
TIBER
Connecting threat intelligence
and red teaming
Marc Smeets & Stan Hegt
19 March 2019
OUTFLANK
clear advice with a hacker mindset

PART I

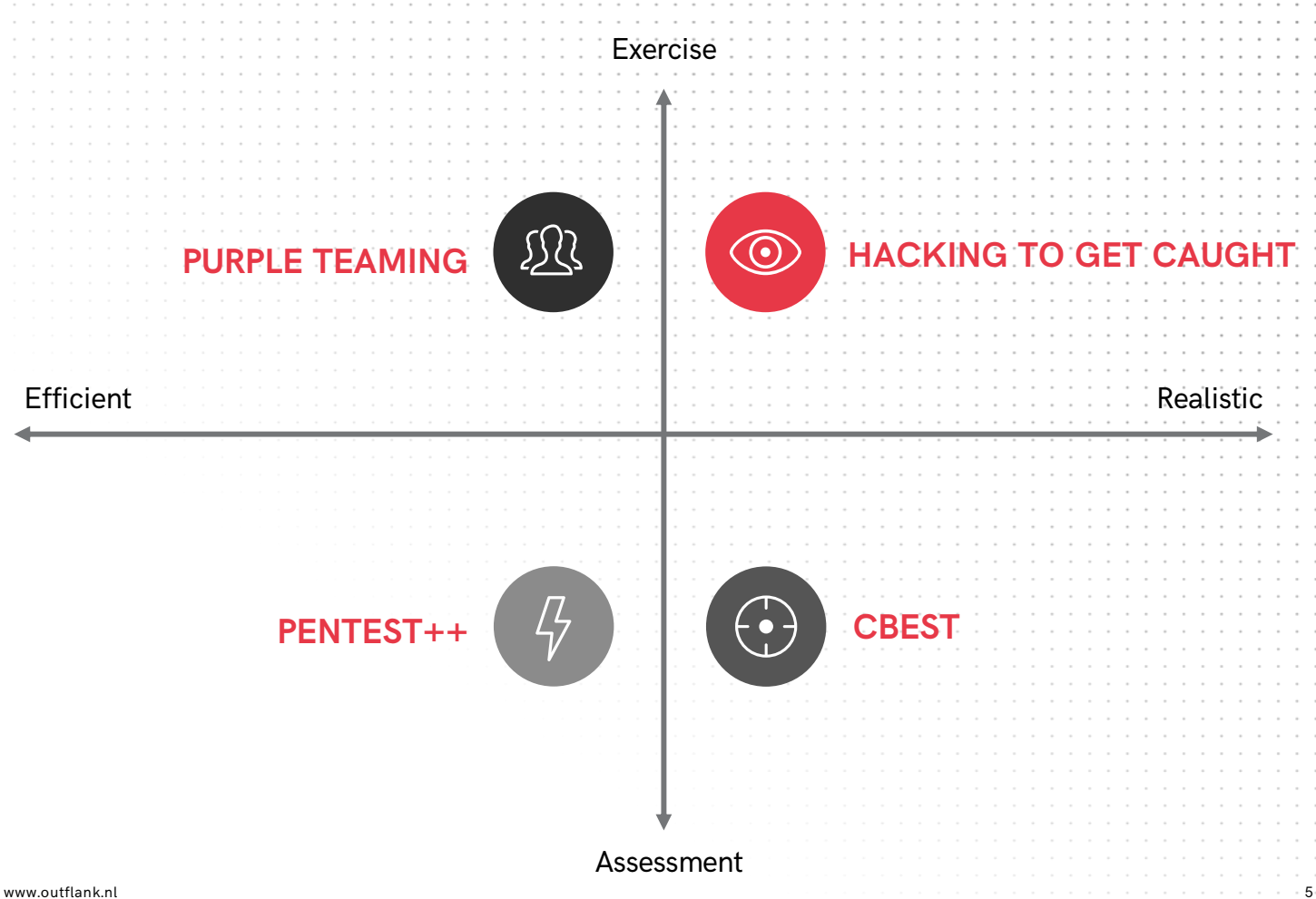
About Red Teaming

OUTFLANK

clear advice with a hacker mindset


56
35
53


PAFFEN
SPORT

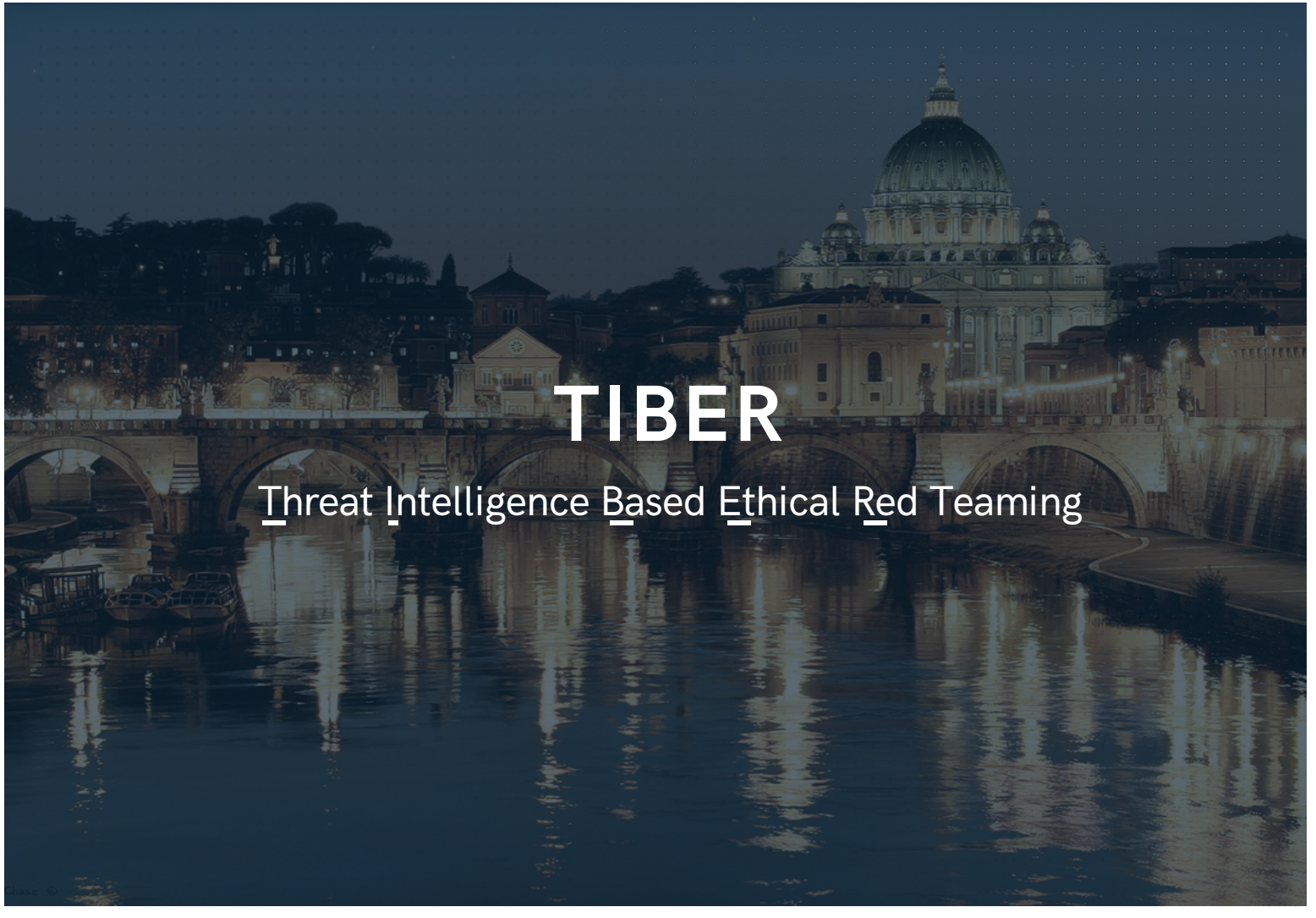

Exercise
PURPLE TEAMING
HACKING TO GET CAUGHT
Efficient
Realistic
PENTEST++
CBEST
Assessment

