HoneySAP

Who really wants your money?

CORE SECURITY

MARTIN GALLO

MARCH 2015

TROOPERS
MAKE THE WORLD A SAFER PLACE

AGENDA

- SAP
- SAP security
- Threat landscape
- Have
- Needs
- Honeypots
- HoneySAP
  - Approach
  - Goal
  - Design
  - Architecture
  - Services
  - Integration
  - Example profiles
- Demo
- Challenges
- Call to contributions
- Conclusions

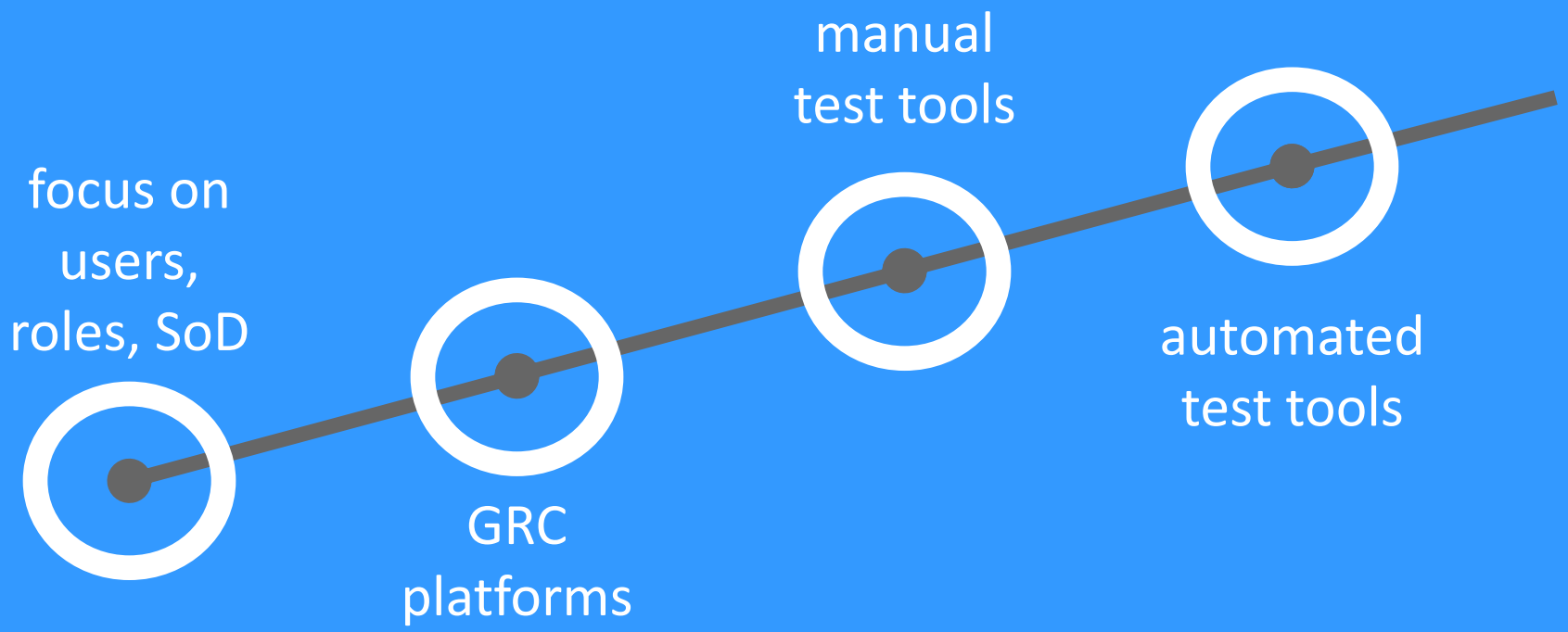
WHAT IS SAP?

software company
business processes
critical systems
$$$

SECURITY IN SAP?

specialized skills
commitment
risk culture
$$$

SECURITY IN SAP?



