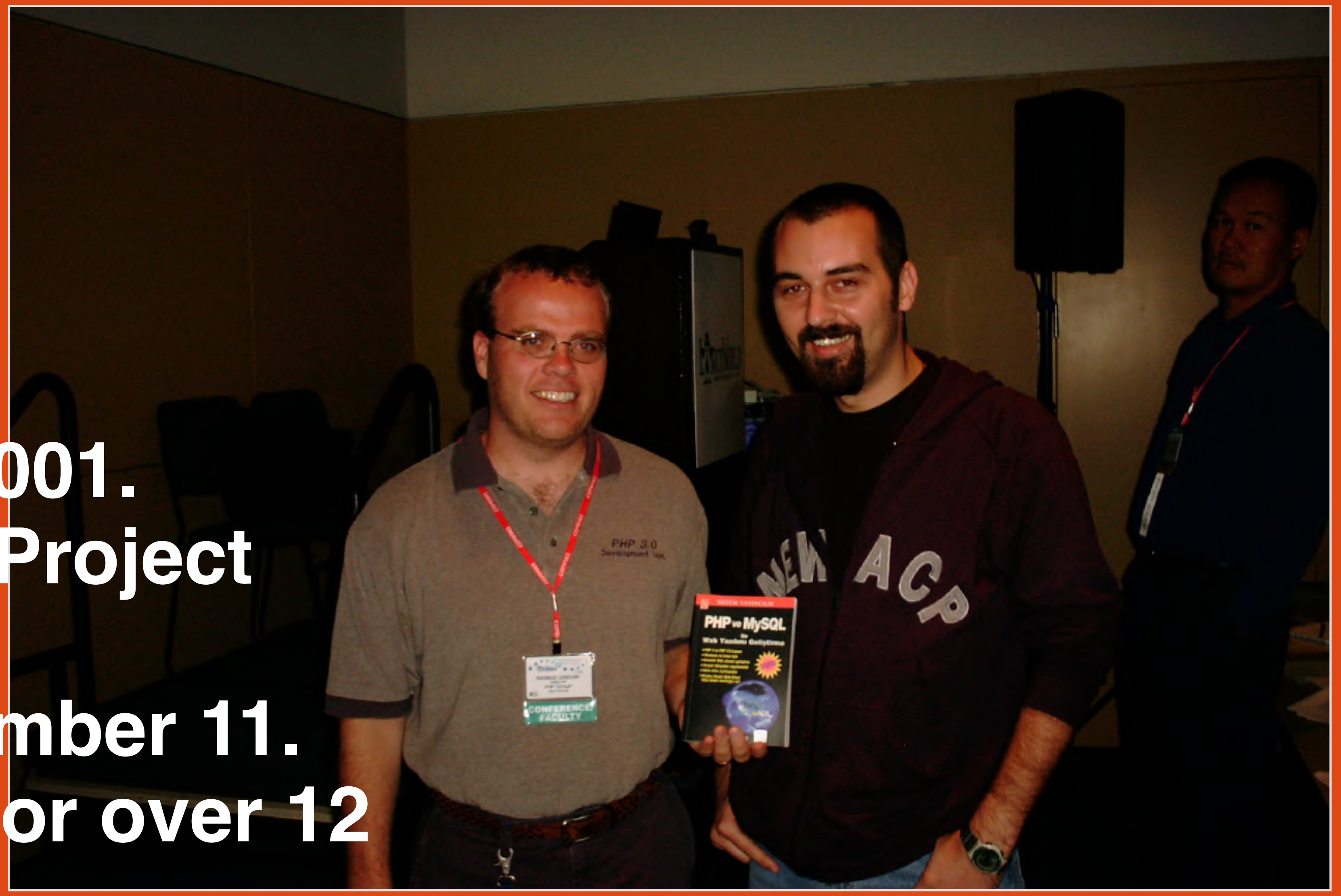
SecOps Strategies & How to Deploy Honeypots into your Kubernetes

21st of March, 2019 | DevOpsPro Europe 2019 / Vilnius / Lithuania

kayra.otaner@secops360.com

About Me

Kayra Otaner



- Have been using Linux since 1994,
- Gentoo & Linux From Scratch Fan (#5893)
- Author of first Php & MySQL book written in Turkish published in 2001.
- Chief Architect for Turkish Navy’s Open Source Ahtapot (Octopus) Project (www.ahtapot.org.tr)
- Lived in New York City, saw second plane hitting WTC live in September 11.
- Worked as Director of IT Operations in NYC/ mostly in Wall Street, for over 12 years.
- Co-Founder and CEO of SecOps360 IT Security and Internet Operations
- Father of two & Devoted Istanbul admirer
- Docker & Security Evangelizer

- https://twitter.com/kayraotaner
- https://www.linkedin.com/in/kayraotaner

SecOps talks

https://devopspro.lt/2017/

DevOps Pro
Home
Speakers
Call for papers
Sponsors
Venue
Contact Us
Other conferences

Kayra Otaner

DataSkala, Turkey

An author of first Php & MySQL book written in Turkish

Later he has moved to New York City, worked as Directo

in Wall Street for over 12 years. Later after returning bac

https://www.youtube.com/watch?v=0FlyOoQ-y4g&t=641s

It essentially acknowledges the fact that conventional Firewalls and IDS/IPS systems, that only protects macro perimeter are not enough.

© Kayra Otaner 2017
kayra.otaner@dataskala.com

Utilizing Docker to create a MicroPerimeter for ZeroTrust Security" - Kayra Otaner

105 views

DATA MINER
Published on Apr 26, 2017

SUBSCRIBE 325

In this talk, Kayra will tell how we can utilize Docker & Container technologies to monitor, analyze, detect and respond.

SHOW MORE

https://www.youtube.com/watch?v=aWU7DL3wtt4&t=122s

Meet our Speakers

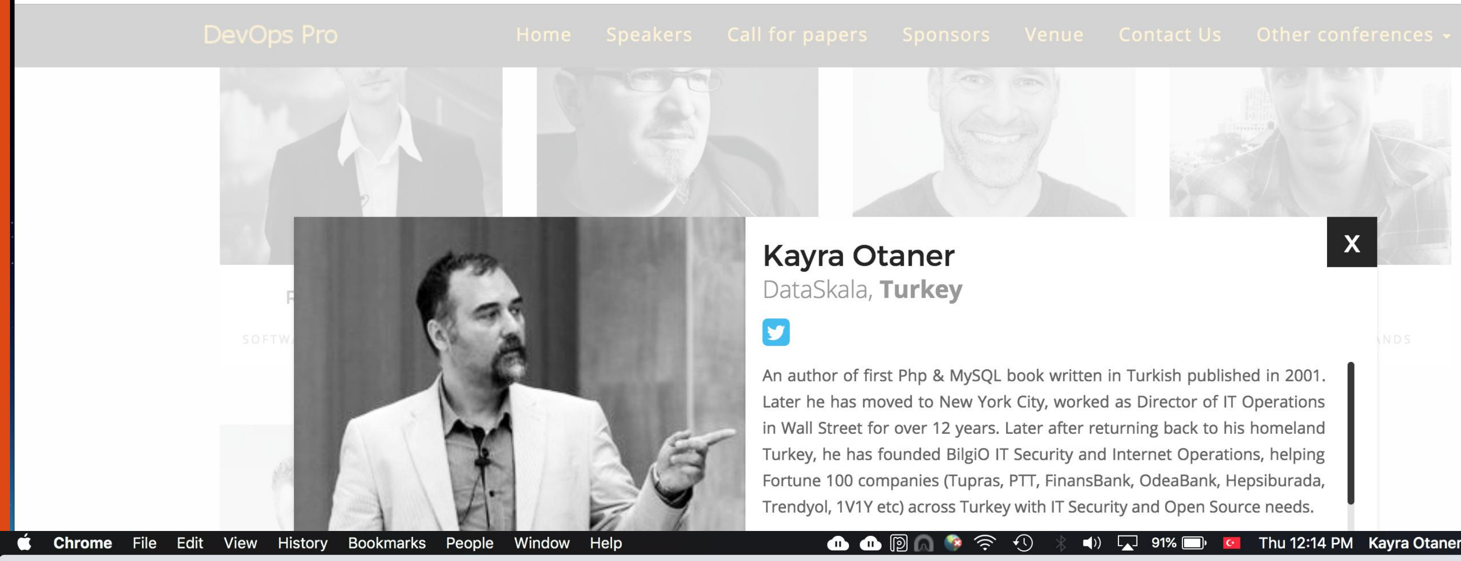
DataSkala, Turkey

Kayra Otaner

Kayra is a Co-Founder and CEO of DataSkala IT Security and Internet Operations Father of two & Devoted Istanbul

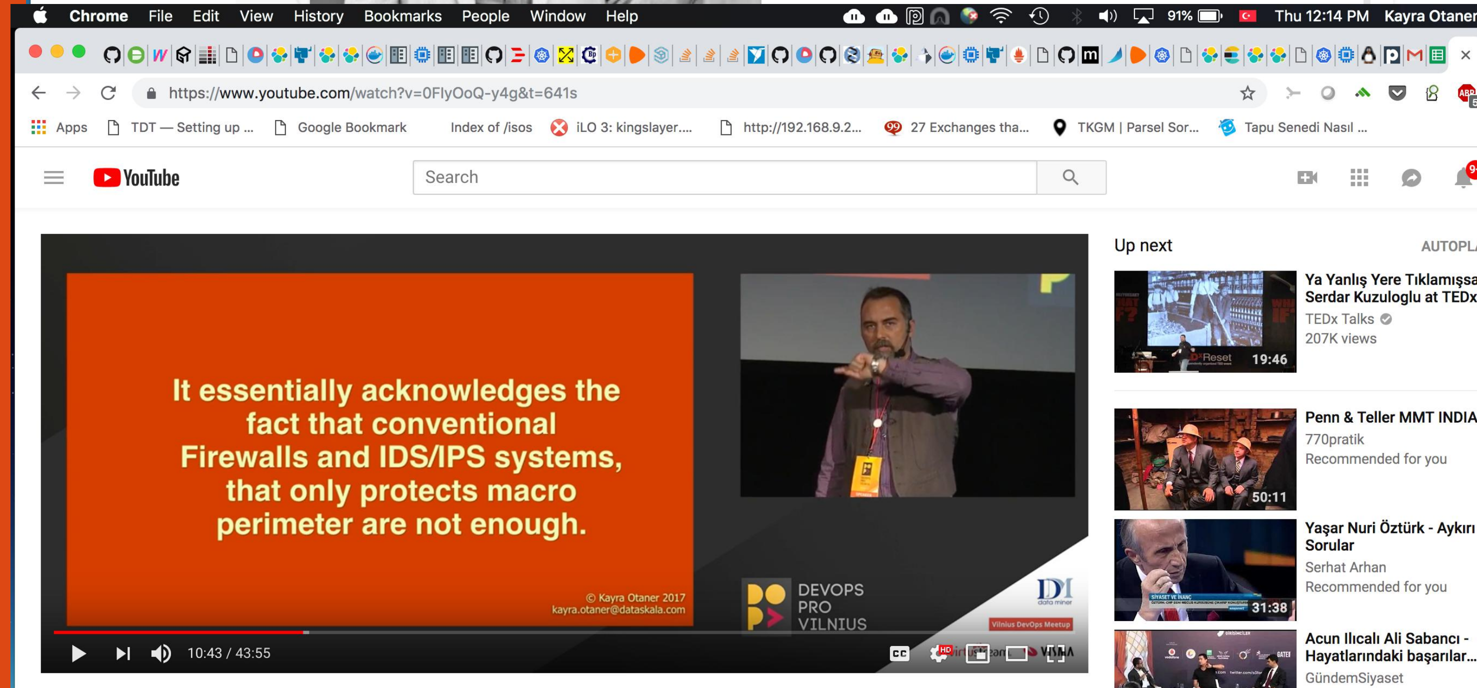
SecOps Talks

- **June 2016, DevOpsDays Istanbul/Turkey**
  Utilizing DevOps for Security Orchestration and Situational Awareness
- **April 2017, DevOpsPro Vilnius/Lithuania**
  Utilizing Docker to create MicroPerimeter for ZeroTrust Security
- **November 2017, DevOpsPro Moscow/Russia**
  Security with Docker: HoneyPots as an environment
- **March 2019, DevOpsPro Europe Vilnius/Lithuania**
  SecOps Strategies & How to Deploy Honeypots into your Kubernetes



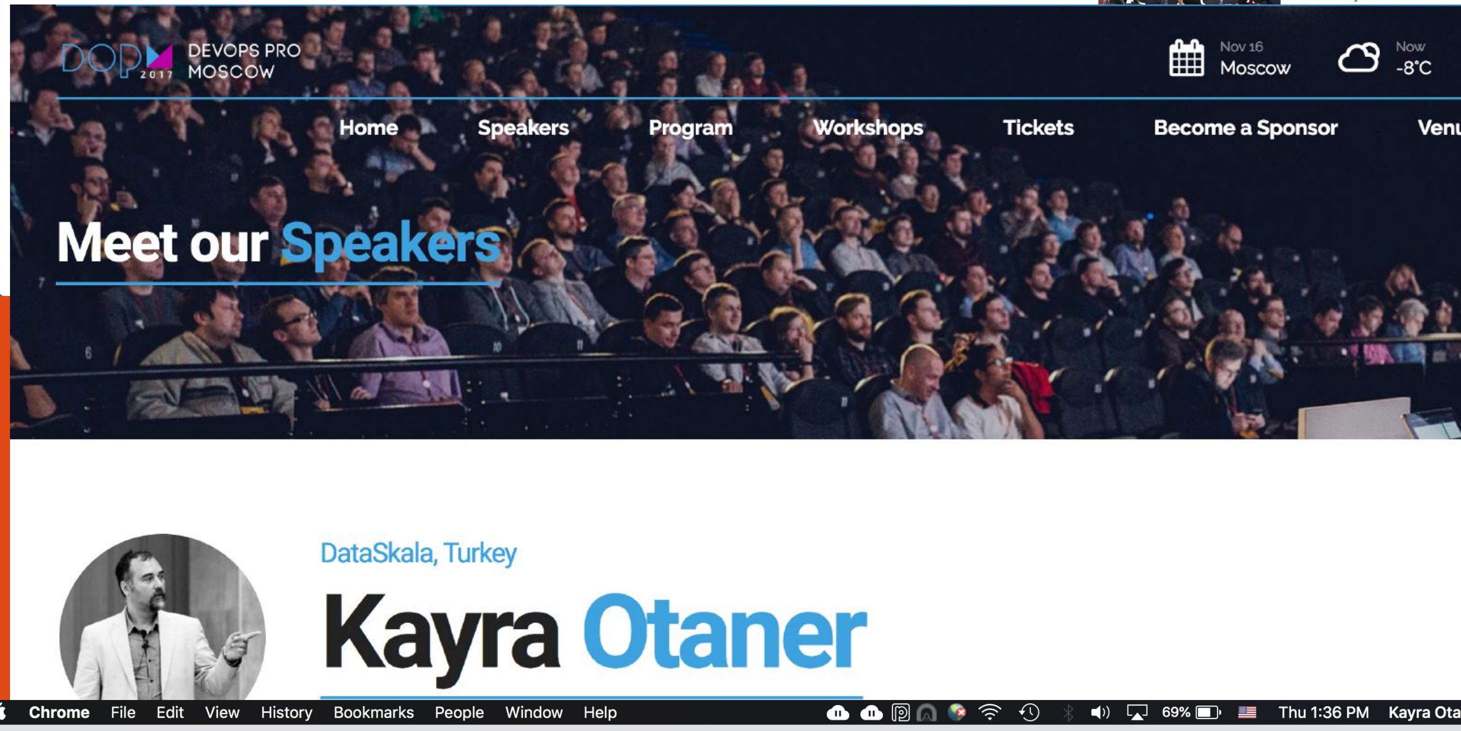
Kayra Otaner
DataSkala, **Turkey**

An author of first Php & MySQL book written in Turkish published in 2001. Later he has moved to New York City, worked as Director of IT Operations in Wall Street for over 12 years. Later after returning back to his homeland Turkey, he has founded BilgiO IT Security and Internet Operations, helping Fortune 100 companies (Tupras, PTT, FinansBank, OdeaBank, Hepsiburada, Trendyol, 1V1Y etc) across Turkey with IT Security and Open Source needs.



It essentially acknowledges the fact that conventional Firewalls and IDS/IPS systems, that only protects macro perimeter are not enough.