PART II

Threat Intelligence Based Red Teaming

OUTFLANK

clear advice with a hacker mindset


TIBER
Threat Intelligence Based Ethical Red Teaming

TIBER PROCESS (SIMPLIFIED)

Target intelligence

- Gather intelligence
- Threat assessment report
- Targeting intelligence report

Scenario testing

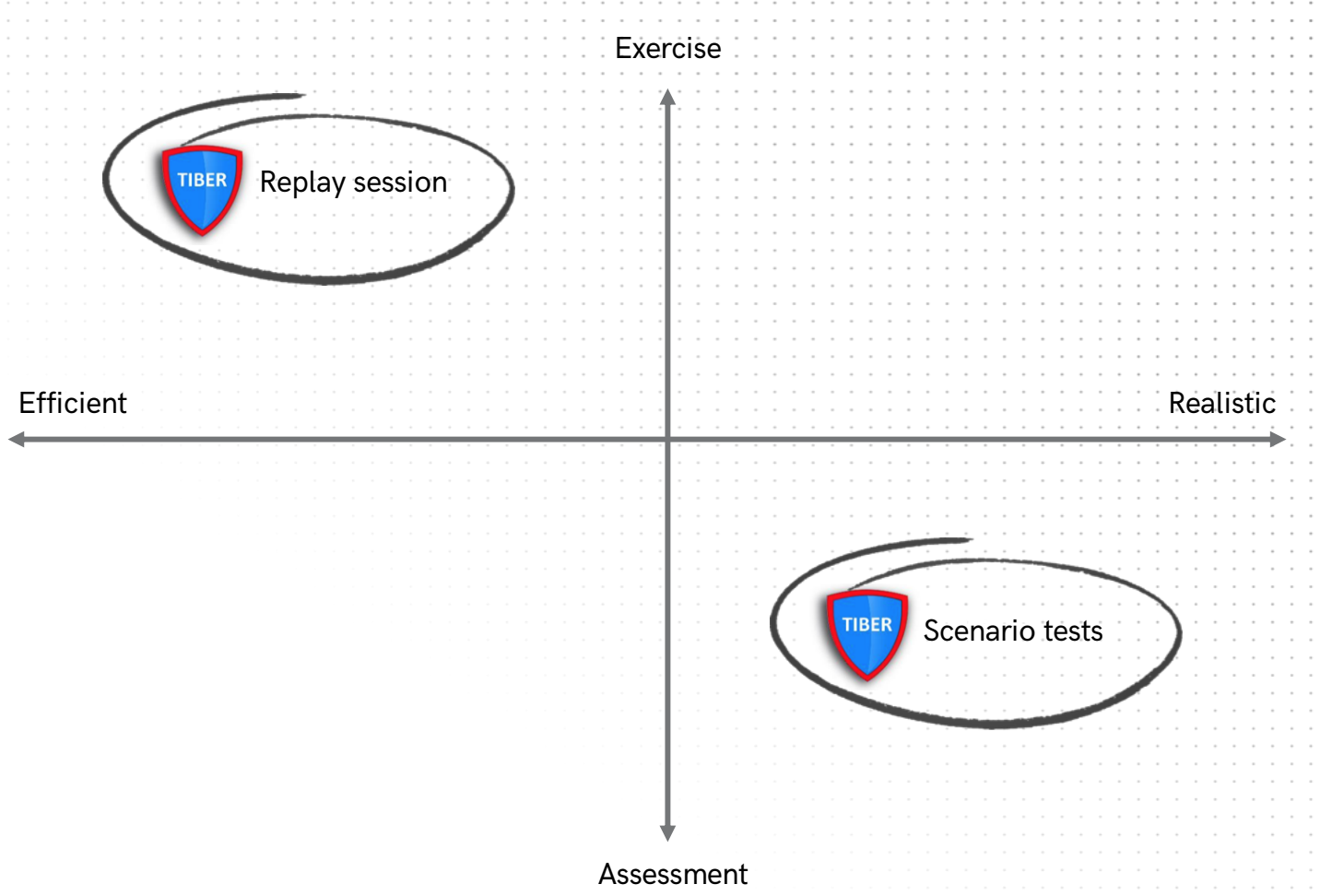
- Draft test plan
- Simulate three attack scenarios
- 12 Week period

