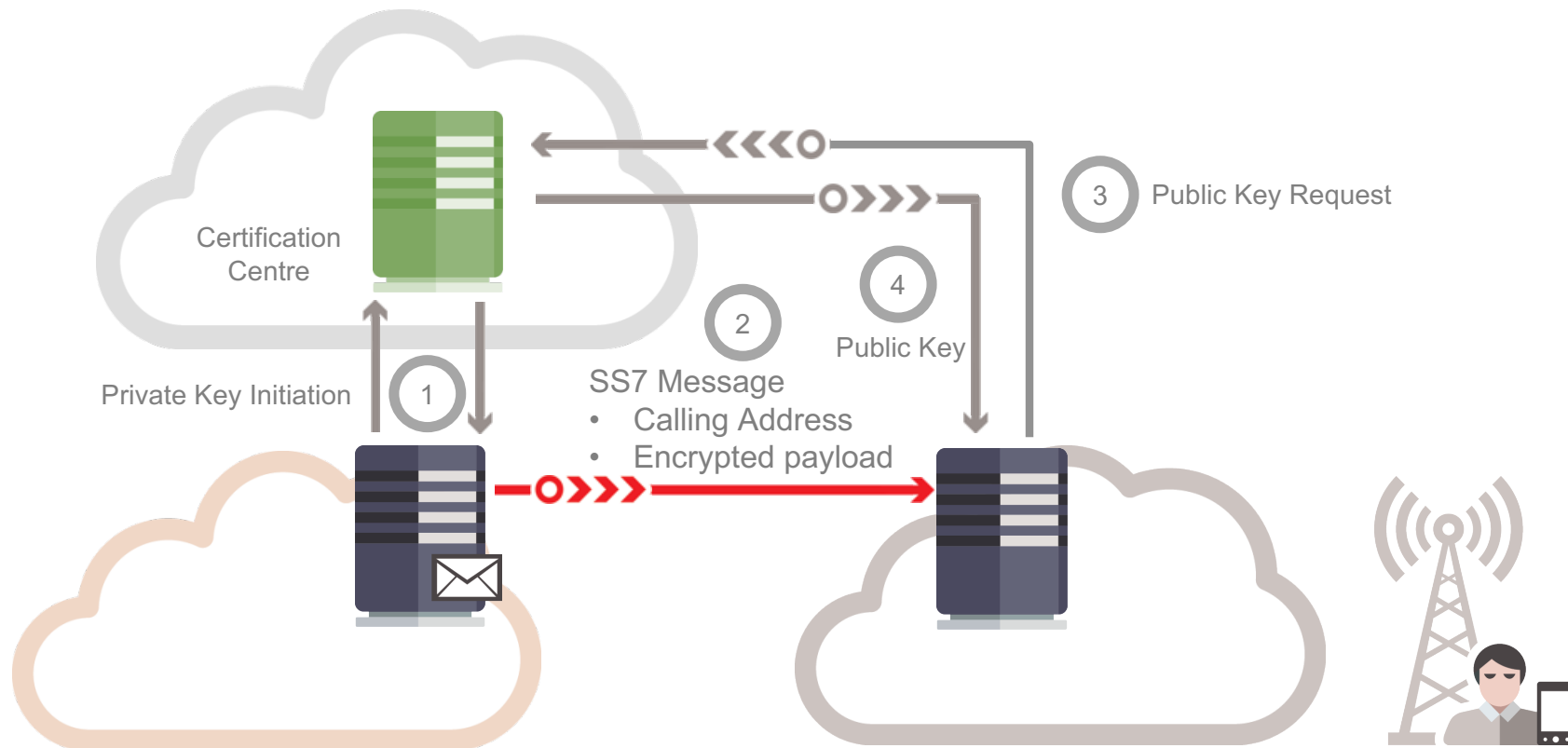
Caller ID Spoofing at SMS Interception Attack

POSITIVE TECHNOLOGIES



PKI in SS7 Networks: Encryption

POSITIVE TECHNOLOGIES





Thank you!

POSITIVE TECHNOLOGIES

ptsecurity.com