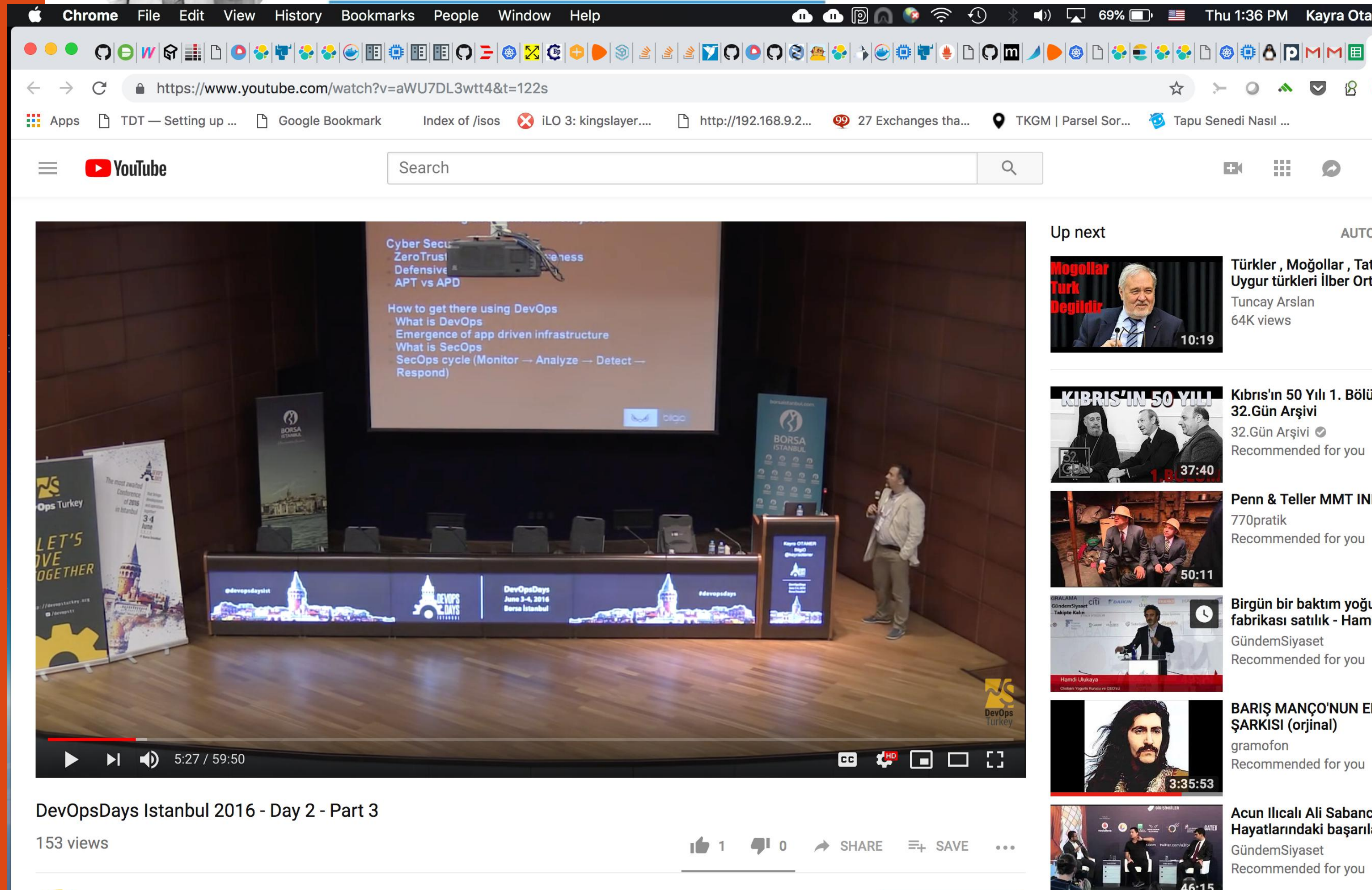
© Kayra Otaner 2017
kayra.otaner@dataskala.com



Meet our Speakers

DataSkala, Turkey

Kayra Otaner



Cyber Secu
ZeroTrust
Defensive
APT vs APD

How to get there using DevOps
What is DevOps
Emergence of app driven infrastructure
What is SecOps
SecOps cycle (Monitor → Analyze → Detect → Respond)

DevOpsDays Istanbul 2016 - Day 2 - Part 3
153 views

Goals of this talk

- Give you clear understanding of what DevOps and SecOps are.
- Reduce your “Time to Discovery”
- Show you how easy it is to deploy honeypots into environment

Know How vs Know Why

The person who know HOW
will always have a job,

The person who knows WHY
will always be his boss

Diane Ravitch

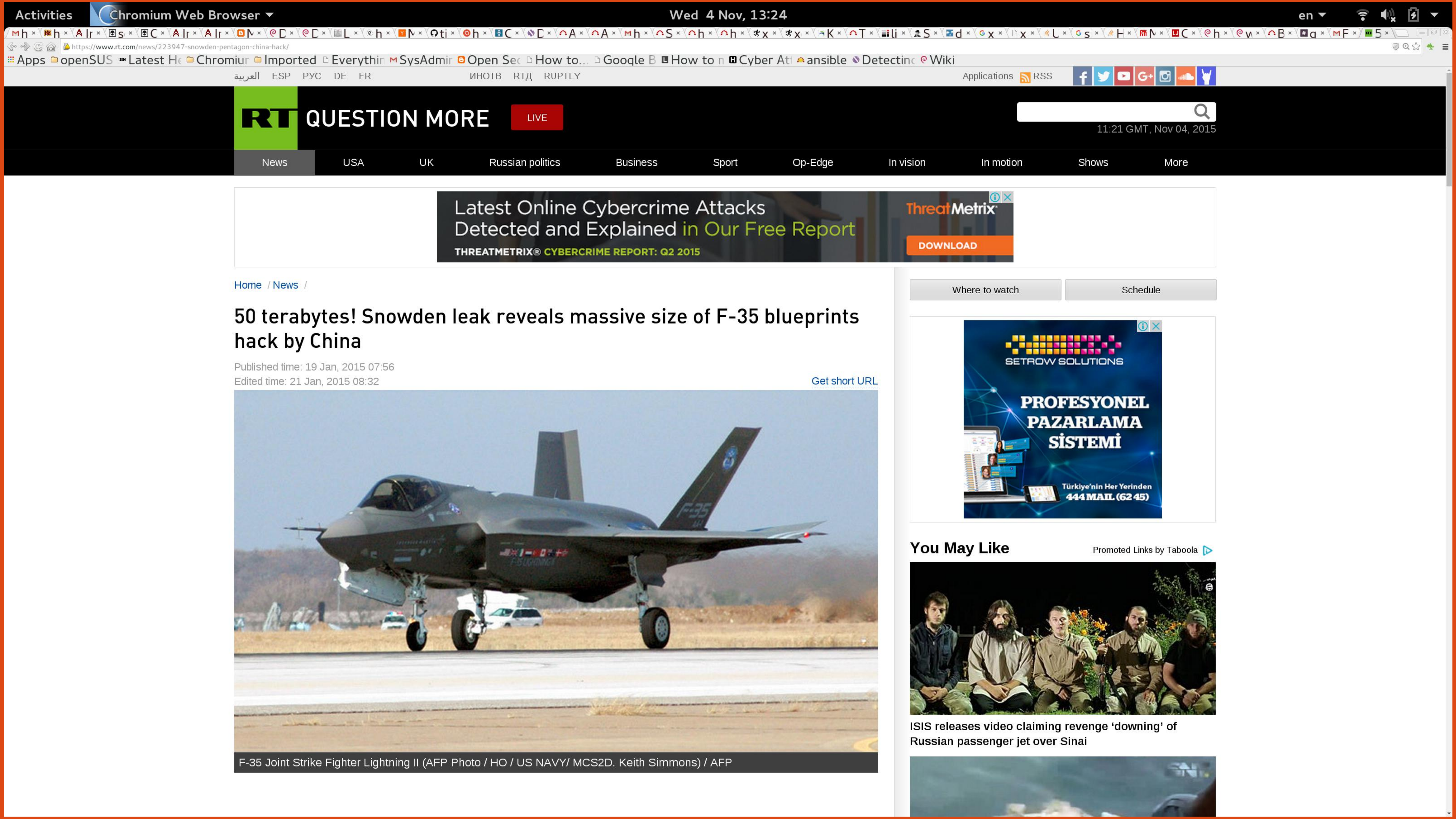
Those who know how will always work for those who know why

What we will be talking about :

- Time to Discovery
- Zero Trust & MCAP: Micro Core and Perimeter
- DevOps vs SecOps
- Security with Docker
- HoneyPots and Deception Technology
- Stateless Microservices + Stateless Infrastructure

You can't defend.
You can't prevent.
The only thing you can do is detect and respond

Bruce Schneier



50 terabytes! Snowden leak reveals massive size of F-35 blueprints hack by China

Published time: 19 Jan, 2015 07:56
Edited time: 21 Jan, 2015 08:32

F-35 Joint Strike Fighter Lightning II (AFP Photo / HO / US NAVY/ MCS2D. Keith Simmons) / AFP

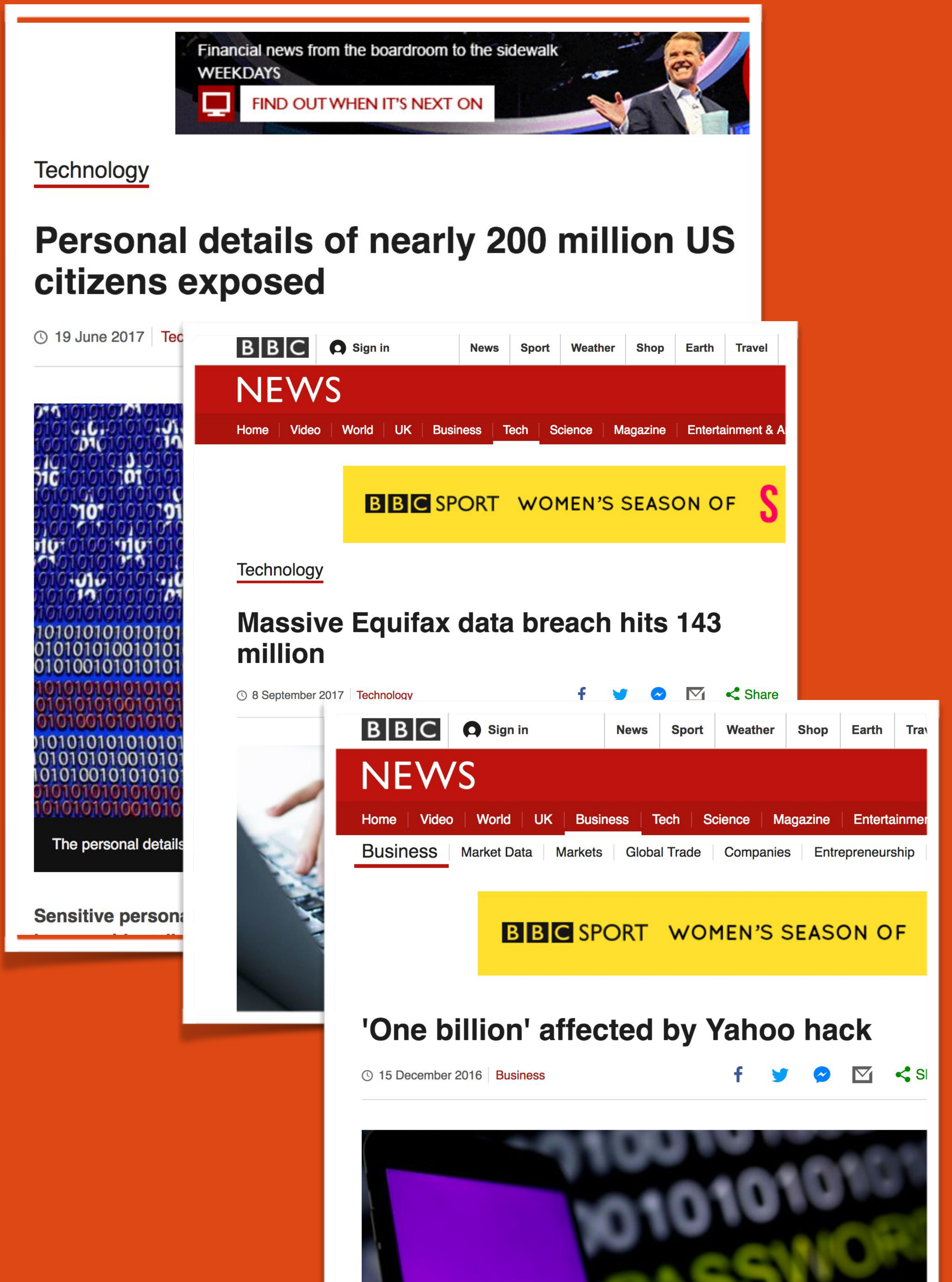
ISIS releases video claiming revenge 'downing' of Russian passenger jet over Sinai

kayra.otaner@secops360.com

Time to Discovery

“Equifax said hackers accessed the information between mid-May and the end of July, when the company discovered the breach.”

“Yahoo said it "believes an unauthorised third party, in August 2013, stole data associated with more than one billion user accounts
The breach "is likely distinct from the incident the company disclosed on September 22, 2016".
However, the three-year-old hack was uncovered as part of continuing investigations by authorities and security experts into the 2014 breach, Yahoo said.“



Technology

Personal details of nearly 200 million US citizens exposed

19 June 2017 | Tec

The personal details

Sensitive person

Technology

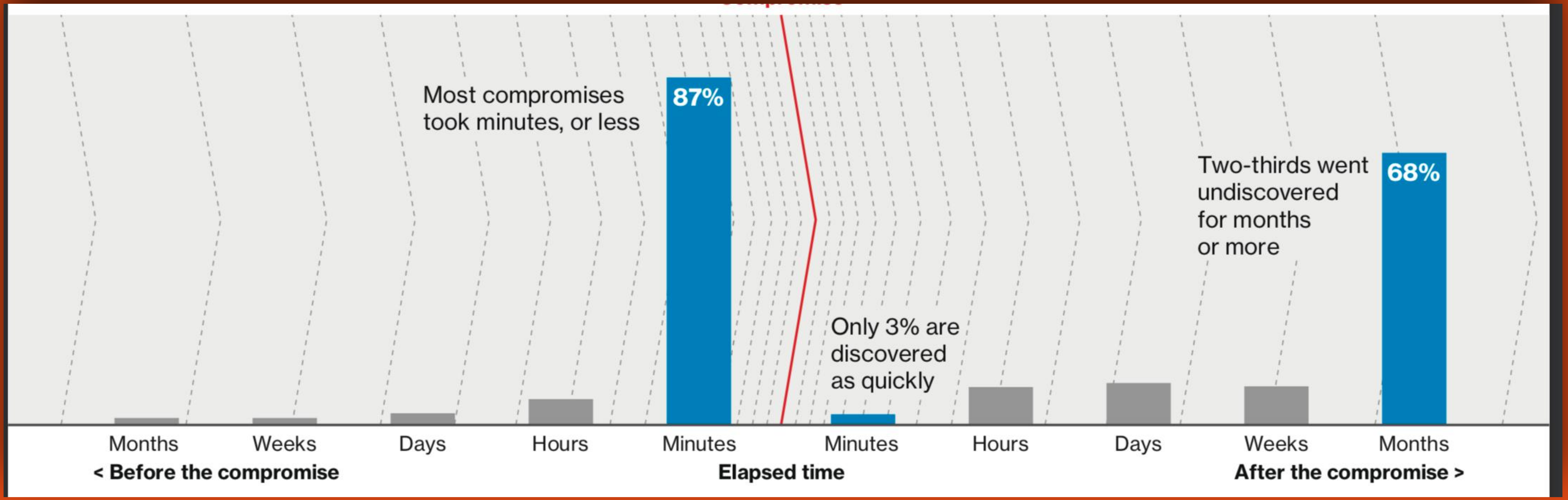
Massive Equifax data breach hits 143 million