THREATS IN SAP?

complexity
customization
lack of knowledge
business dynamics

THREATS IN SAP?

fraud
espionage
sabotage
insider & outsider

Targeted attacks

known for years
traditional attacks
targets not disclosing data
now started appearing in media

more recent
malware looking for SAP
entry point for targeted attacks

Broad attacks

THREATS

LANDSCAPE

WHAT DO WE HAVE?

some knowledge
distributed
weak defenses

WHAT DO WE NEED?

learn
share
act

MEET

Honeypots

HONEYPOTS

types
goals
implementations

HONEYPOTS

interaction

high / medium / low

purpose

research / production

HONEYPOTS

gather information

catch malware

deceit/distract

…

HONEYPOTS


honeyd
tftp
smtp
dionaea
rdp
clientside
rdpy
upnp
compot
linux
nova
kippo
browser
smb
ssh
wordpot
telnet
mirage
amun
mssql
ics
spam
honssh
ftp
bash
honeyc
mailoney
mysql
wordpress
shockpot
http
thug
bifrozt
glastopf
shiva
sftp
vnc
dns
rdphoneypot
scada
sip

MEET

HoneySAP

APPROACH

low-interaction
research centric
open source

GOALS

specific purpose
identify behavior
flexibility
agility

DESIGN

extendible

add services

add feeds

DESIGN

modular

dynamic loader

services, feeds & datastore

DESIGN

easy to configure

JSON & YAML

default profiles

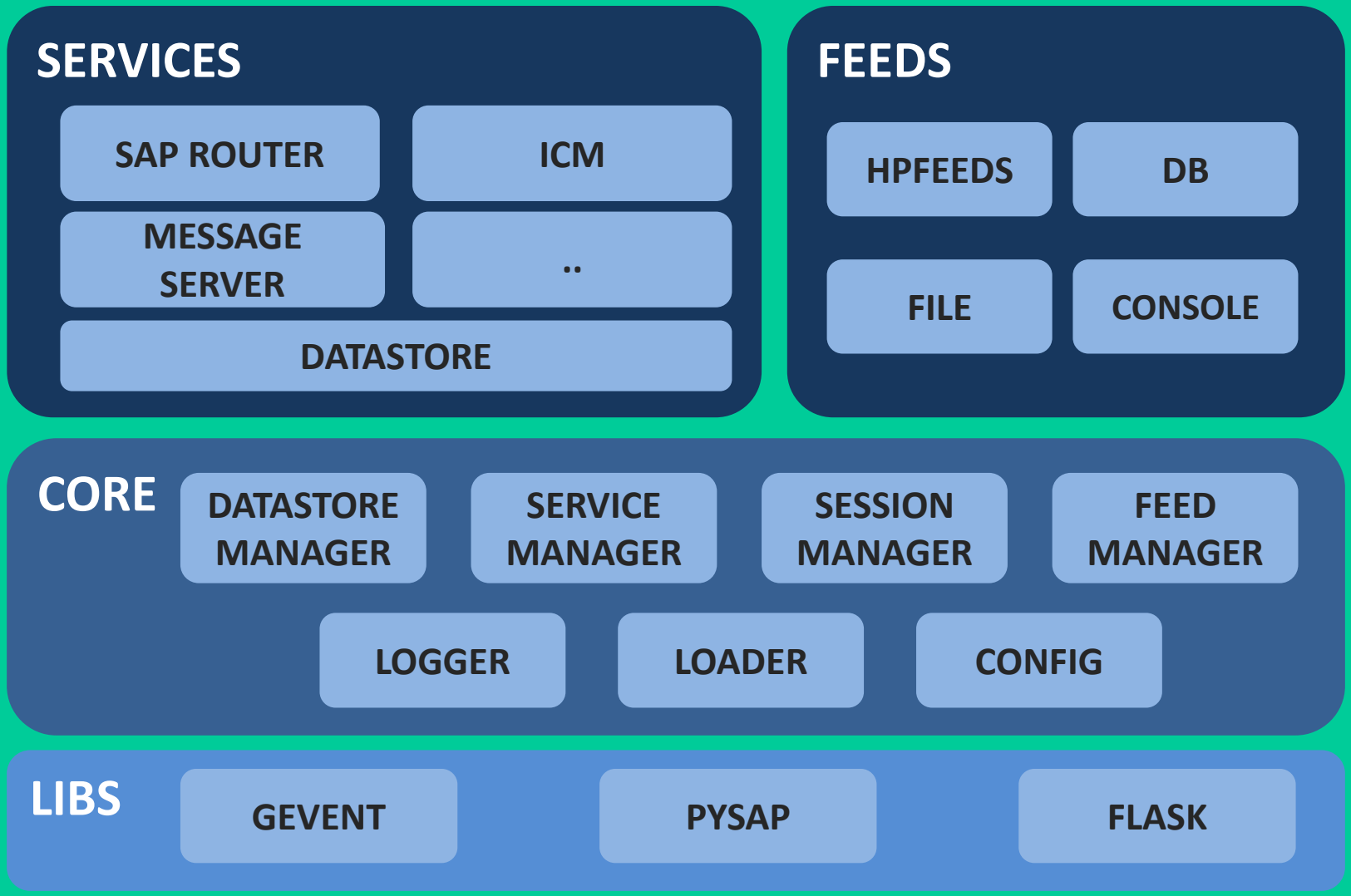
DESIGN

easy to deploy

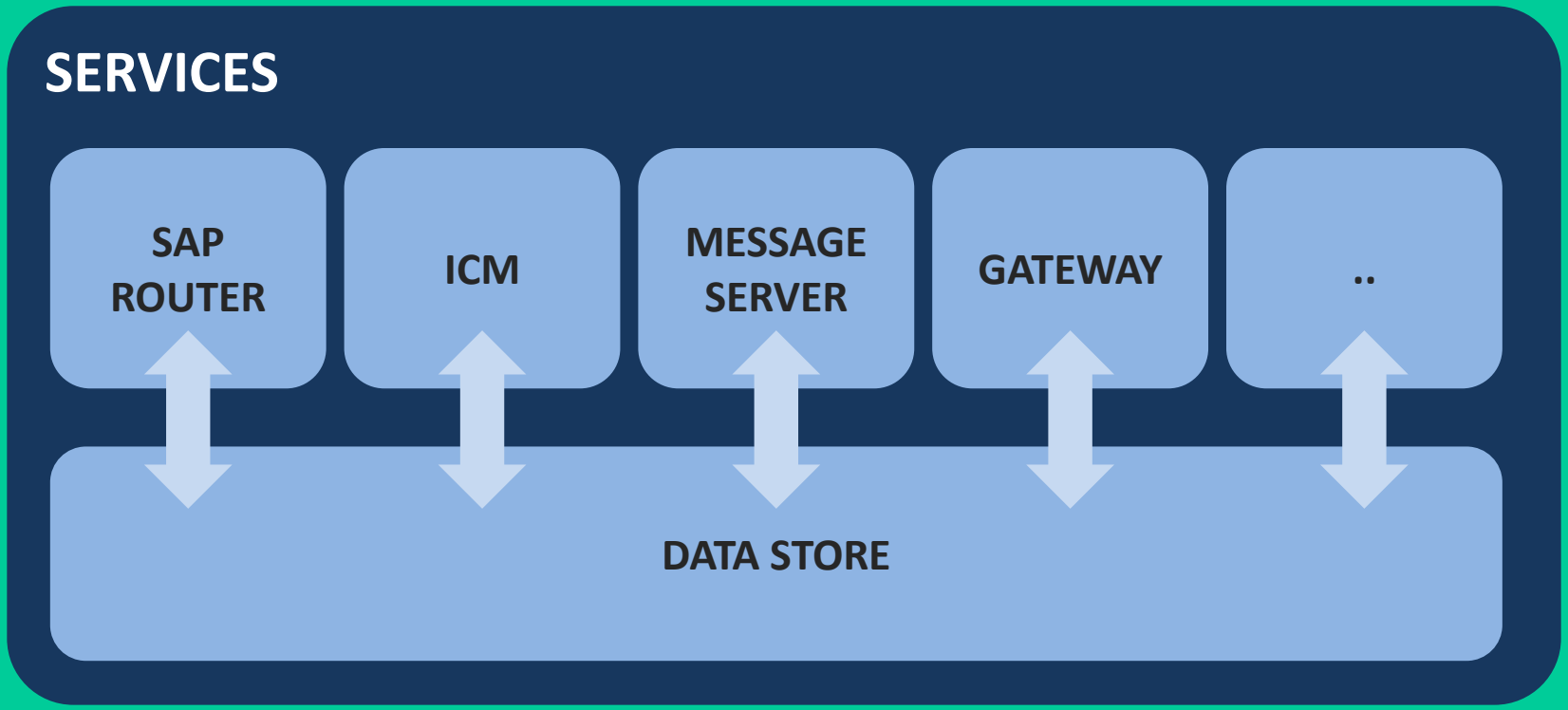
vagrant + ansible

docker?

ARCHITECTURE



ARCHITECTURE



HTTP-based services

- ICM
- MESSAGE SERVER
- WEB DISPATCHER
- NW GATEWAY
- ..