Replay and evaluation

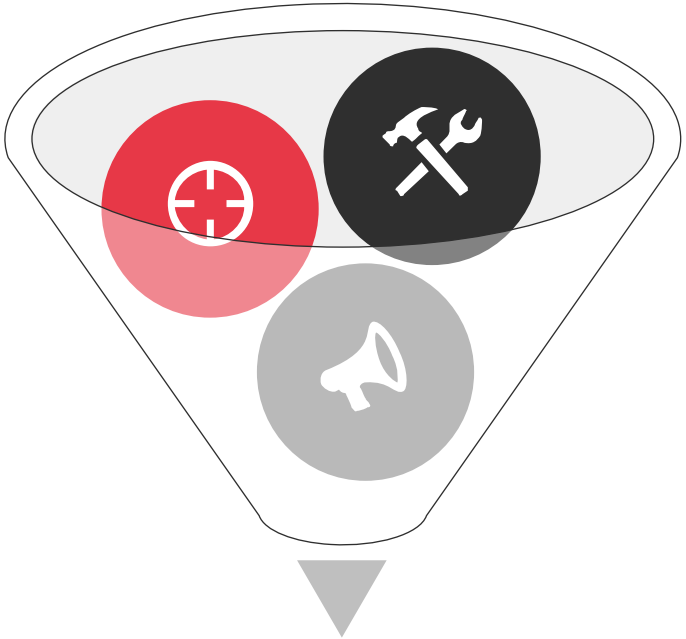
- Purple teaming session
- Evaluate simulated attack
- Repeat steps for tuning of defenses

Reporting and feedback

- Red team report
- Mitigation plan
- Feedback session


Exercise
TIBER
Replay session
Efficient
Realistic
TIBER
Scenario tests
Assessment

TI INPUT FOR SCENARIO SELECTION



2 scenarios based on current threats
+ 1 forward-looking, creative scenario

Generic CFI TI report

Sector specific yearly TI report from central bank, private parties and intelligence agency