8 September 2017 | Technology

'One billion' affected by Yahoo hack

15 December 2016 | Business

2018 Data Breach Investigations Report



Most compromises took minutes, or less

Only 3% are discovered as quickly

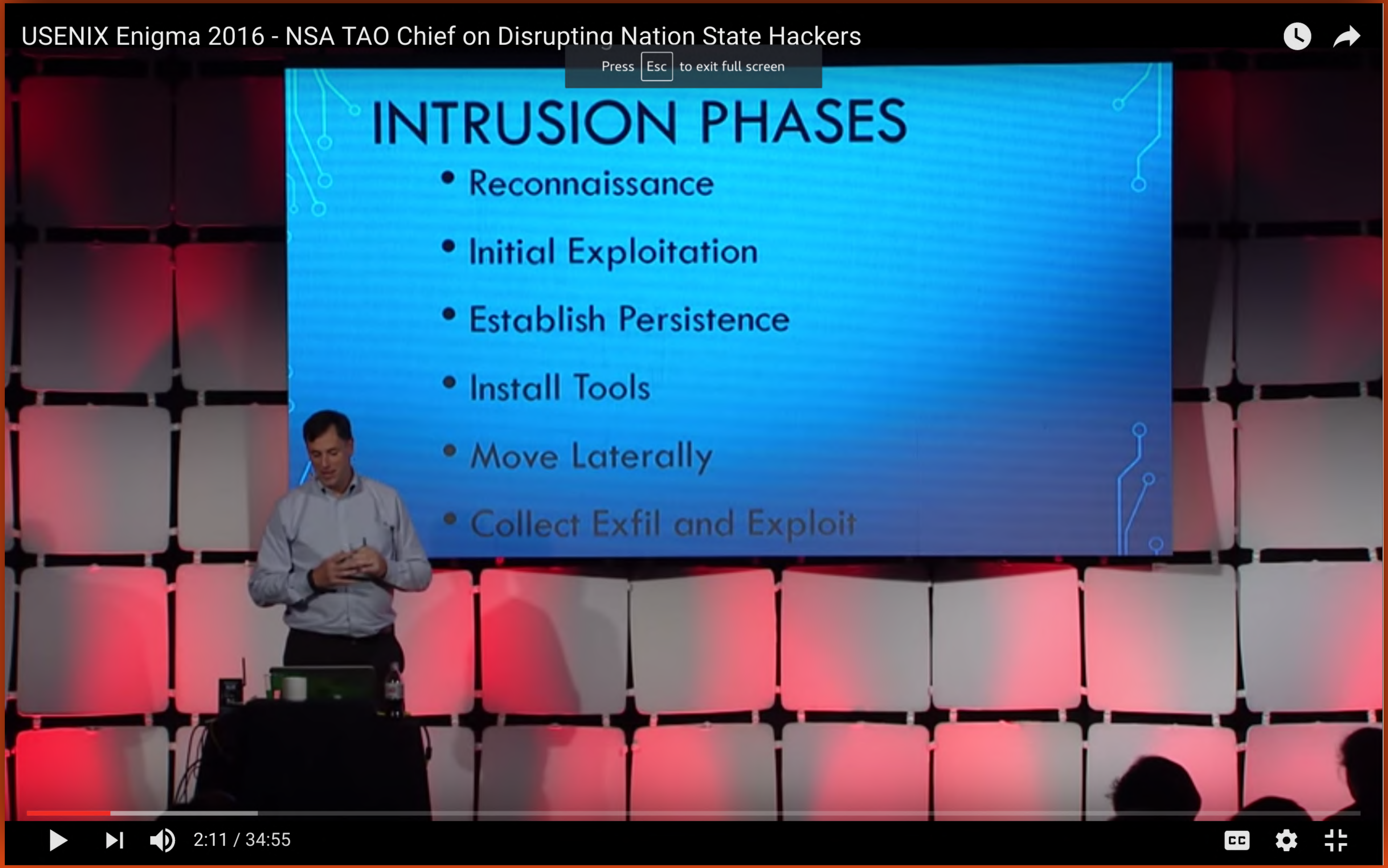
Two-thirds went undiscovered for months or more

53,308 security incidents, 2,216 data breaches, 65 countries, 67 contributors.
Verizon DBIR
https://enterprise.verizon.com/resources/reports/dbir/

kayra.otaner@secops360.com

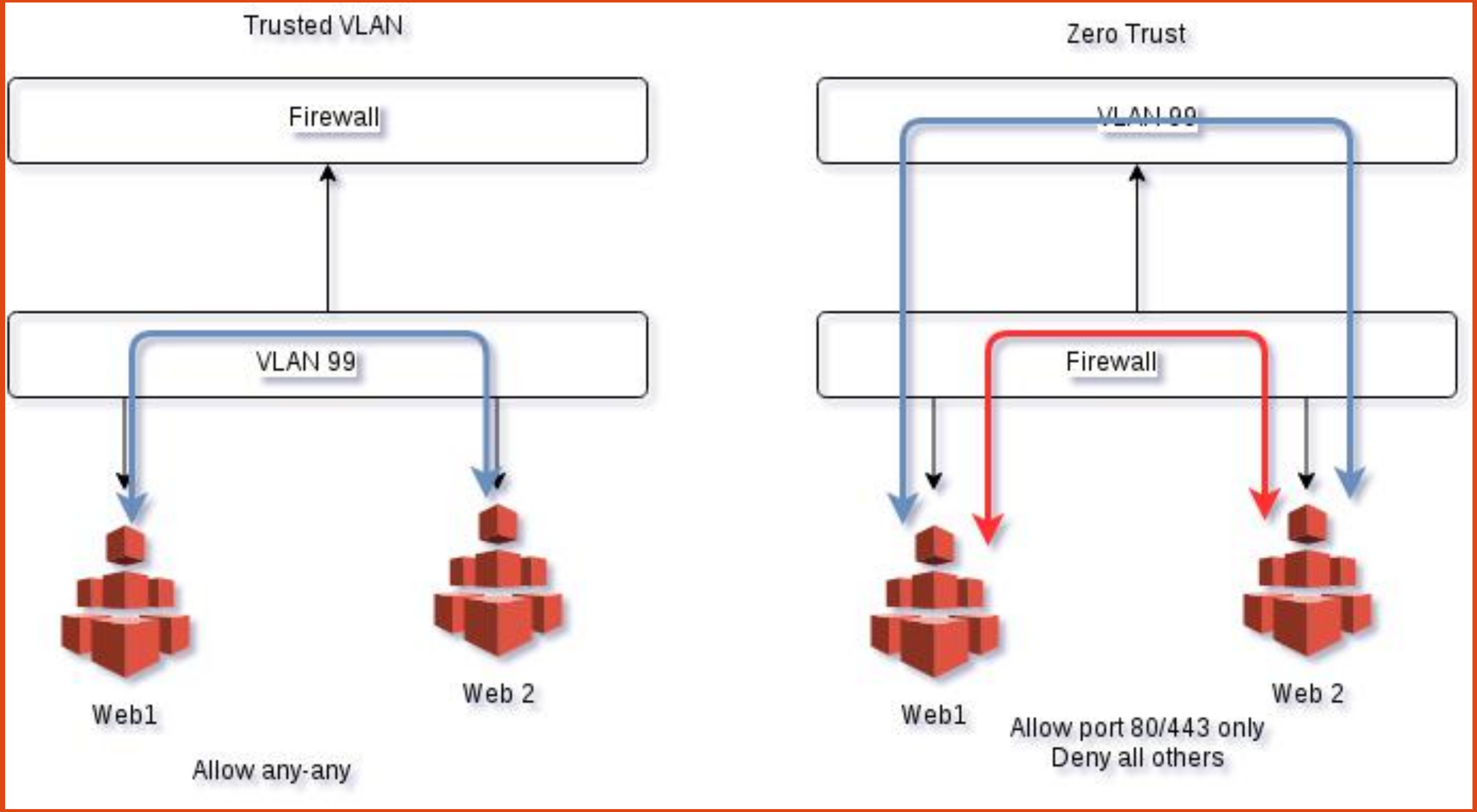
NSA TAO
(Tailored Access Operations)

From their slides :
- We hunt sysadmins
- Know your network, Understand your network (22:00)
- Consider you’re already penetrated 29”

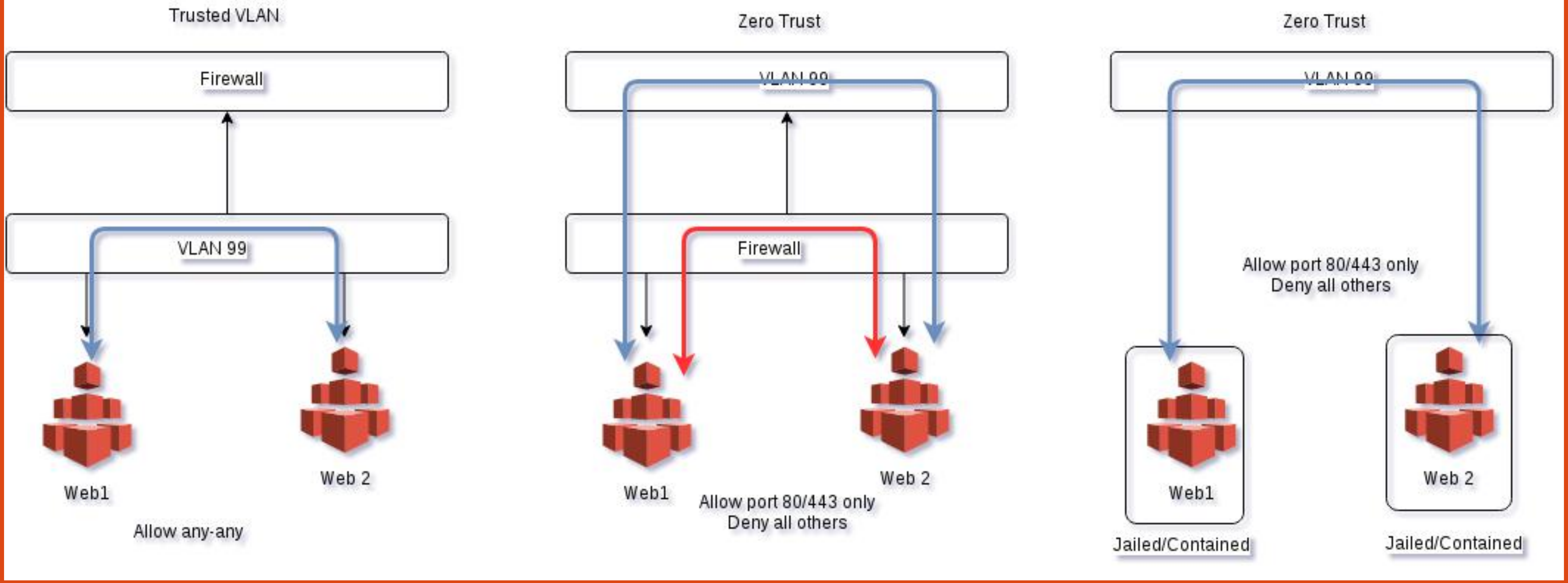

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

INTRUSION PHASES
- Reconnaissance
- Initial Exploitation
- Establish Persistence
- Install Tools
- Move Laterally
- Collect Exfil and Exploit

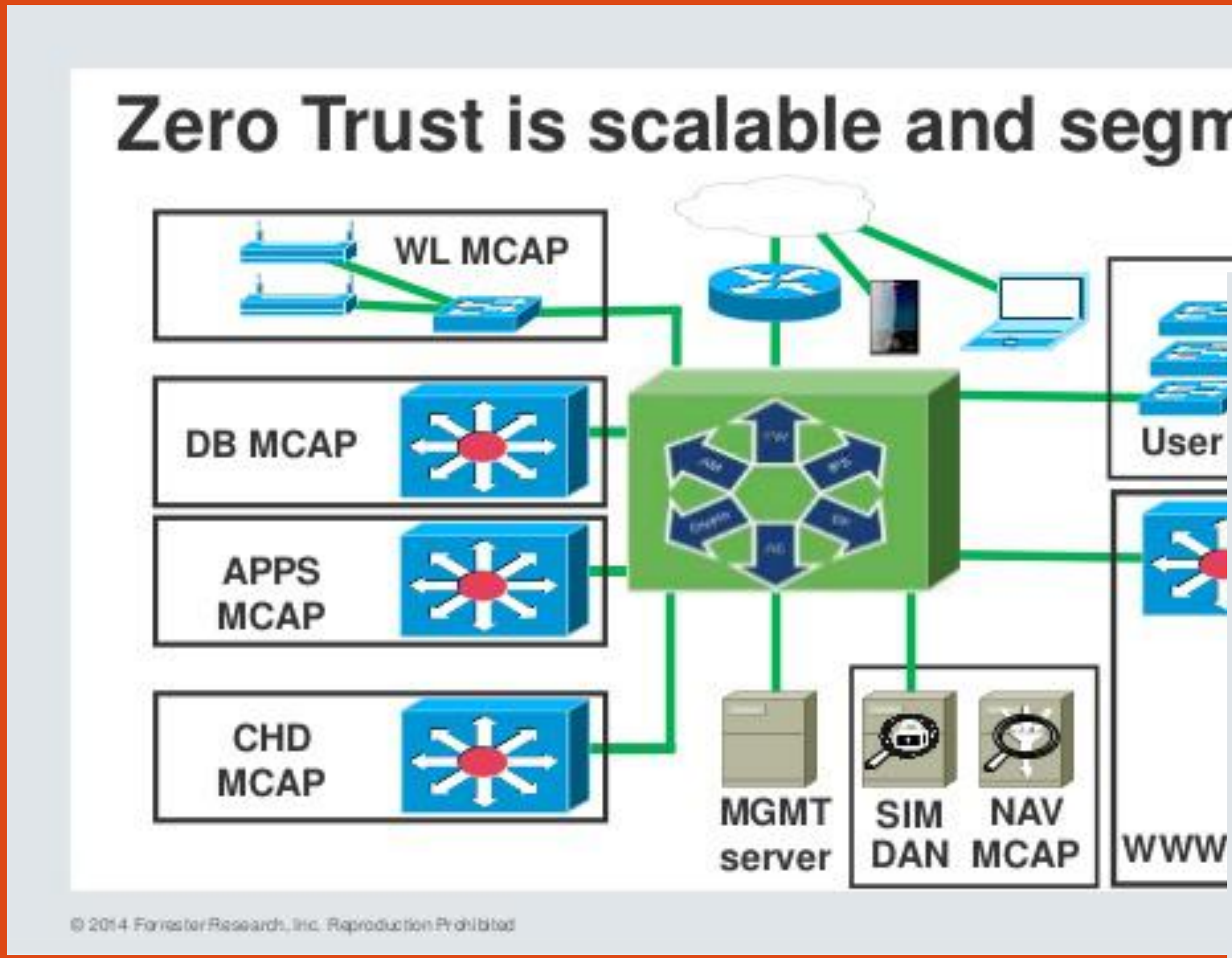
Focus on Lateral Movement, remove 'Trusted VLAN'



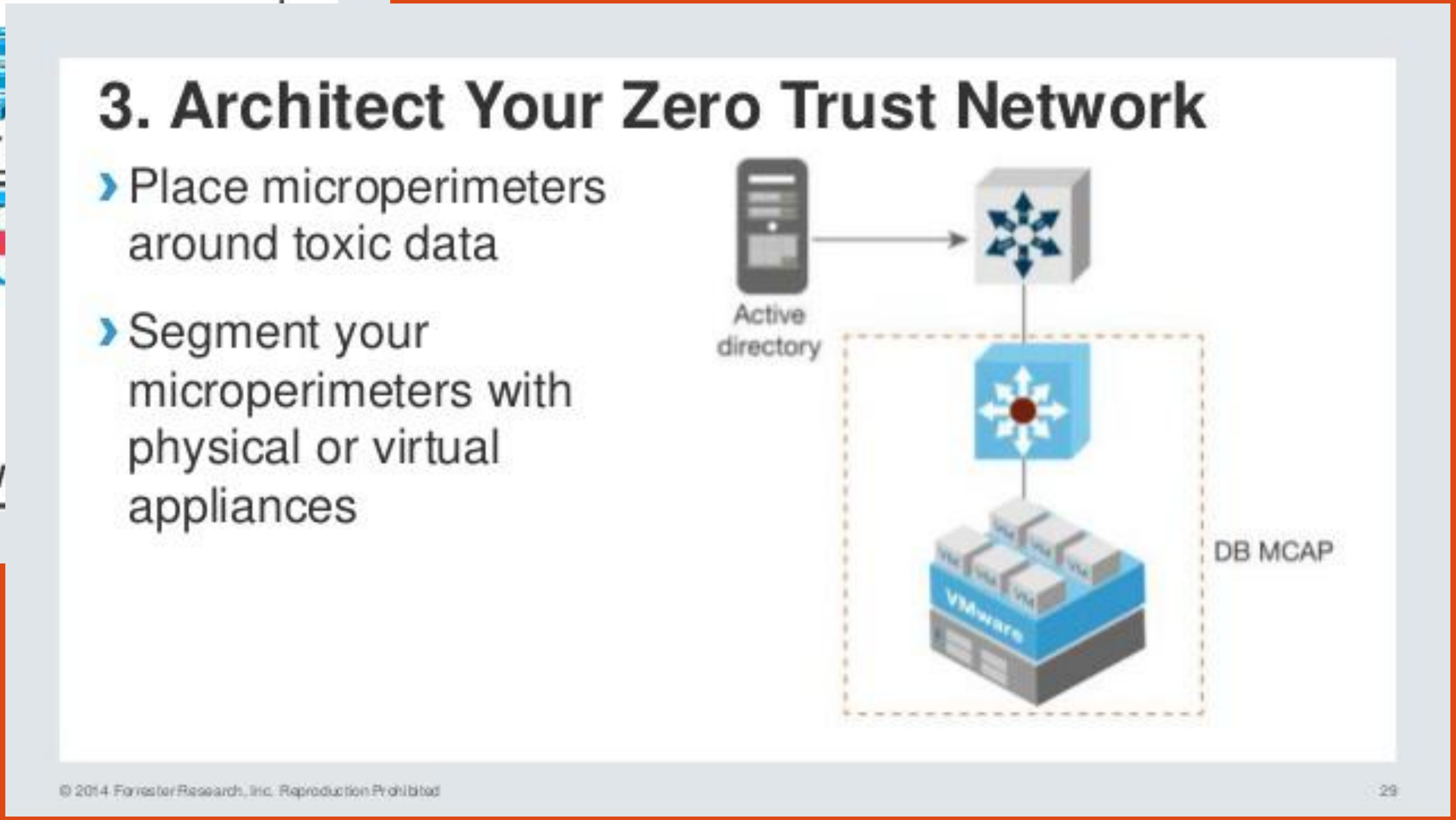
What if, if we can bring firewall & IDS even closer to the App, and create micro perimeter?