PySAP-based services

- ROUTER
- MESSAGE SERVER
- DISPATCHER
- GATEWAY
- ..

SERVICES

virtual services

don’t bind to real addresses

allows routing/dispatching

SERVICES

forwarder service

forwards traffic to ext. services

can be run as a virtual service

INTEGRATION

honeypots

routing/dispatching, honeynets, deployment

actual systems

routing/dispatching

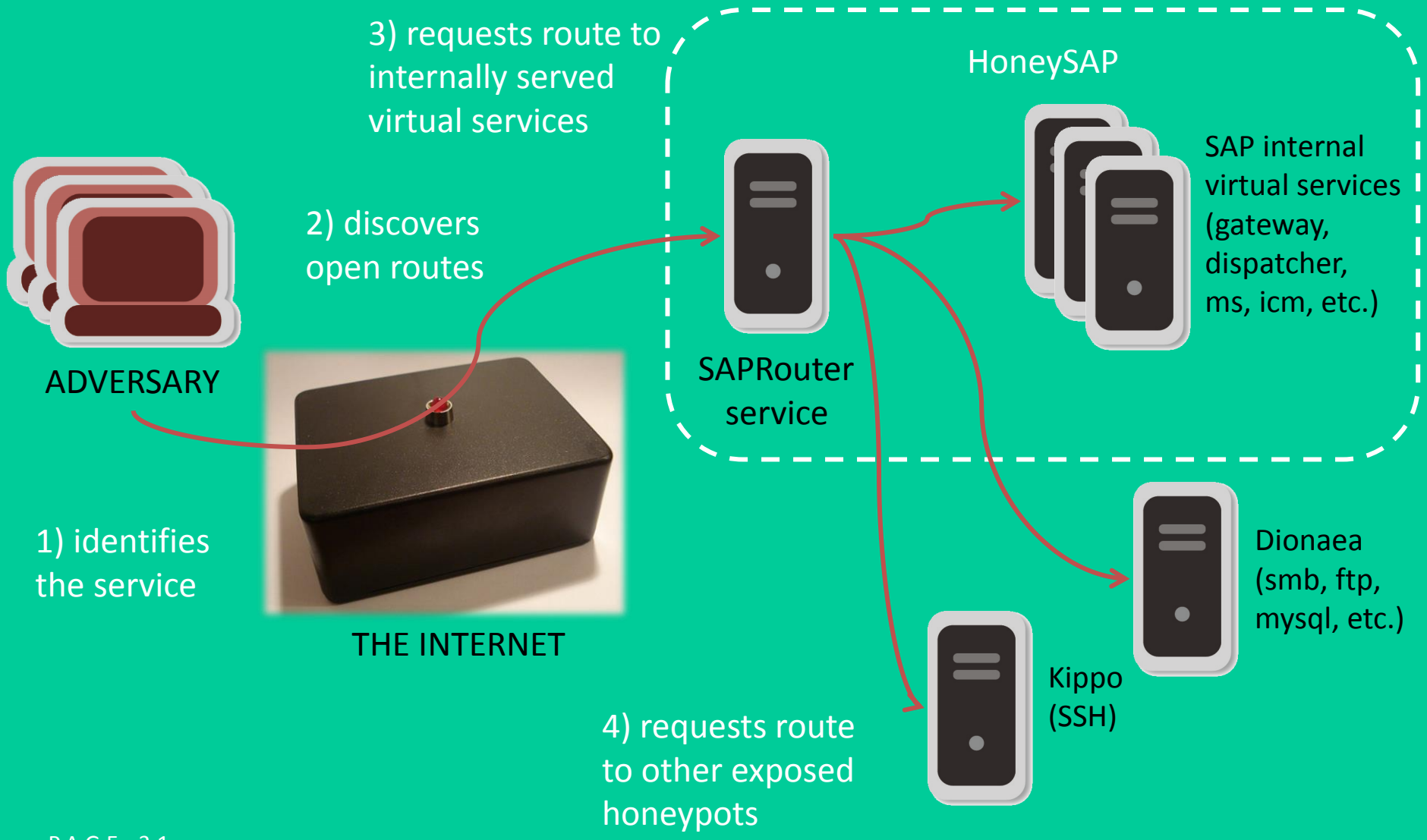
INTEGRATION

standard feeds

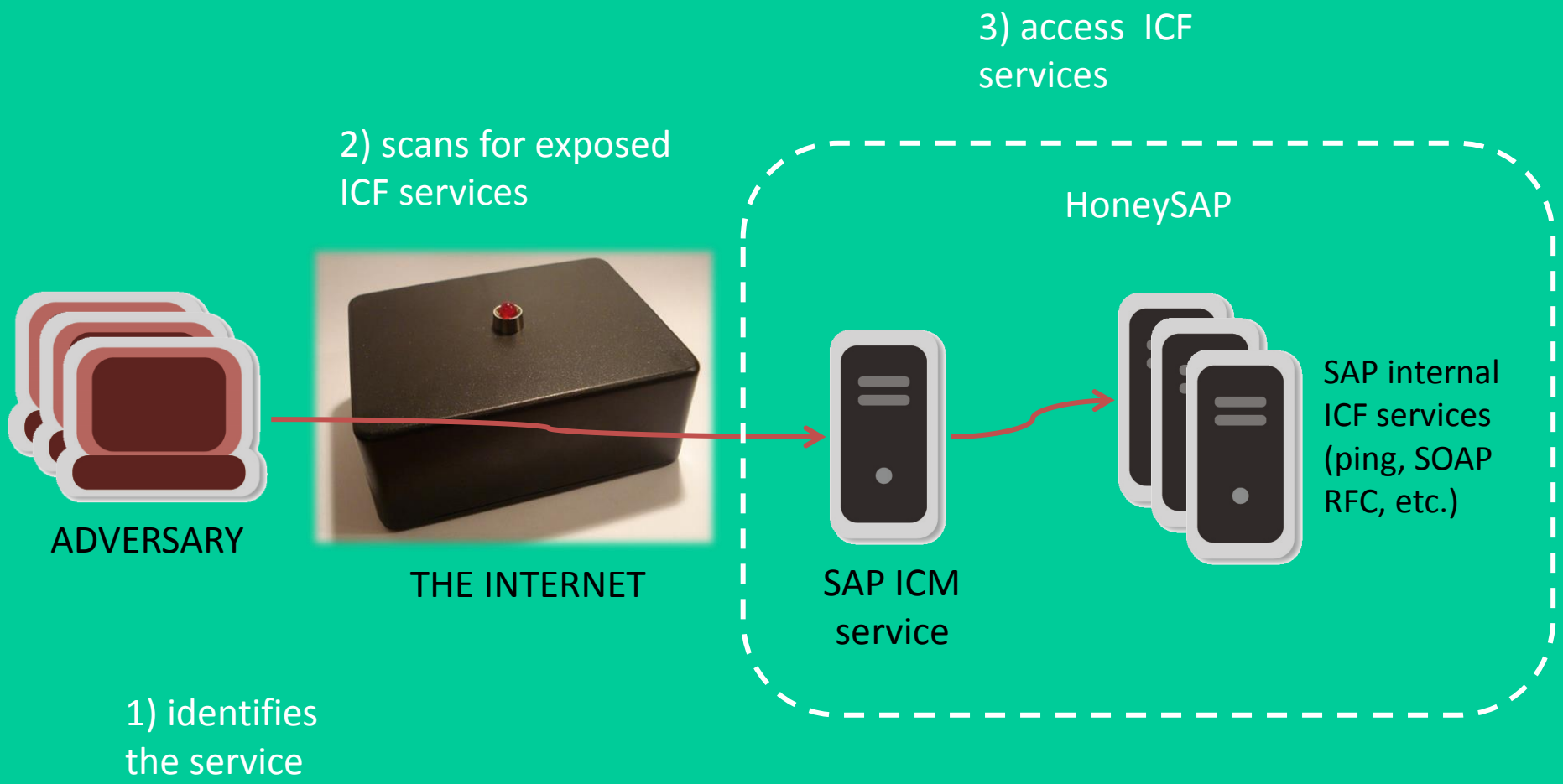
hpfeeds, taxii, stix

..