Scoping document

Document by target FI detailing critical economic functions and systems

Target intelligence

Report by TI provider on threat posture of target FI

TYPICAL TI DELIVERABLES

Similar incidents

- Post-mortem analysis
- C2 and malware artefacts
- IOCs

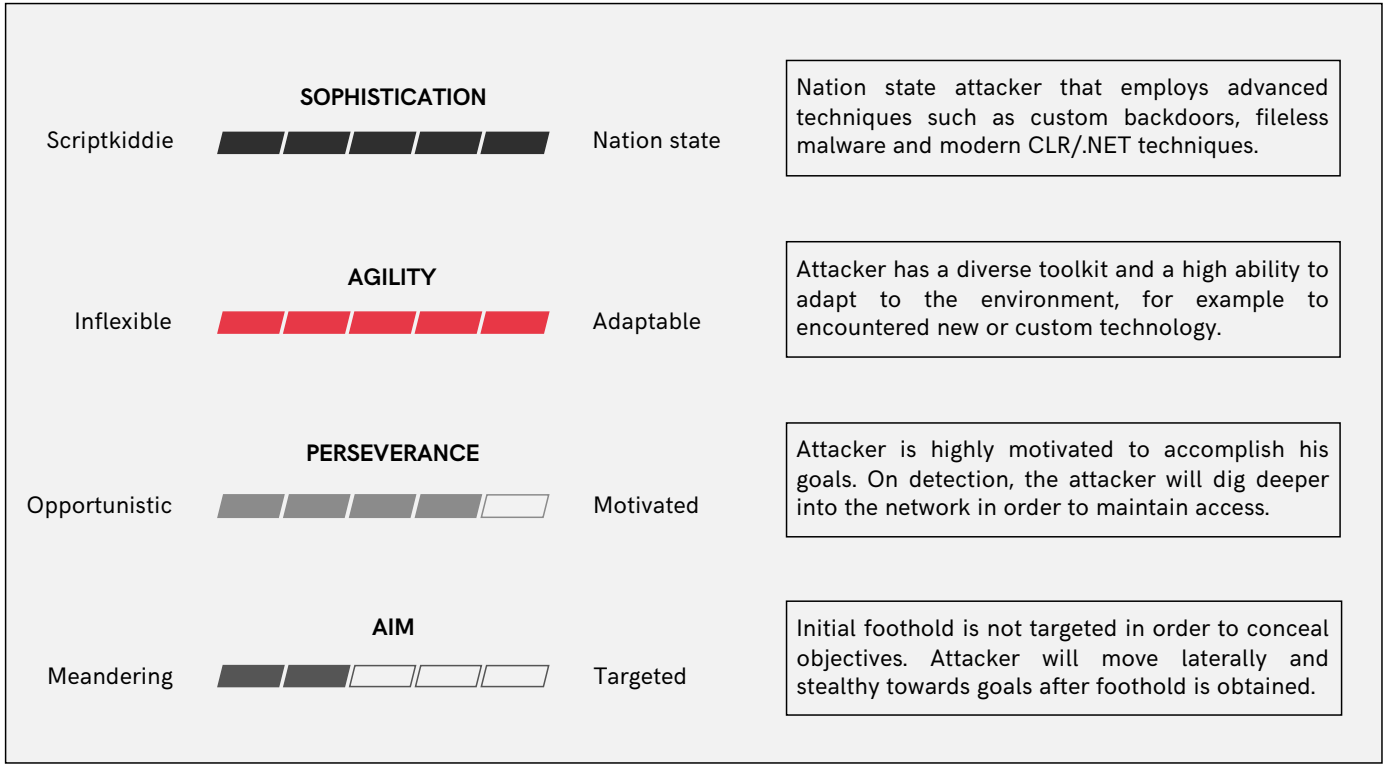
Threat actors

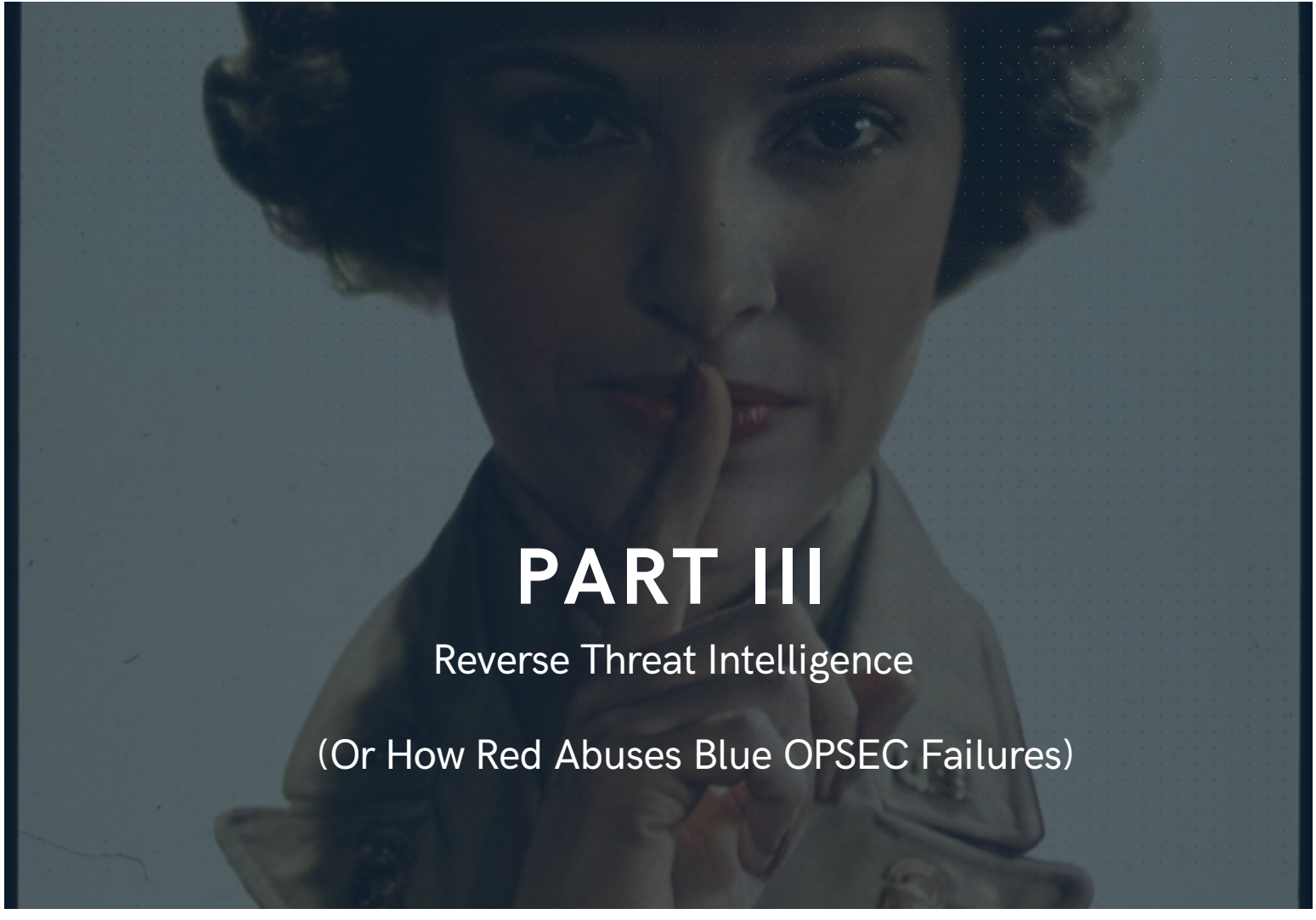
- Attribution
- TTPs
  (usually mapped to ATT&CK)
- Mapping to CEF of target
  (motivation)
- Mapping to systems of target
  (objectives)

Targeting intelligence

- Passive perimeter recon
- Social media
- Credential and data leaks

ATTACKER MODEL: EXAMPLE





PART III

Reverse Threat Intelligence

(Or How Red Abuses Blue OPSEC Failures)