kayra.otaner@secops360.com



Zero Trust is scalable and segmented



3. Architect Your Zero Trust Network

- Place microperimeters around toxic data
- Segment your microperimeters with physical or virtual appliances

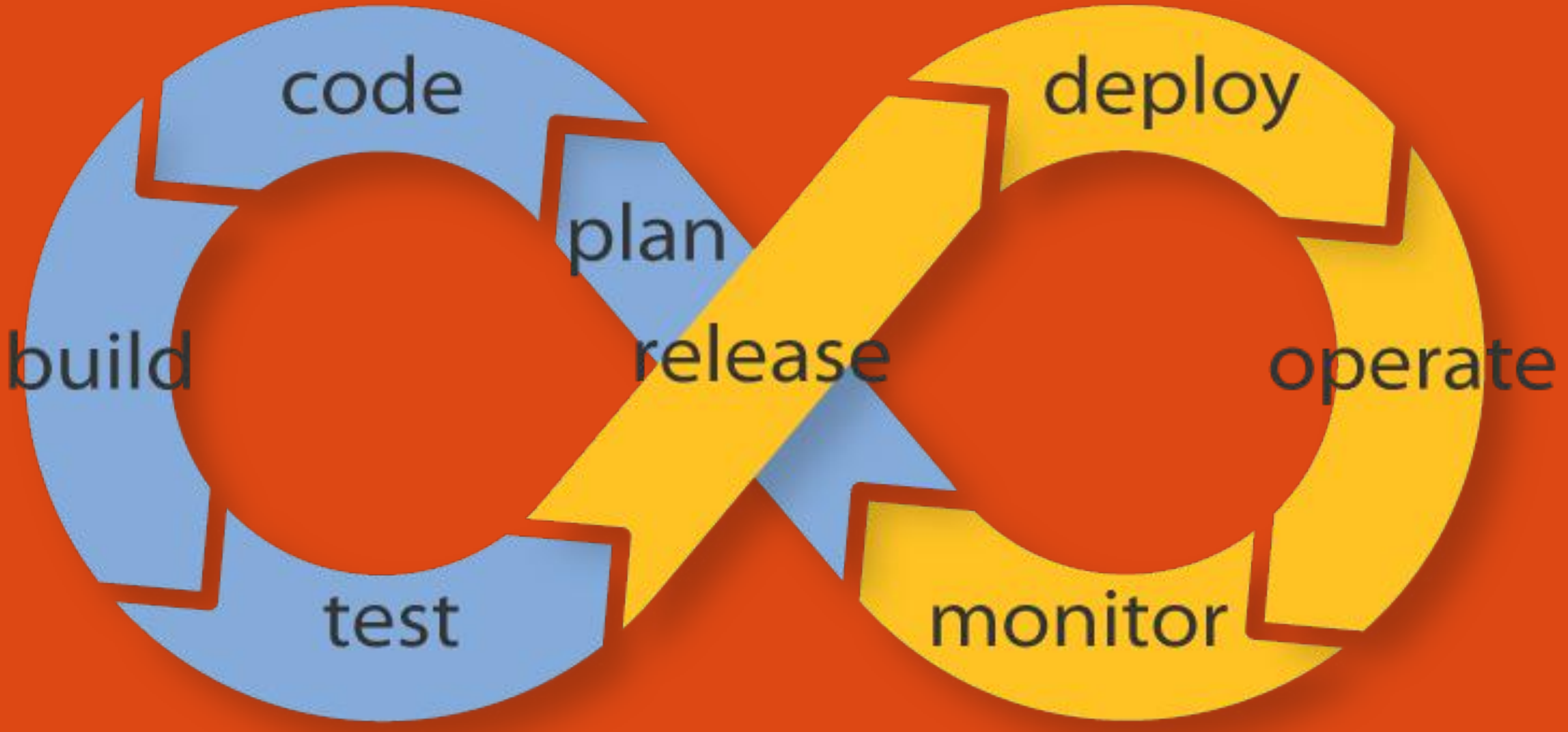
https://www.slideshare.net/AlgoSec/5-steps-to-a-zero-trust-network-from-theory-to-practice

kayra.otaner@secops360.com

What is DevOps?
What is SecOps?

DevOps

Developers love it because it makes their life easier.

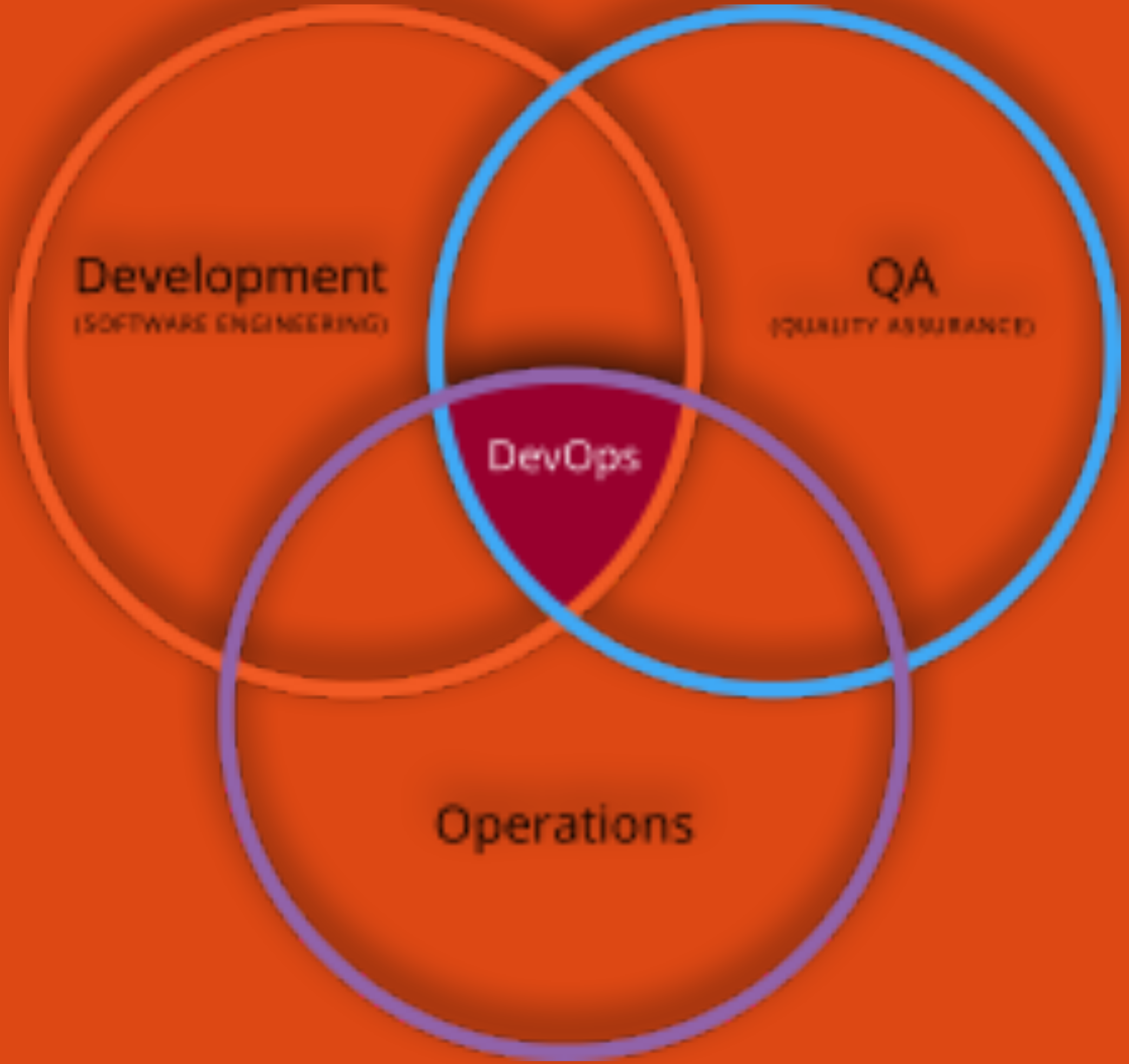


Endless Possibilities: DevOps can create an infinite loop of release and feedback for all your code and deployment targets.

DevOps is

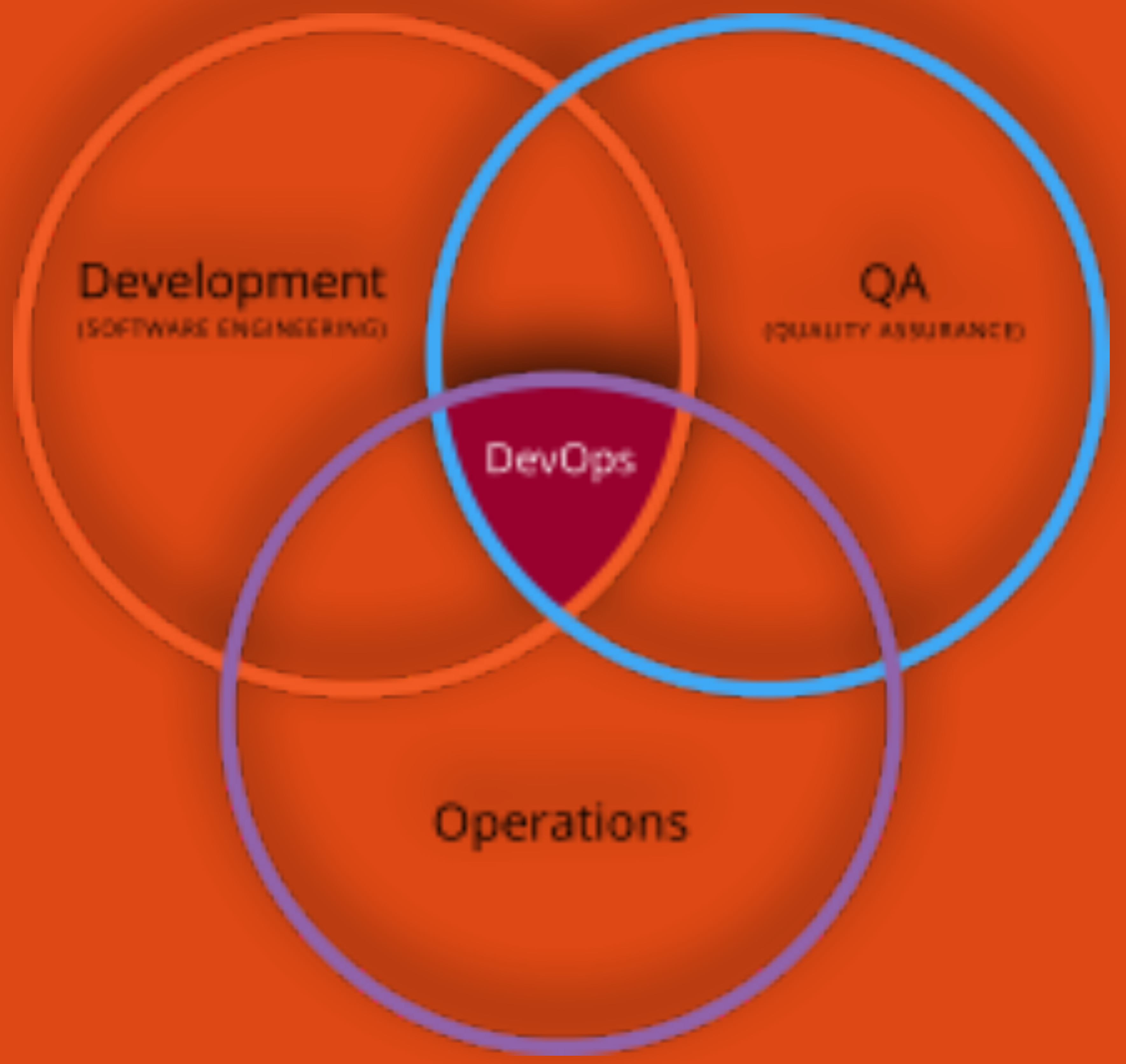
(from System Administrator perspective)

Building systems that manages other systems so that I don't need to manage 10000 systems.


Development
(SOFTWARE ENGINEERING)
QA
(QUALITY ASSURANCE)
DevOps
Operations

Conventional Environments

Dev: Developer owned environments
Stage: Developer owned environments
QA : QA & Test teams own and use
UAT : User Acceptance Test, for clients use
Preprod: Operations Teams
Prod: Operations Teams



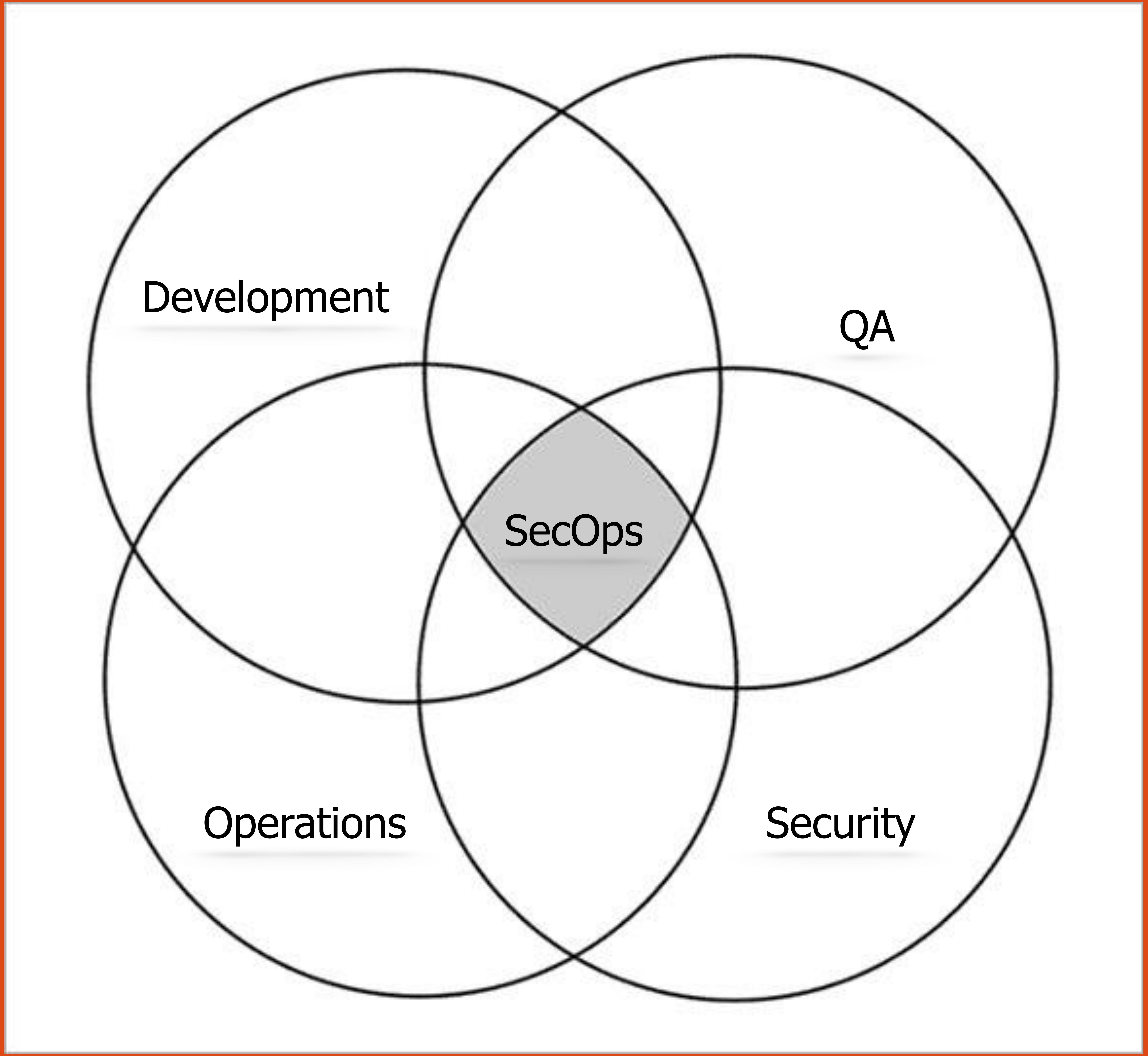
kayra.otaner@secops360.com

SecOps is :

Building systems that SECURELY builds other systems and keeps them secure so that we don't need to do it using man power.