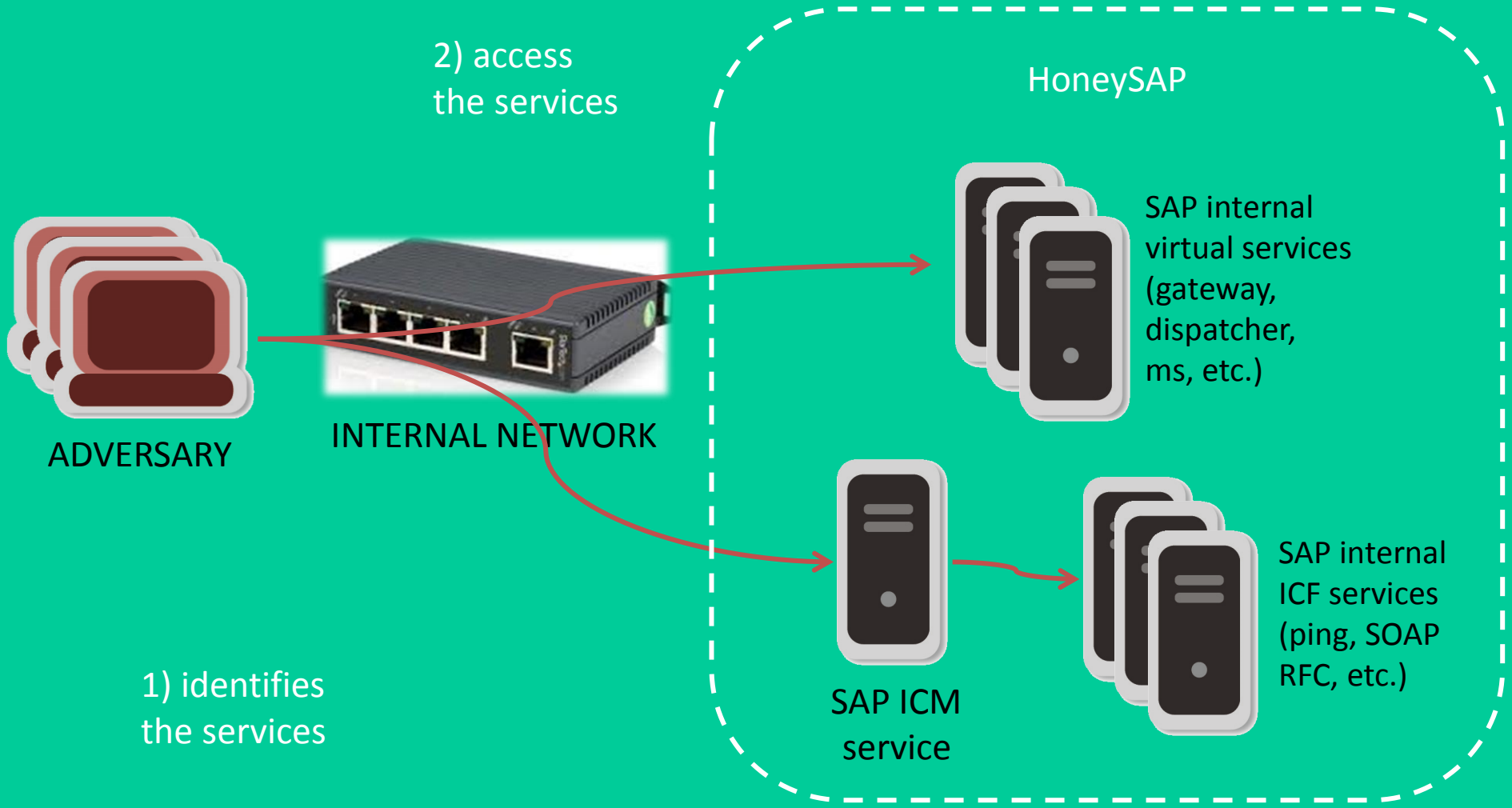
EXAMPLE PROFILE



EXAMPLE PROFILE



EXAMPLE PROFILE



DEMO TIME

CHALLENGES

core development

modular structure

gevent + scapy/flask

CHALLENGES

+ knowledge on each service

packets not enough behavior

CHALLENGES

detection

non-standard behavior

error messages

http services

CHALLENGES

performance?

not sure yet

CHALLENGES

what to log?
determine IoA/IoC

CHALLENGES

deployments

make it easier to deploy

integration

CALL FOR CONTRIBUTIONS

run, test, patch, submit
collect & analyze
extend

CALL FOR CONTRIBUTIONS

grab it soon from

https://github.com/CoreSecurity/

http://corelabs.coresecurity.com/

GPLv2 license

working on data feed

CONCLUSIONS

more knowledge about services
new source of attacks info
diff. approach for defense

Q&A

???

THANK YOU !

mgallo@coresecurity.com
@martingalloar