OFFENSIVE INFRA – TYPICAL SETUP

C2

- Redirectors / reverse proxies
- Domain fronting
- C2-servers / CS Team servers

Fake identities

- Social media profiles
- Websites

Tracking and debugging

- Tracking pixels

Delivery

- Web servers
- Email
- File sharing service
- Messaging platforms
- …

Generic backend components

- Communication channels
- Test environments
- Log aggregation

OFFENSIVE INFRA – TYPICAL CHALLENGES

Oversight

Insight

"Every contact leaves a trace" - Locard's exchange principle

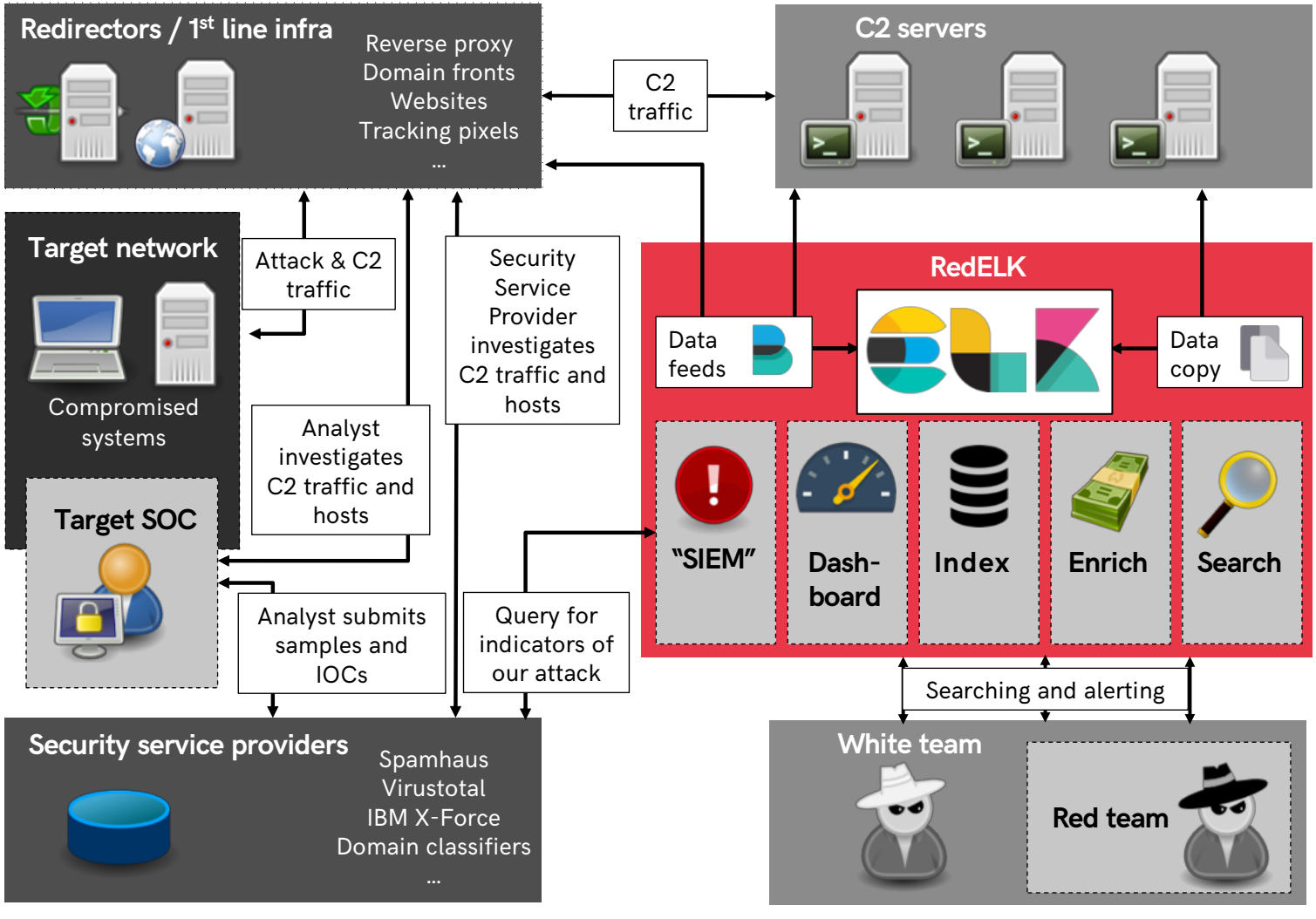
TOOLING -> RedELK

+

=

https://outflank.nl/blog/2019/02/14/introducing-redelk-part-1-why-we-need-it/

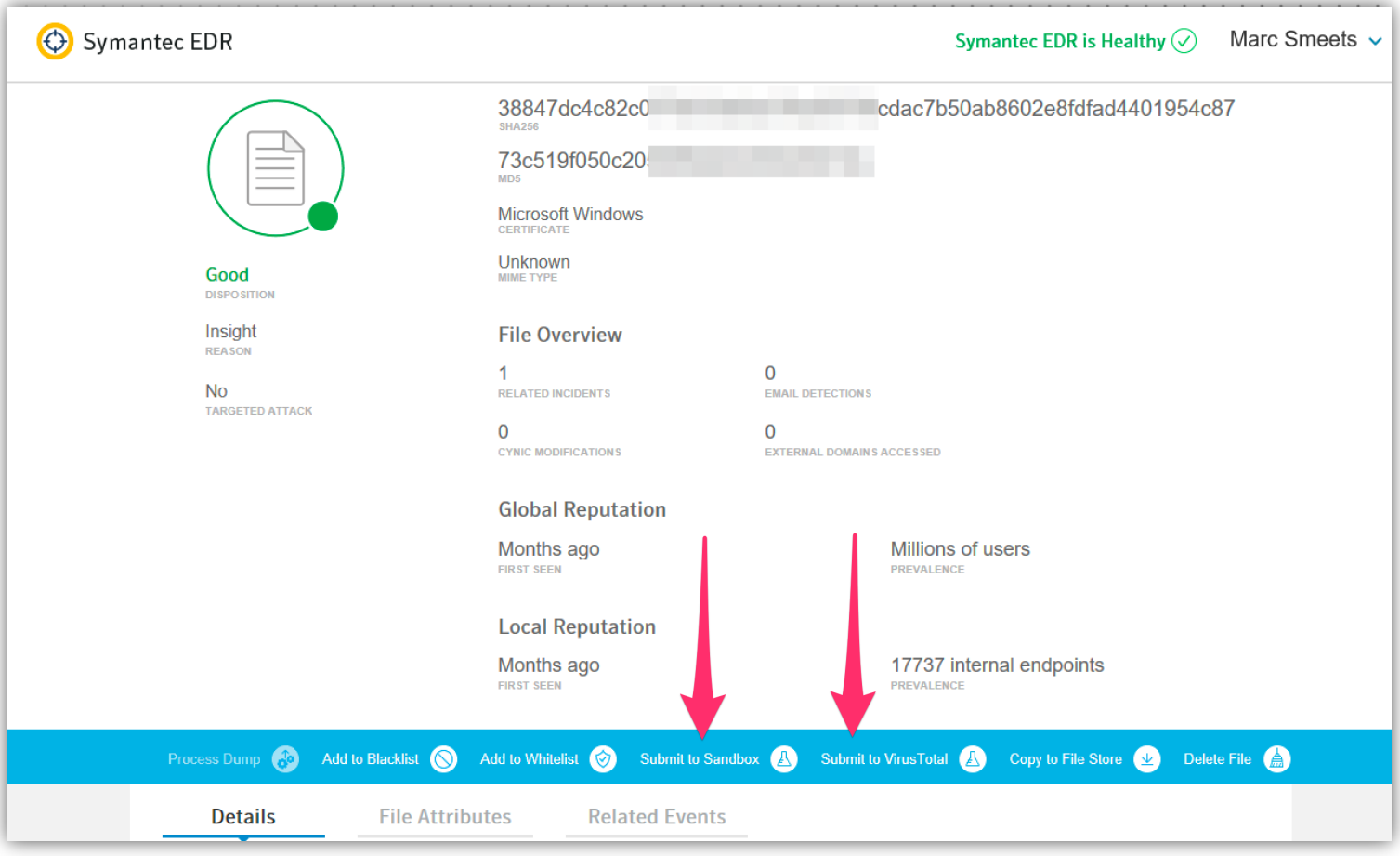
https://github.com/outflanknl/RedELK/


Redirectors / 1st line infra
Reverse proxy
Domain fronts
Websites
Tracking pixels
...
C2 traffic
C2 servers
Target network
Compromised systems
Attack & C2 traffic
Security Service Provider investigates C2 traffic and hosts
RedELK
Data feeds
Data copy
"SIEM"
Dash-board
Index
Enrich
Search
Target SOC
Analyst investigates C2 traffic and hosts
Analyst submits samples and IOCs
Query for indicators of our attack
Searching and alerting
Security service providers
Spamhaus
Virustotal
IBM X-Force
Domain classifiers
...
White team
Red team