SecOps

Dev: Developer owned environments
Stage: Developer owned environments
QA : QA & Test teams own and use
UAT : For clients use
Preprod: Operations Teams
Prod: Operations Teams
Honeypots: Security Teams



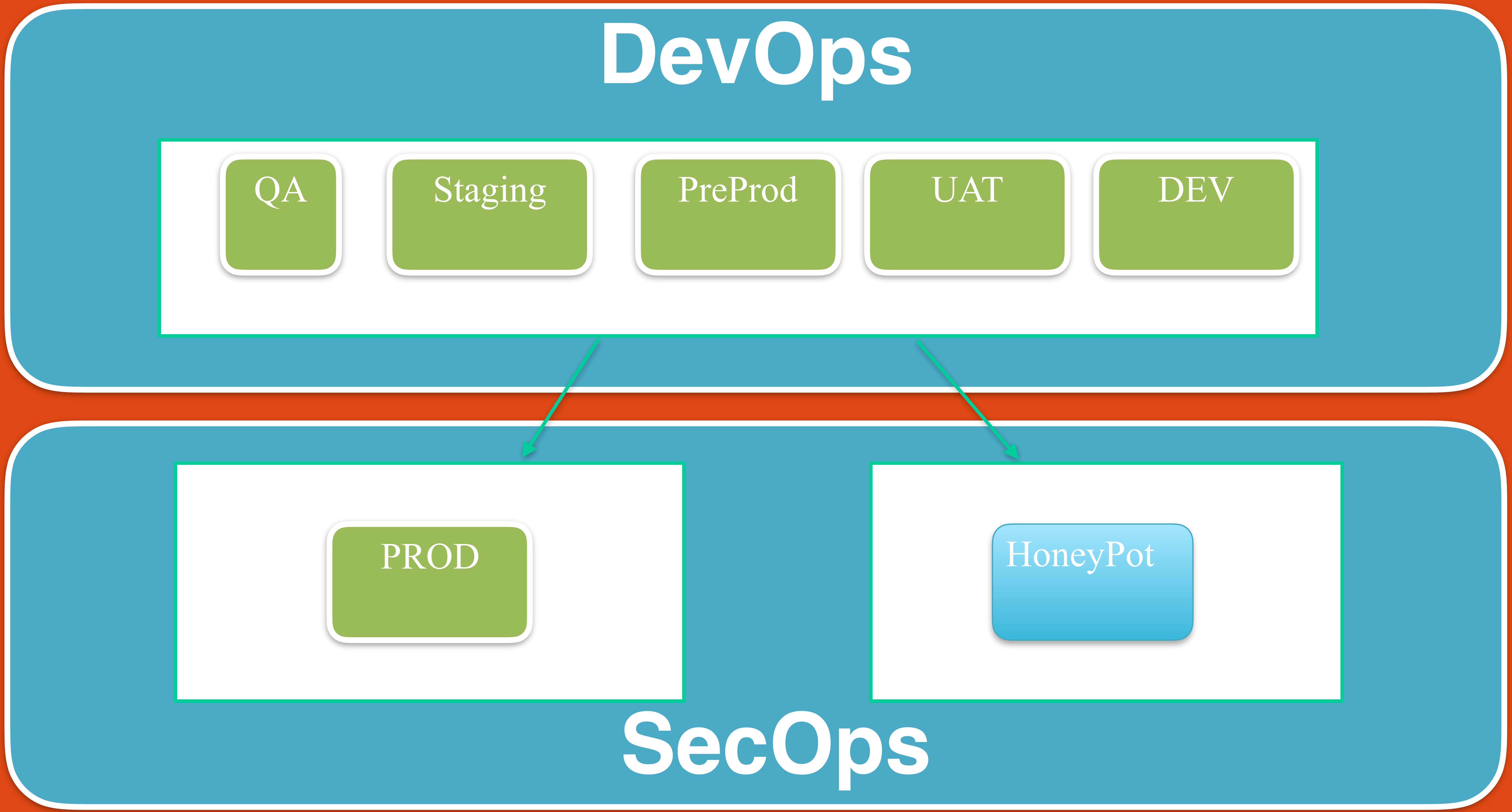
kayra.otaner@secops360.com

HoneyPot Environments

Conventional Environments
Stage
Dev
Prod
PreProd
QA

and now

HoneyPots



kayra.otaner@secops360.com

Change in Skill Set

- By bringing Firewall/IDS/Switch/Hypervisor features closer to the app, we're effectively eliminating needs of having dedicated people to operate them.
- We still need processes to operate functionality required to have secure and stable systems.

APT vs APD

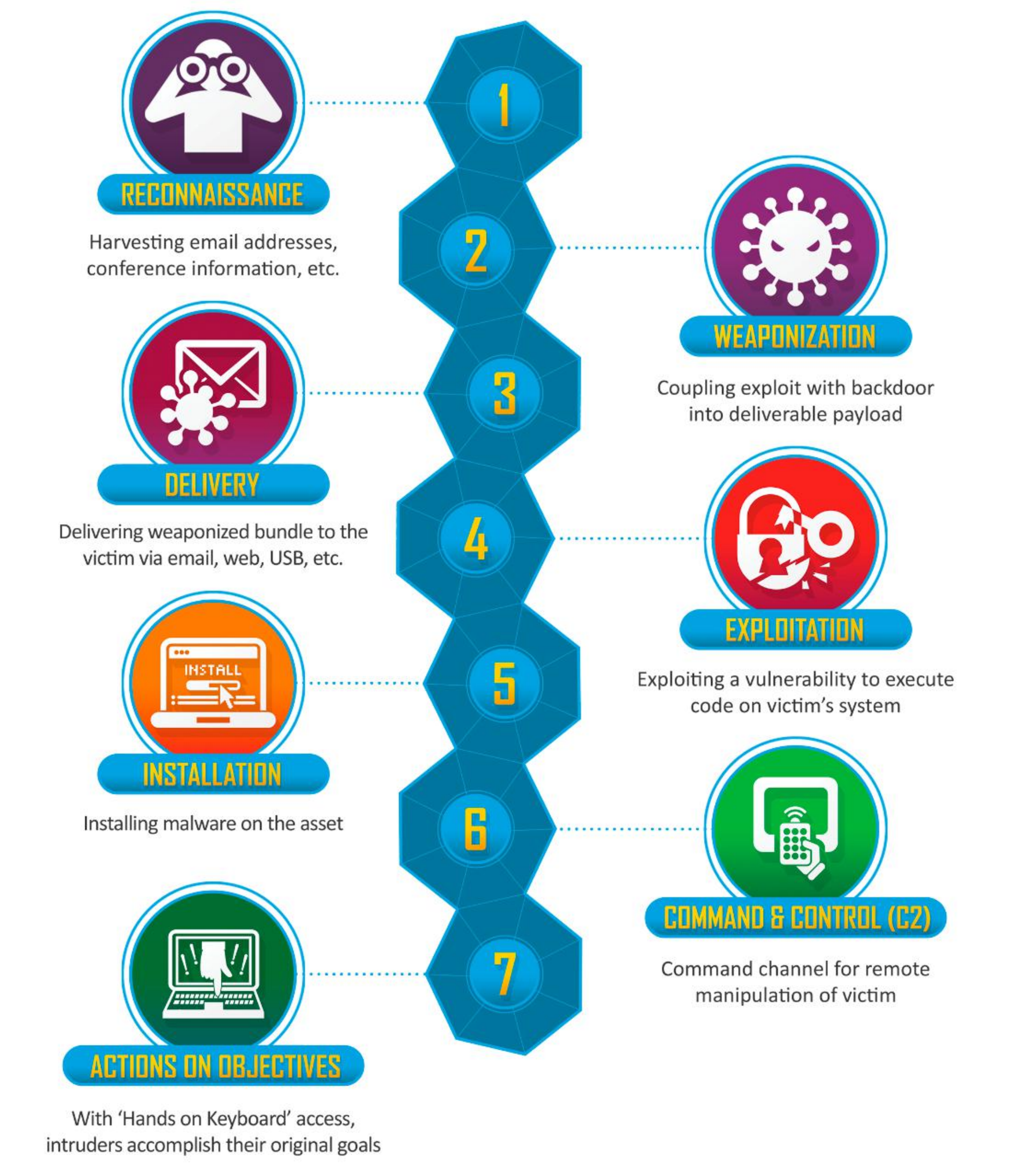
Advanced Persistent Threat
vs
Advanced Persistent Defense

kayra.otaner@secops360.com

Cyber Kill Chain

Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

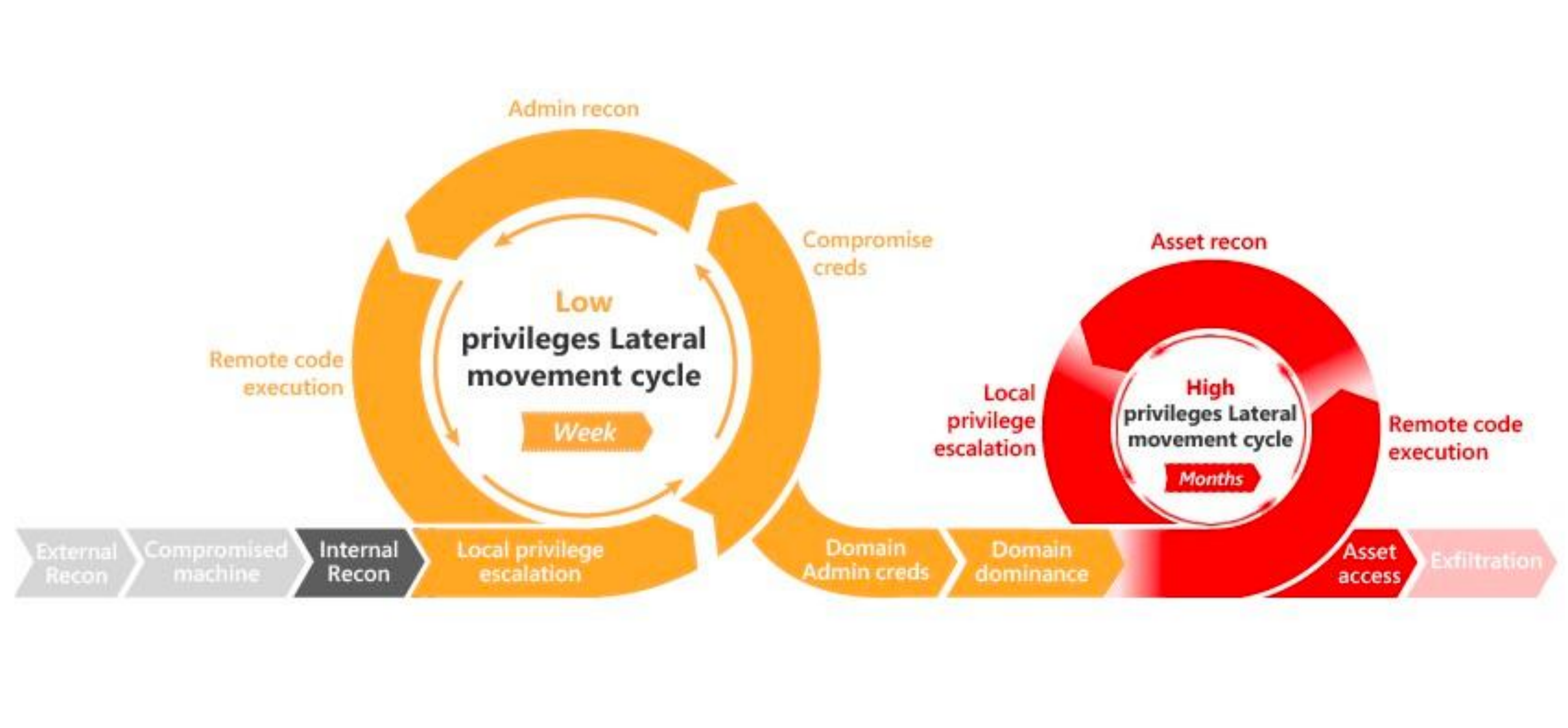
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

kayra.otaner@secops360.com

Key Steps

Establish Persistence
Lateral Movements

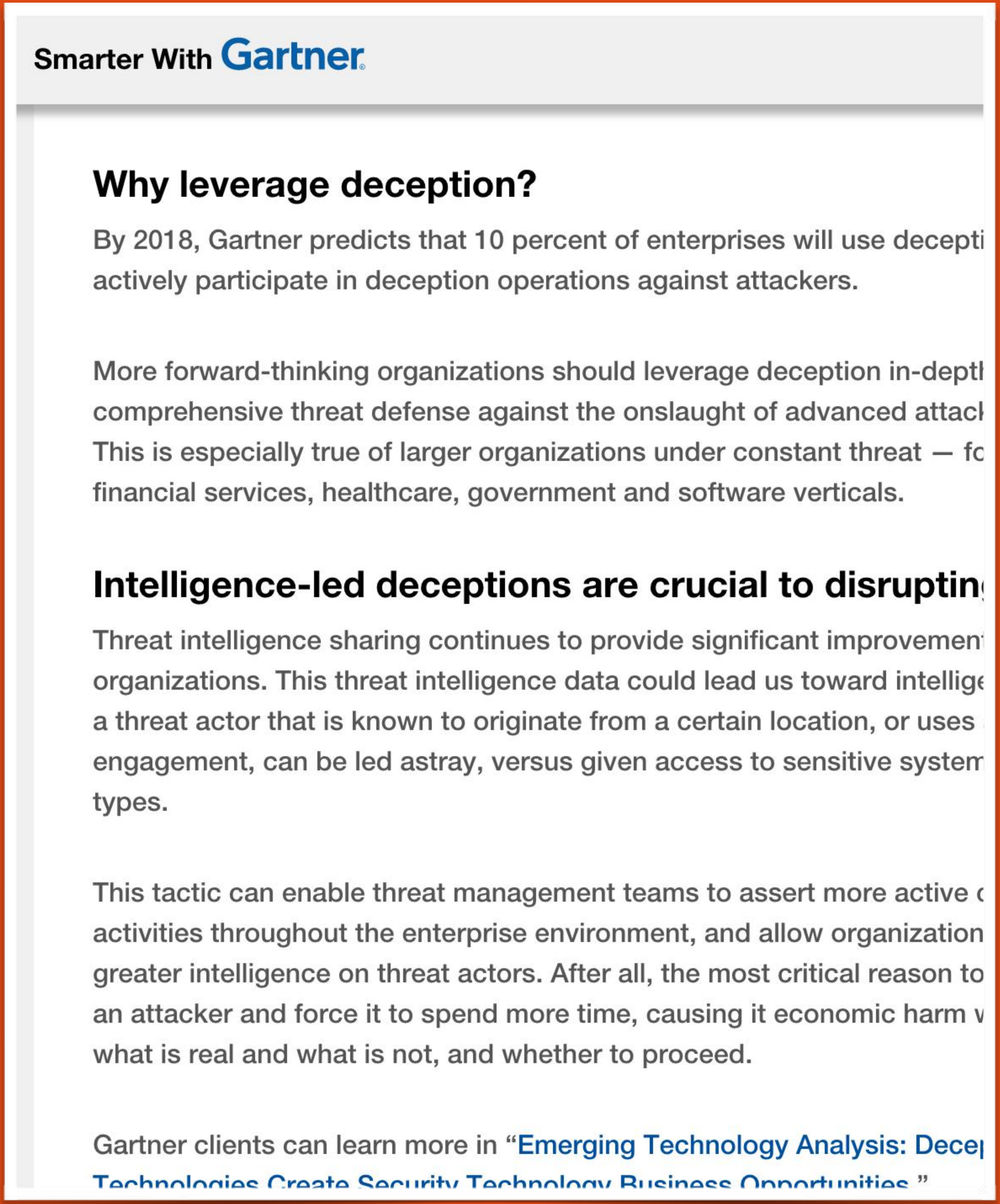


HoneyPots

Gartner Reports

Gartner analyst earlier noted that, "by 2018 ... 10 percent of enterprises will use deception tools and tactics, and actively participate in deception operations against attackers.” Gartner also noted deception technology as a "far underutilized technology that can provide serious advantages over attacker

http://www.gartner.com/newsroom/id/3347717



Smarter With Gartner

Why leverage deception?

By 2018, Gartner predicts that 10 percent of enterprises will use decepti actively participate in deception operations against attackers.

More forward-thinking organizations should leverage deception in-deptl comprehensive threat defense against the onslaught of advanced attacl This is especially true of larger organizations under constant threat — fc financial services, healthcare, government and software verticals.

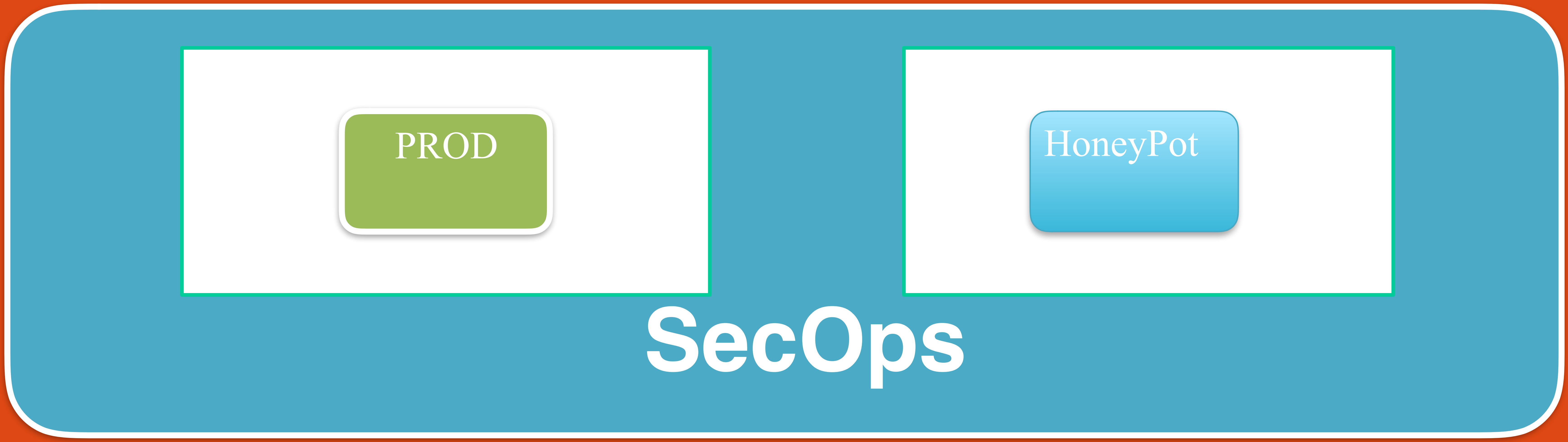
Intelligence-led deceptions are crucial to disruptin

Threat intelligence sharing continues to provide significant improvemen organizations. This threat intelligence data could lead us toward intellige a threat actor that is known to originate from a certain location, or uses engagement, can be led astray, versus given access to sensitive system types.

This tactic can enable threat management teams to assert more active activities throughout the enterprise environment, and allow organization greater intelligence on threat actors. After all, the most critical reason to an attacker and force it to spend more time, causing it economic harm v what is real and what is not, and whether to proceed.

Gartner clients can learn more in “Emerging Technology Analysis: Decep Technologies Create Security Technology Business Opportunities.”

HoneyPot Ideas?



Once you have the MCAP setup properly, you can either clone your app completely and create a separate dedicated 'honeypot environment' or can create a 'sister environment' that mimics what you might have in your platform

kayra.otaner@secops360.com

HoneyPot types

- Low interaction
  - Generic protocol emulators, close to 50 protocol emulators are available on the net
- High Interaction
  - Generally specific to your environment, looks and acts like real applications

Low Interaction HoneyPots

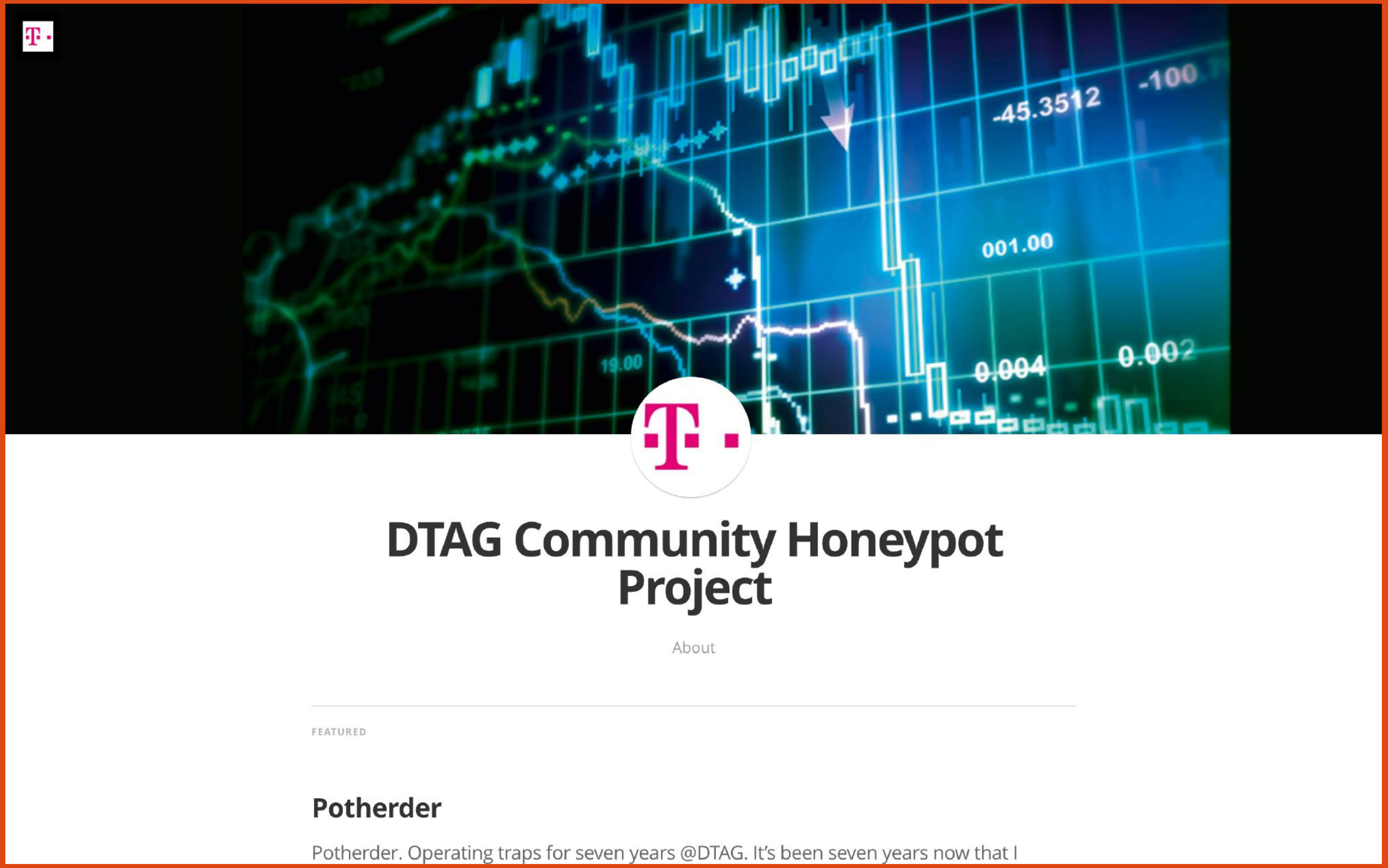
Deutsche Telekom sponsors an Open Source low interaction honeypot distro

http://dtag-dev-sec.github.io/

Latest version is 18.11

It is a collection of dockerized images of various publicly available honeypots :

- conpot,
- cowrie,
- dionaea,
- elasticpot,
- emobility,
- glastopf,
- honeytrap,
- mailoney,
- rdpy and
- vnclowpot



DTAG Community Honeypot Project

About

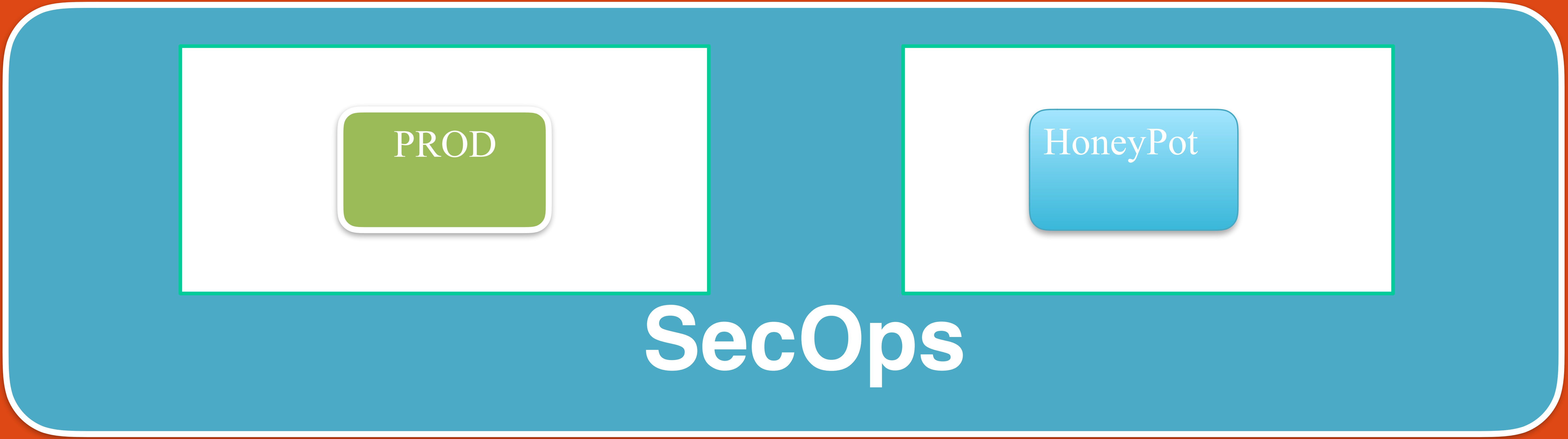
FEATURED

Potherder

Potherder. Operating traps for seven years @DTAG. It's been seven years now that I

kayra.otaner@secops360.com

High Interaction HoneyPot Ideas?



1. Ansible Tower became Open Source: AWX
2. MySQL with sample data from your production systems
3. SSH dockerized (—net=host) with lots of usernames from your old co-workers ;-)
4. Samba/NFS shares with files such as '2019SalaryAndPromtions.xls'
5. Syslog servers with real looking events coming through
6. Wordpress, Drupal, Joomla or PhpMyAdmin application with a database behind it.

kayra.otaner@secops360.com

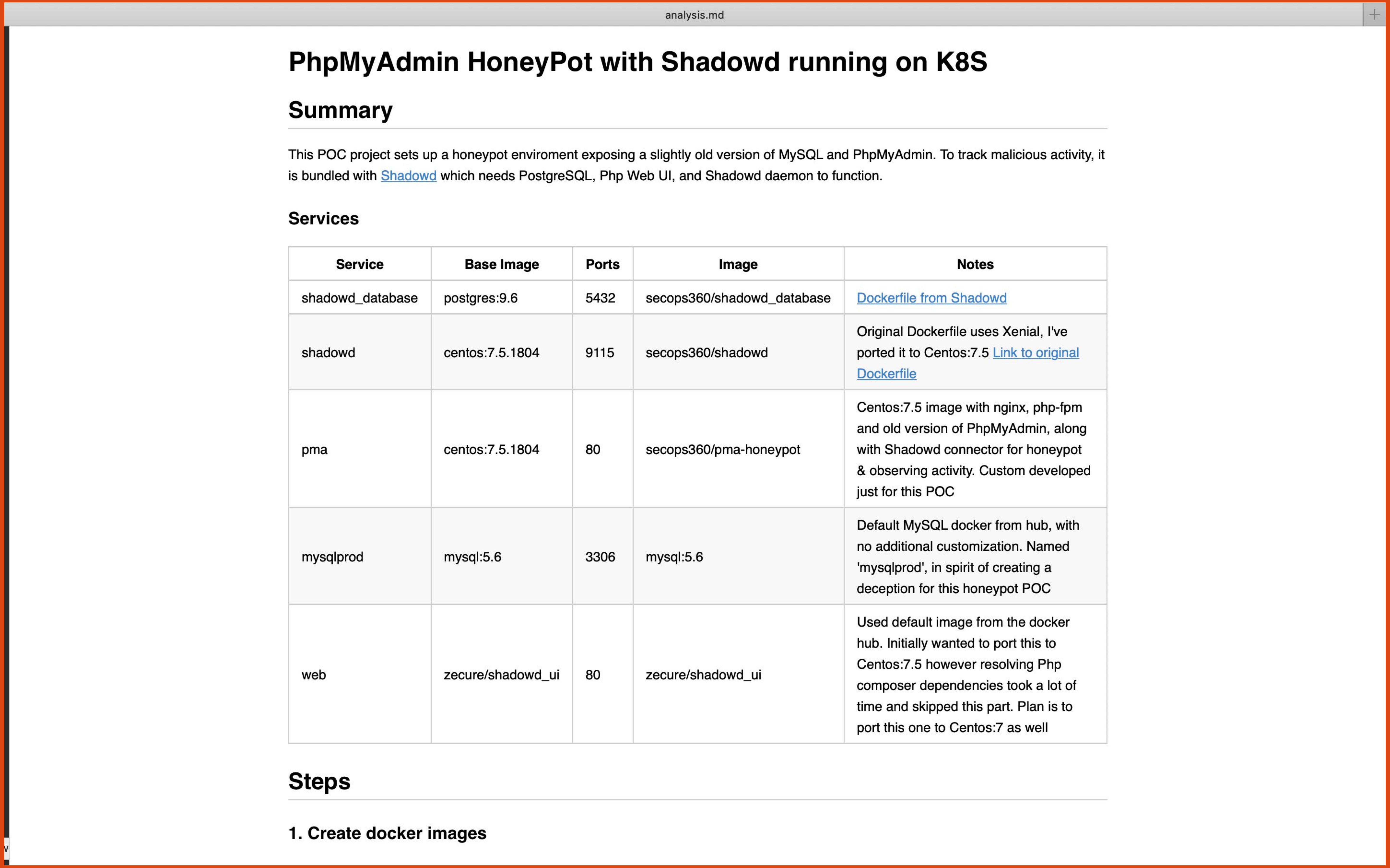
POC: PhpMyAdmin HoneyPot with Shadowd running on K8S

Blue Print for High Interaction Honeypot

- Nginx
- Php-fpm
- MySQL
- PhpMyAdmin
- Shadowd

kayra.otaner@secops360.com

POC: PhpMyAdmin HoneyPot with Shadowd running on K8S



PhpMyAdmin HoneyPot with Shadowd running on K8S

Summary

This POC project sets up a honeypot enviroment exposing a slightly old version of MySQL and PhpMyAdmin. To track malicious activity, it is bundled with Shadowd which needs PostgreSQL, Php Web UI, and Shadowd daemon to function.

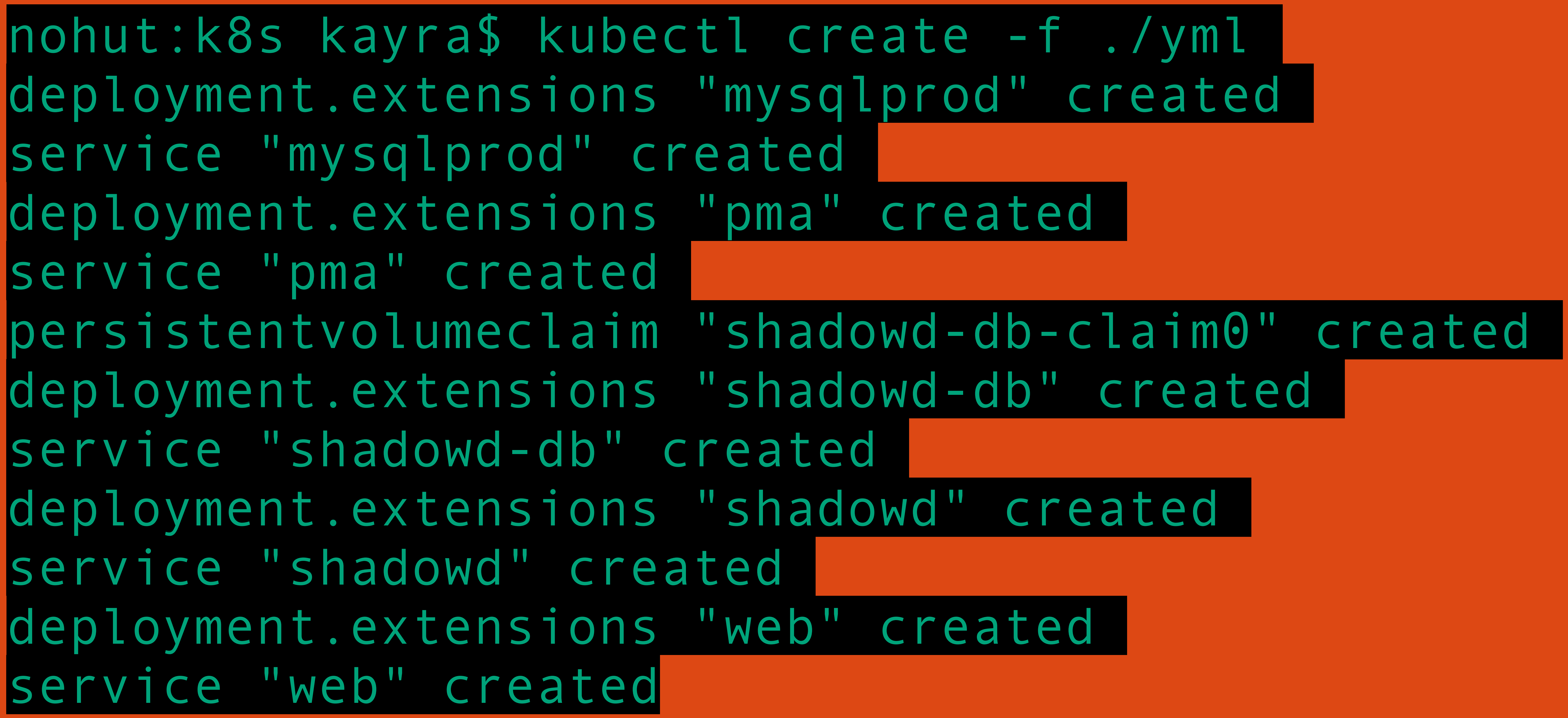
Services

Service	Base Image	Ports	Image	Notes
shadowd_database	postgres:9.6	5432	secops360/shadowd_database	Dockerfile from Shadowd
shadowd	centos:7.5.1804	9115	secops360/shadowd	Original Dockerfile uses Xenial, I've ported it to Centos:7.5 Link to original Dockerfile
pma	centos:7.5.1804	80	secops360/pma-honeypot	Centos:7.5 image with nginx, php-fpm and old version of PhpMyAdmin, along with Shadowd connector for honeypot & observing activity. Custom developed just for this POC
mysqlprod	mysql:5.6	3306	mysql:5.6	Default MySQL docker from hub, with no additional customization. Named 'mysqlprod', in spirit of creating a deception for this honeypot POC
web	zecure/shadowd_ui	80	zecure/shadowd_ui	Used default image from the docker hub. Initially wanted to port this to Centos:7.5 however resolving Php composer dependencies took a lot of time and skipped this part. Plan is to port this one to Centos:7 as well