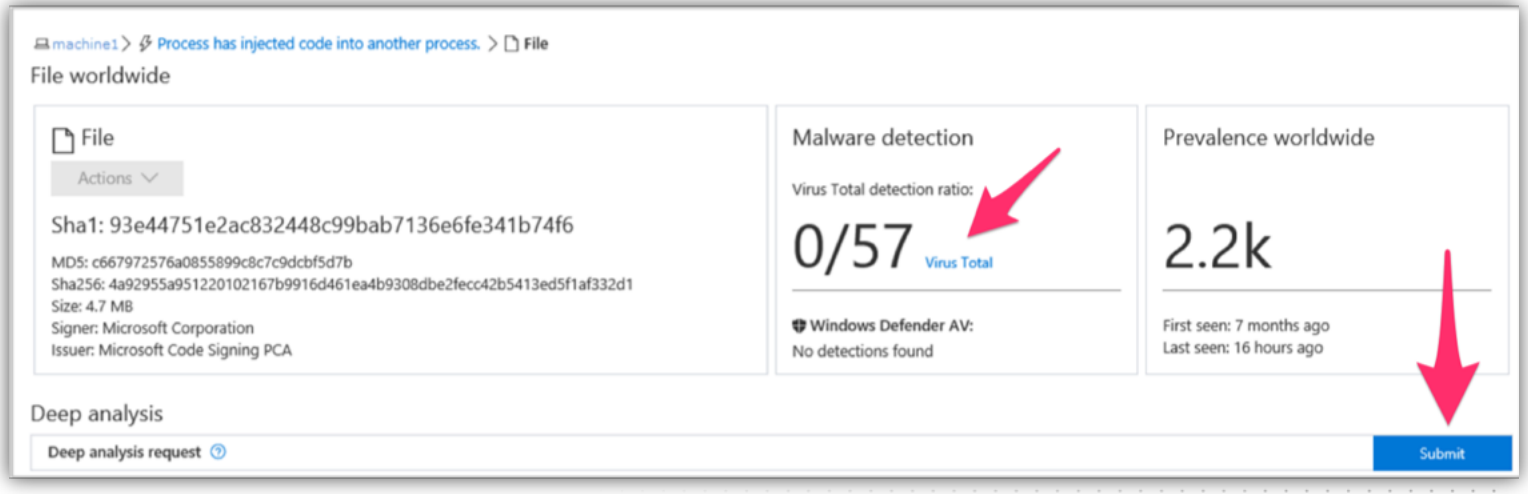
INDICATORS

ONLINE SERVICES

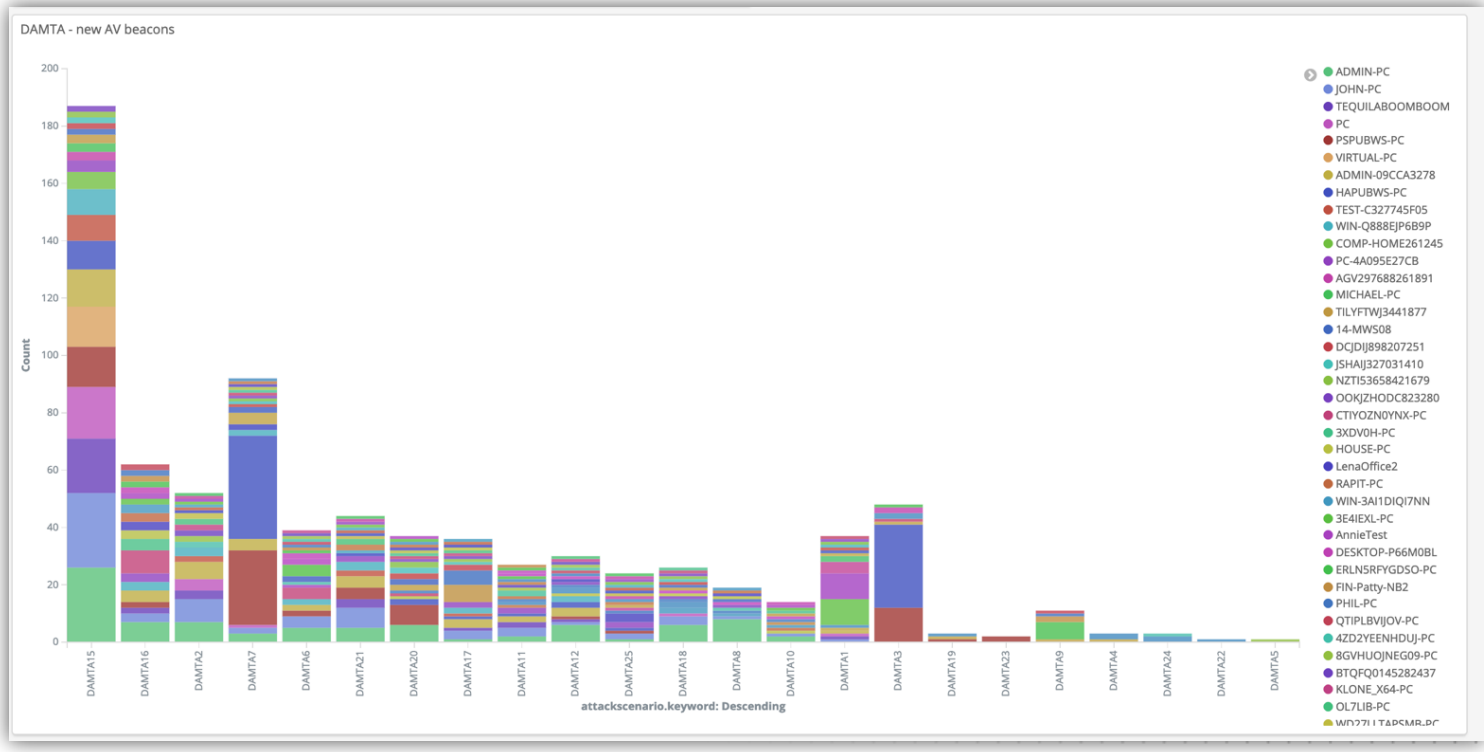
HASH OF MALWARE



HASH OF MALWARE



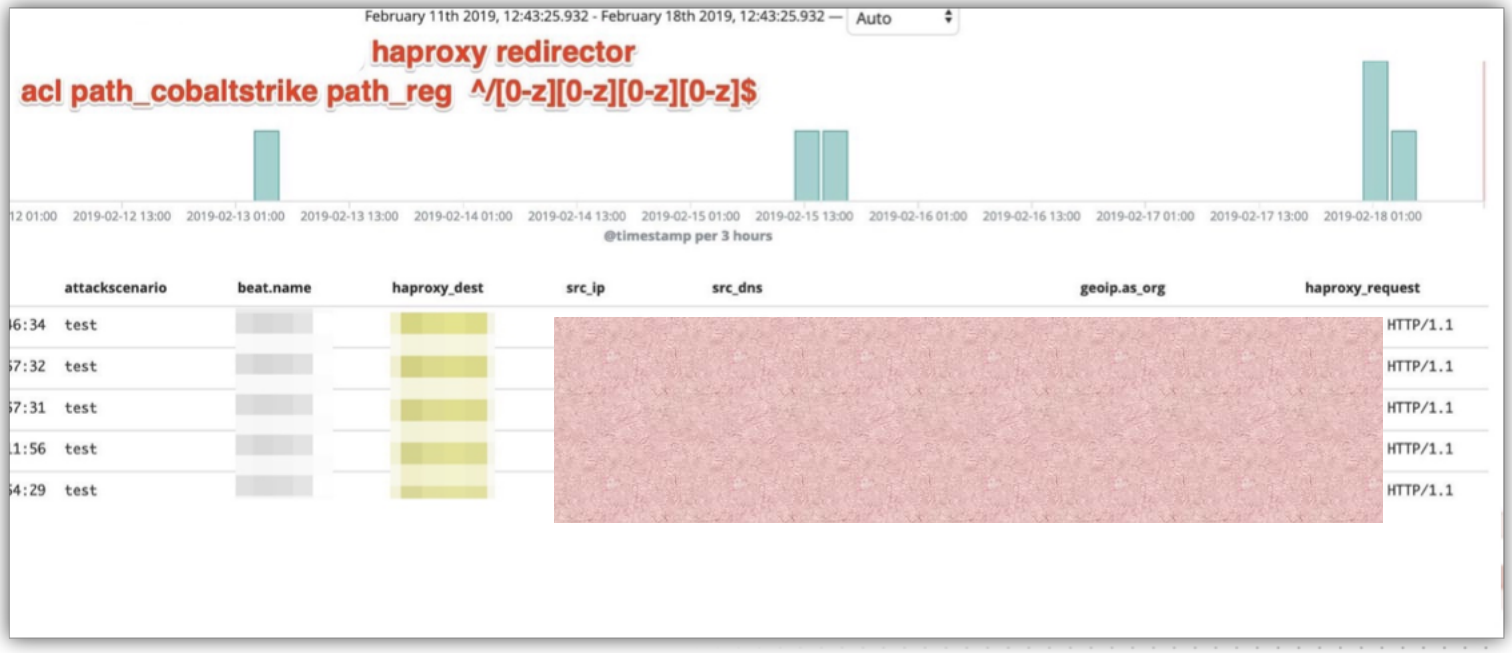
SANDBOX CONNECTIONS



INDICATORS

TRAFFIC TO INFRASTRUCTURES

C2 TOOL ARTEFACT SCANNERS



ANALYST TRAFFIC

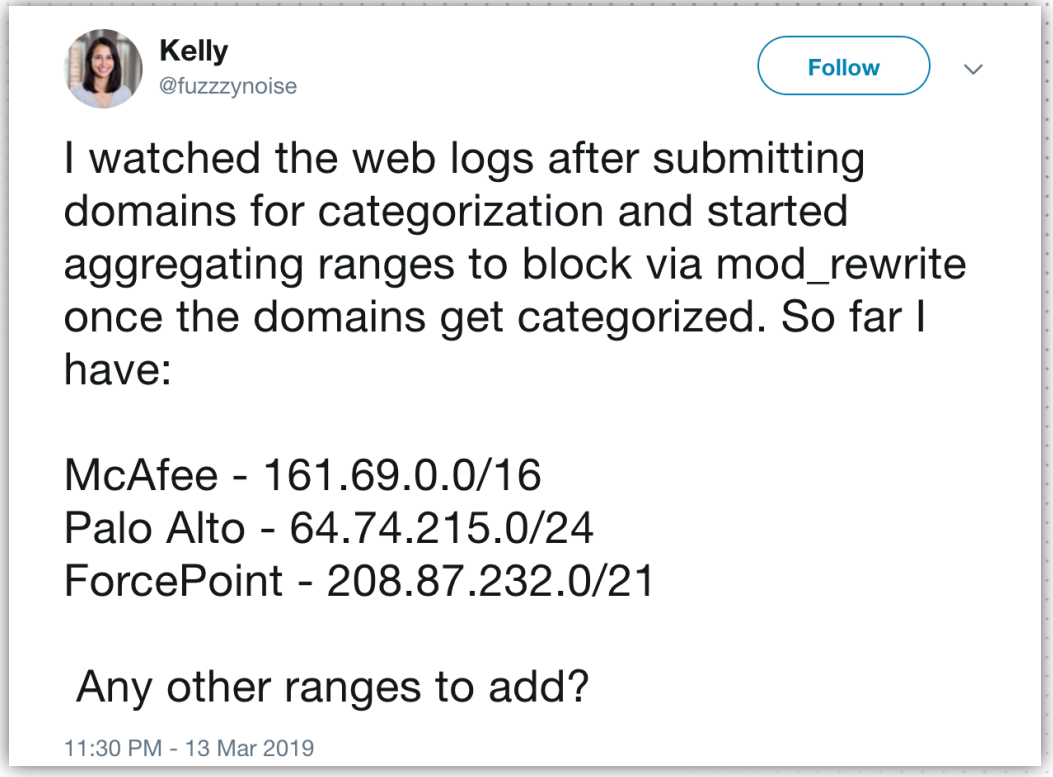
haproxy_useragent.keyword: Descending	src_ip.keyword: Descending	src_dns.keyword: Descending	
curl/7.35.0	[redacted]	[redacted]	azonaws.com
python-requests/2.13.0			
python-requests/2.13.0			m
python-requests/2.13.0			
python-requests/2.20.1			zonaws.com
Python-urllib/2.7			
curl/7.35.0			azonaws.com
python-requests/2.13.0			
python-requests/2.13.0			
curl/7.62.0			
Python-urllib/3.6			

IM PREVIEW

haproxy_dest	src_ip	src_dns		geoip.as_org	haproxy_request	haproxy_useragent
www-decoy			16	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_2 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			11	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_22 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			17	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_223 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			10	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_2234 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			17	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_ HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			3	Telegram Messenger LLP	GET /test_TELEGRAM-2019031 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			19	Telegram Messenger LLP	GET /test_TELEGRAM-20190317 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			12	Telegram Messenger LLP	GET /test_TELEGRAM-201903 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			18	Telegram Messenger LLP	GET /test_TELEGRAM-20190 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			18	Telegram Messenger LLP	GET /test_TELEGRAM-2019 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			8	Telegram Messenger LLP	GET /test_TELEGRAM-20 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			16	Telegram Messenger LLP	GET /test_TELEGRAM-201 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy			5	Telegram Messenger LLP	GET /test_TELEGRAM-2 HTTP/1.1	TelegramBot (like TwitterBot)

https://hunch.ly/osint-articles/osint-article-how-to-blow-your-online-cover

DOMAIN CLASSIFIER



DOMAIN CLASSIFIER

attackscenario	beat.name	haproxy_dest	src_ip	src_dns	geoip.as_org	haproxy_request
scen1	redir-https2	www-decoy		170	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		.10	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		.10	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		170	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		146	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		146	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		146	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		.10	PALO ALTO NETWORKS	GET / HTTP/1.1
scen1	redir-https2	www-decoy		.10	PALO ALTO NETWORKS	GET / HTTP/1.1

INDICATORS

TARGET INTERNAL CHECKS

KRBTGT RESET

```
[redacted] get-aduser krbtgt -properties passwordlastset