Steps

1. Create docker images

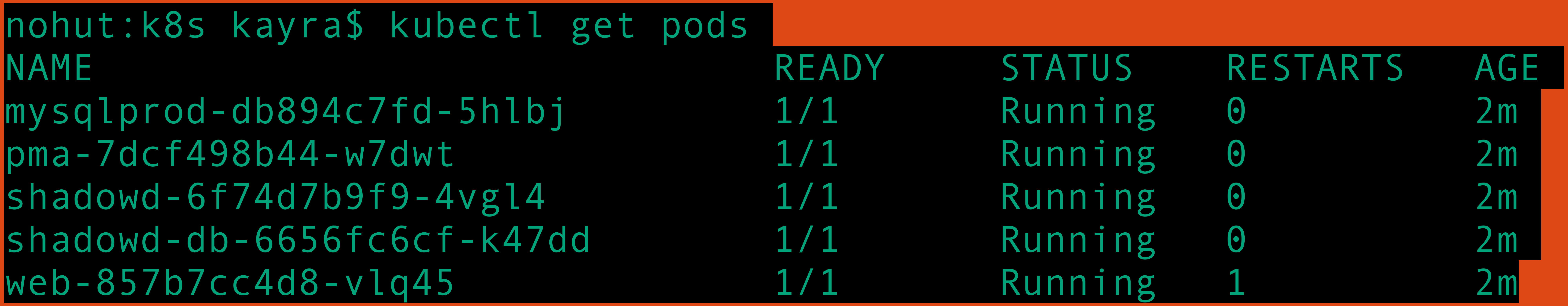
POC: PhpMyAdmin HoneyPot with Shadowd running on K8S



```
nohut:k8s kayra$ kubectl create -f ./yml
deployment.extensions "mysqlprod" created
service "mysqlprod" created
deployment.extensions "pma" created
service "pma" created
persistentvolumeclaim "shadowd-db-claim0" created
deployment.extensions "shadowd-db" created
service "shadowd-db" created
deployment.extensions "shadowd" created
service "shadowd" created
deployment.extensions "web" created
service "web" created
```

kayra.otaner@secops360.com

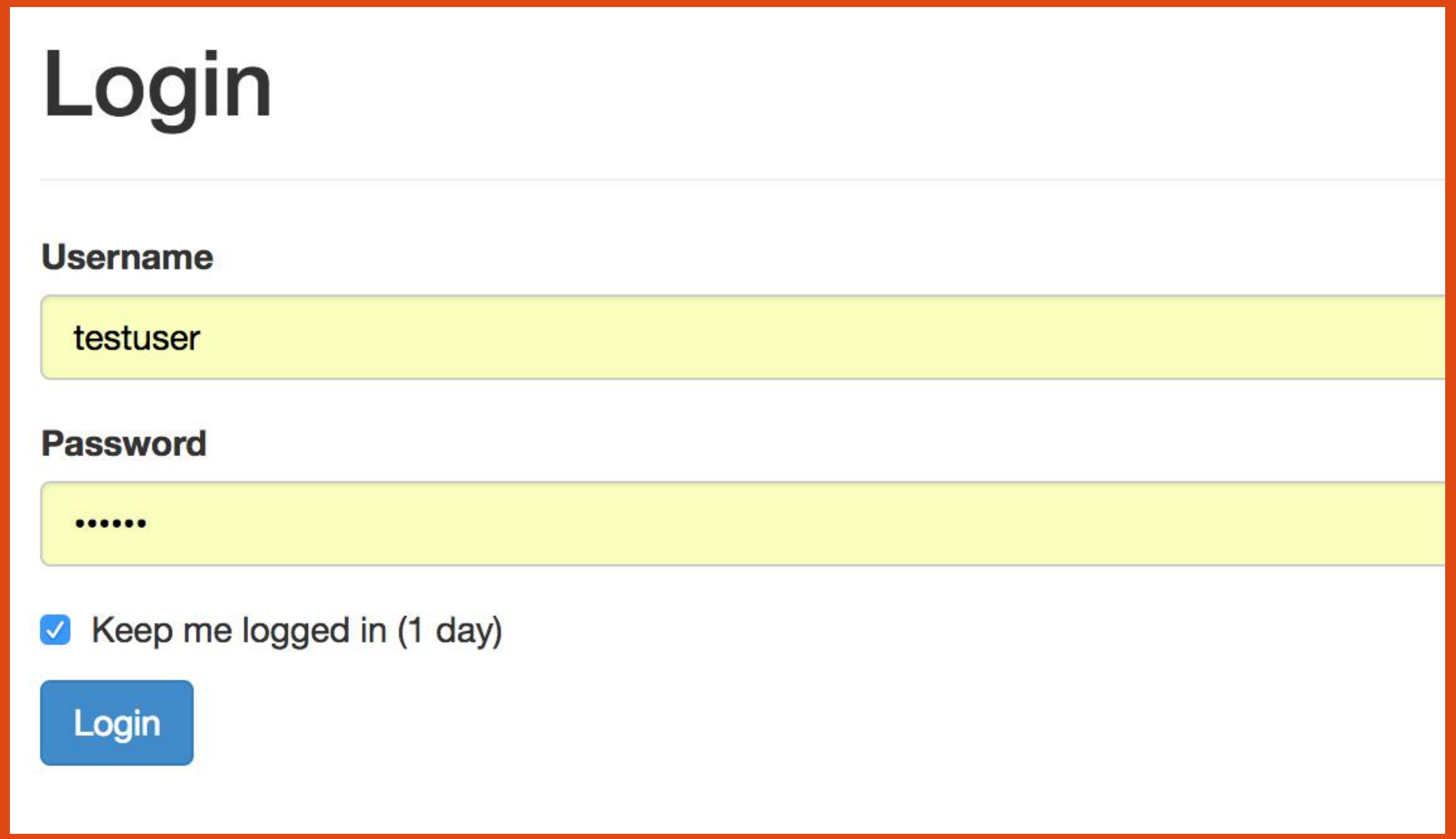
POC: PhpMyAdmin HoneyPot with Shadowd running on K8S



```
nohut:k8s kayra$ kubectl get pods
NAME                              READY     STATUS    RESTARTS   AGE
mysqlprod-db894c7fd-5hlbj         1/1       Running   0          2m
pma-7dcf498b44-w7dwt              1/1       Running   0          2m
shadowd-6f74d7b9f9-4vgl4          1/1       Running   0          2m
shadowd-db-6656fc6cf-k47dd        1/1       Running   0          2m
web-857b7cc4d8-vlq45              1/1       Running   1          2m
```

kayra.otaner@secops360.com

POC: PhpMyAdmin HoneyPot with Shadowd running on K8S

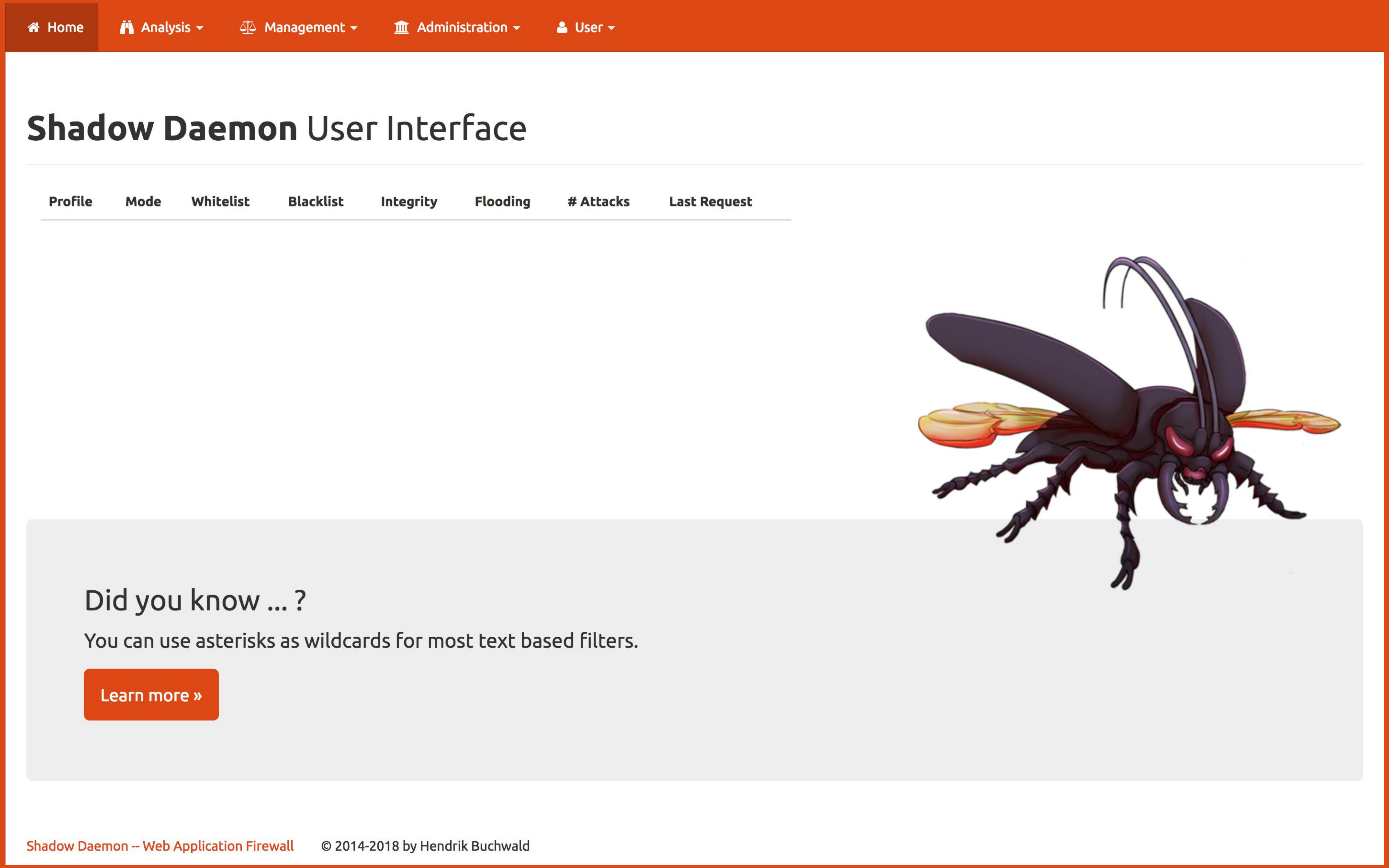


Login

Username: testuser

Password: ••••••

☑ Keep me logged in (1 day)



Shadow Daemon User Interface

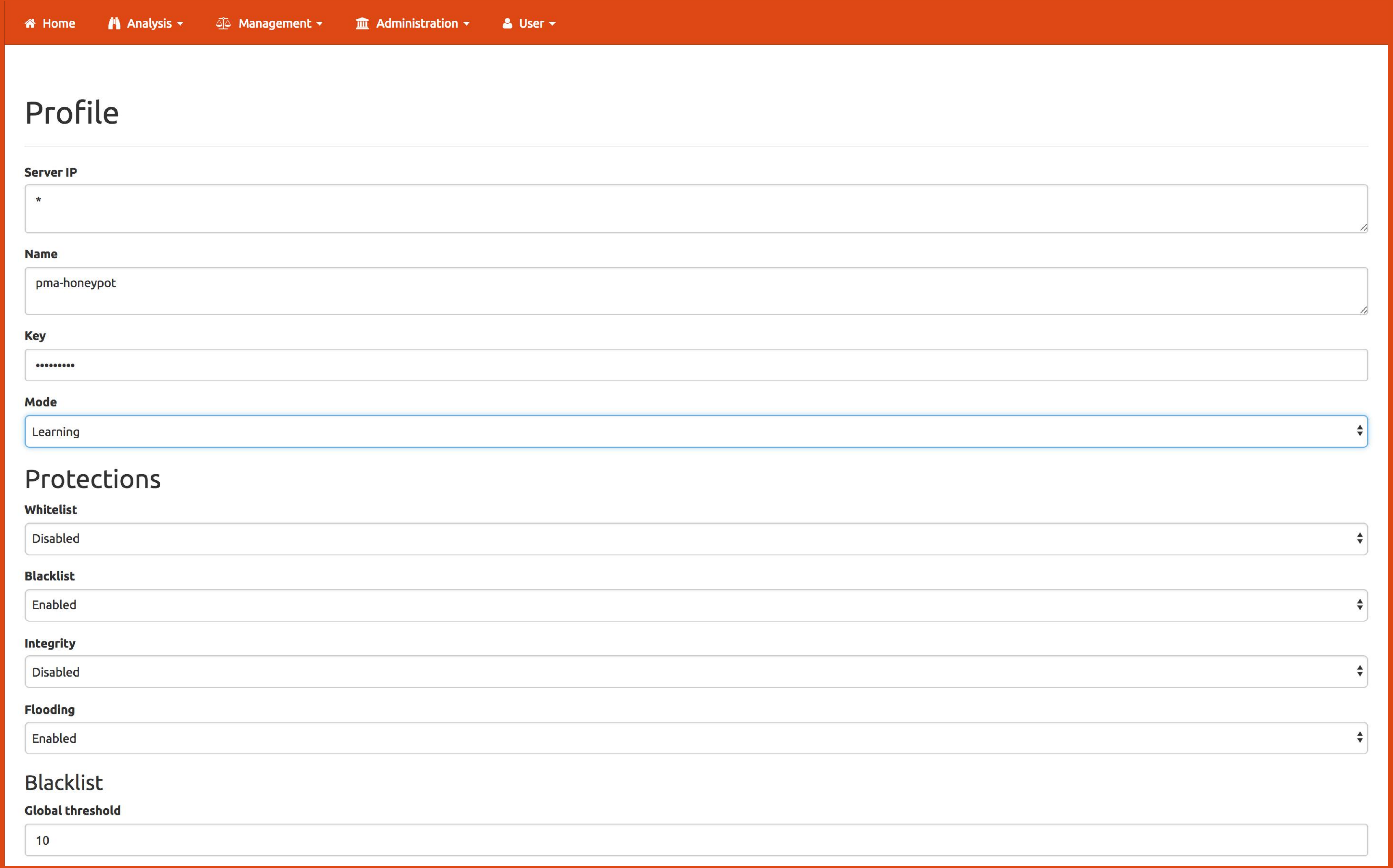
Profile	Mode	Whitelist	Blacklist	Integrity	Flooding	# Attacks	Last Request

Did you know ... ?

You can use asterisks as wildcards for most text based filters.

Shadow Daemon -- Web Application Firewall © 2014-2018 by Hendrik Buchwald

POC: PhpMyAdmin HoneyPot with Shadowd running on K8S



Profile

Server IP

*

Name

pma-honeypot

Key

•••••••••

Mode

Learning

Protections

Whitelist

Disabled

Blacklist

Enabled

Integrity

Disabled

Flooding

Enabled

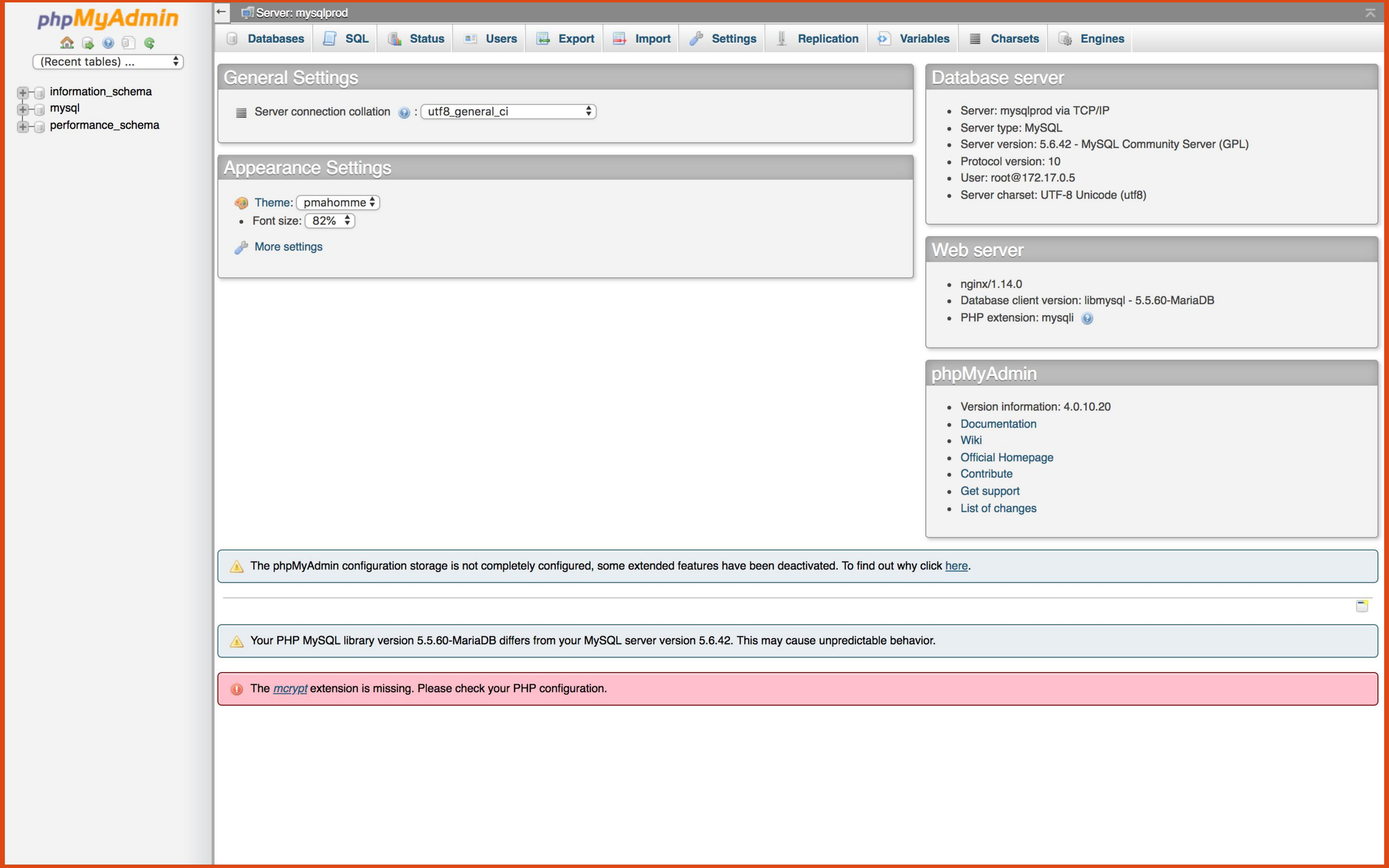
Blacklist

Global threshold

10

kayra.otaner@secops360.com

POC: PhpMyAdmin HoneyPot with Shadowd running on K8S



General Settings

- Server connection collation : utf8_general_ci

Appearance Settings

- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: mysqlprod via TCP/IP
- Server type: MySQL
- Server version: 5.6.42 - MySQL Community Server (GPL)
- Protocol version: 10
- User: root@172.17.0.5
- Server charset: UTF-8 Unicode (utf8)

Web server

- nginx/1.14.0
- Database client version: libmysql - 5.5.60-MariaDB
- PHP extension: mysqli

phpMyAdmin

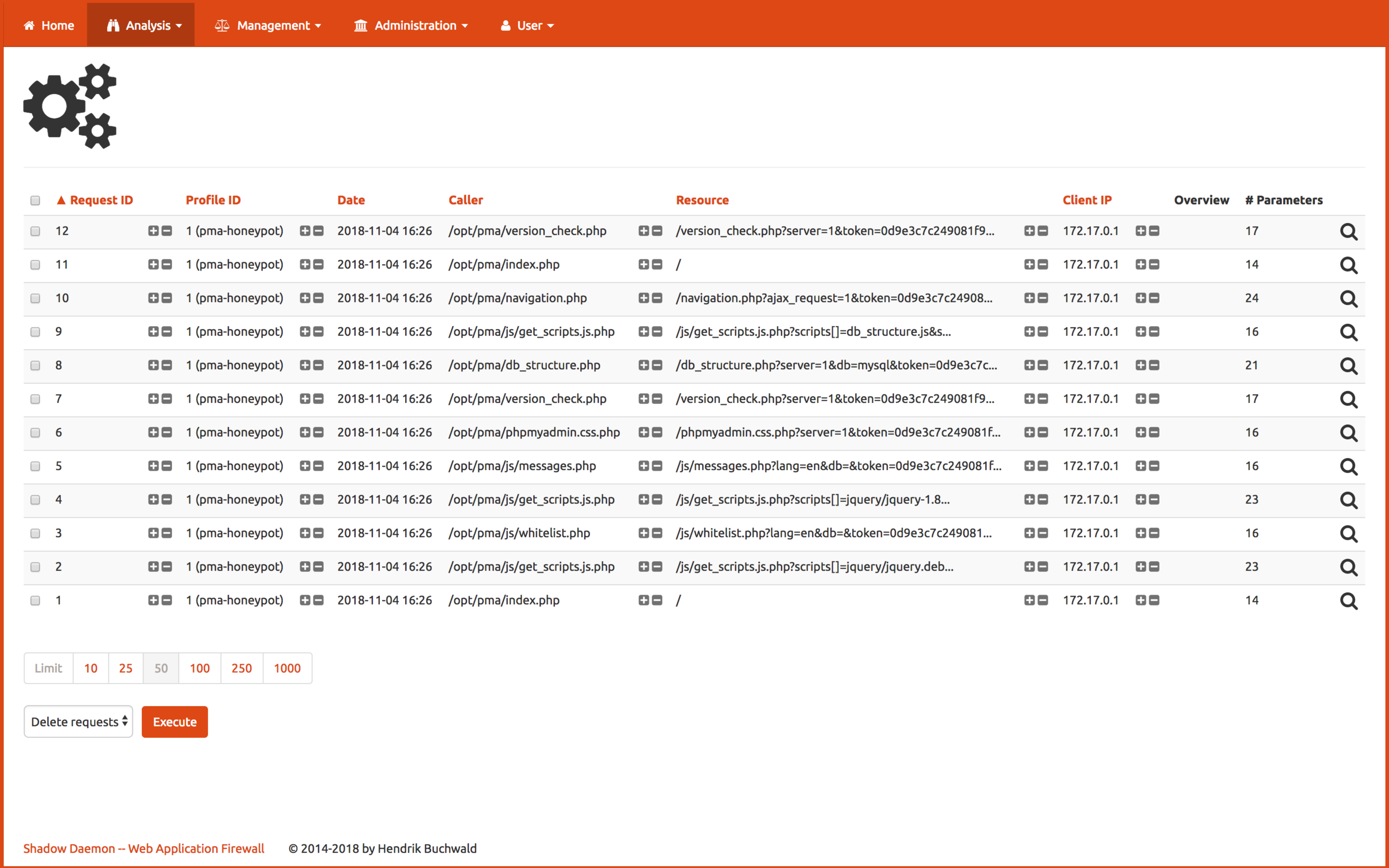
- Version information: 4.0.10.20
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

⚠ The phpMyAdmin configuration storage is not completely configured, some extended features have been deactivated. To find out why click here.

⚠ Your PHP MySQL library version 5.5.60-MariaDB differs from your MySQL server version 5.6.42. This may cause unpredictable behavior.

ⓘ The *mcrypt* extension is missing. Please check your PHP configuration.

kayra.otaner@secops360.com

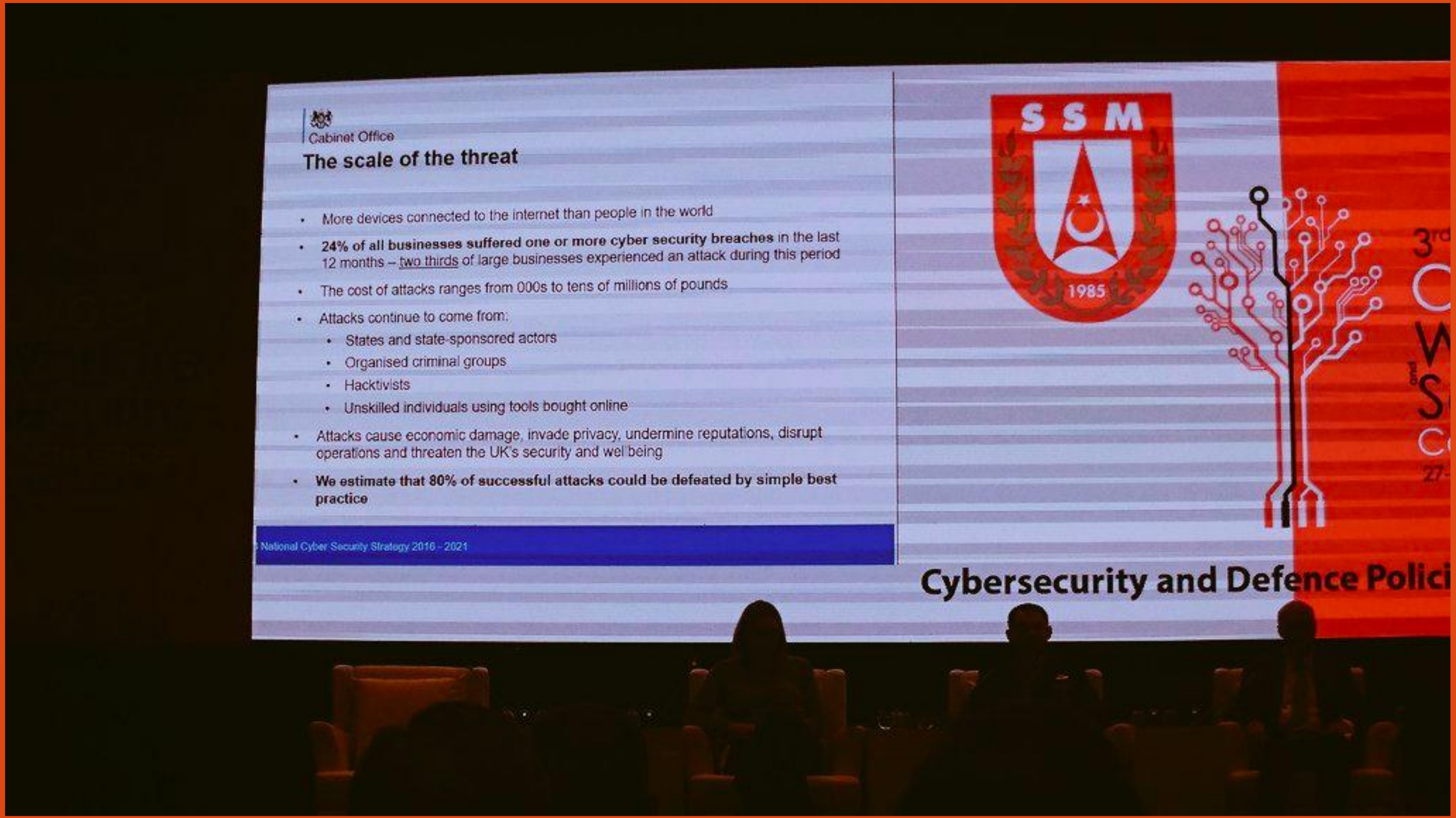


□	▲ Request ID	Profile ID	Date	Caller	Resource	Client IP	Overview	# Parameters
□	12	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/version_check.php	/version_check.php?server=1&token=0d9e3c7c249081f9...	172.17.0.1		17
□	11	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/index.php	/	172.17.0.1		14
□	10	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/navigation.php	/navigation.php?ajax_request=1&token=0d9e3c7c24908...	172.17.0.1		24
□	9	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/js/get_scripts.js.php	/js/get_scripts.js.php?scripts[]=db_structure.js&s...	172.17.0.1		16
□	8	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/db_structure.php	/db_structure.php?server=1&db=mysql&token=0d9e3c7c...	172.17.0.1		21
□	7	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/version_check.php	/version_check.php?server=1&token=0d9e3c7c249081f9...	172.17.0.1		17
□	6	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/phpmyadmin.css.php	/phpmyadmin.css.php?server=1&token=0d9e3c7c249081f...	172.17.0.1		16
□	5	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/js/messages.php	/js/messages.php?lang=en&db=&token=0d9e3c7c249081f...	172.17.0.1		16
□	4	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/js/get_scripts.js.php	/js/get_scripts.js.php?scripts[]=jquery/jquery-1.8...	172.17.0.1		23
□	3	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/js/whitelist.php	/js/whitelist.php?lang=en&db=&token=0d9e3c7c249081...	172.17.0.1		16
□	2	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/js/get_scripts.js.php	/js/get_scripts.js.php?scripts[]=jquery/jquery.deb...	172.17.0.1		23
□	1	1 (pma-honeypot)	2018-11-04 16:26	/opt/pma/index.php	/	172.17.0.1		14

Shadow Daemon -- Web Application Firewall © 2014-2018 by Hendrik Buchwald

Head of International Cyber Security Team, UK Foreign and Commonwealth Office

We estimate that 80% of successful attacks could be defeated by simple best practice.



Cabinet Office

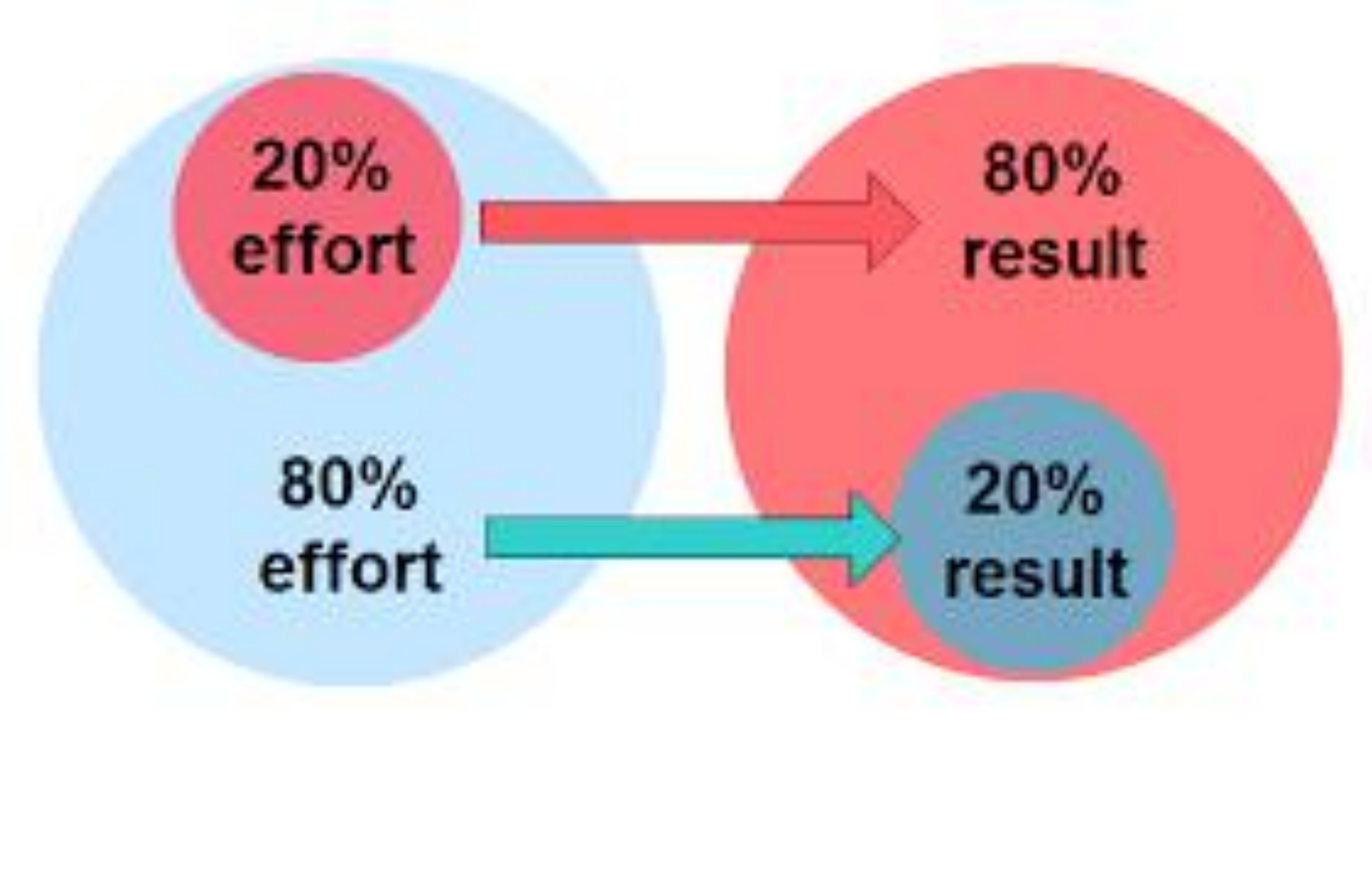
The scale of the threat

- More devices connected to the internet than people in the world
- **24% of all businesses suffered one or more cyber security breaches** in the last 12 months – two thirds of large businesses experienced an attack during this period
- The cost of attacks ranges from 000s to tens of millions of pounds
- Attacks continue to come from:
  - States and state-sponsored actors
  - Organised criminal groups
  - Hacktivists
  - Unskilled individuals using tools bought online
- Attacks cause economic damage, invade privacy, undermine reputations, disrupt operations and threaten the UK's security and wel being
- **We estimate that 80% of successful attacks could be defeated by simple best practice**

National Cyber Security Strategy 2016 - 2021

kayra.otaner@secops360.com

Is applying best practices good enough for your environment?



kayra.otaner@secops360.com

Those who know do,
Those who understand, teach
Aristotle

Follow me on :
https://twitter.com/kayraotaner

- **https://www.linkedin.com/in/kayraotaner**

kayra.otaner@secops360.com