DistinguishedName : CN=krbtgt,CN=Users,DC=[redacted]DC=net
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : d029589c-f6ad-4b4c-96c2-2613d[redacted]
PasswordLastSet   : 23/08/2010 17:20:00
SamAccountName    : krbtgt
SID               : S-1-5-21-1561531455-114652488[redacted]-502
Surname           :
UserPrincipalName : krbtgt@[redacted]net
```

INDICATORS OF ANALYSES / INVESTIGATION / DETECTION

TYPE OF CHECK	DETAIL
Online service	**AV hash** : hash of our malware is known at VirusTotal or others
	Infra blacklist : IP, URL of TLS cert blacklist
Traffic to infra	**C2 scanners** : global scans for C2 tool artefacts
	AV sandbox : C2 session from a known malware sandbox
	Analyst traffic : typical traffic from analyst, eg TOR IP, curl, other URIs
	Sec Vendor traffic : security vendor visits our infra – each with own characteristics
	Instant Messaging : ‘previews’ of Instant Messaging clients
Target internal	**KRBTGT / admin reset** : unexpected password changes of critical accounts
	Security tool : unexpected change of AV / EDR tools installed

PART IV

Going forward

OUTFLANK

clear advice with a hacker mindset

LESSONS TO BE LEARNED

Red teaming != red teaming

Our goals:

- **We want stronger TI for better red teaming**
  - Better adjusted to real actor's tactics and behavior
  - Input for TIBER et al: more details about target, i.e. desktop OS and office versions

- **We need stronger blue teams**
  - We are in this to defend our customers. Stronger blue enables stronger red -> makes blue stronger -> stronger red, etc.

OUTFLANK

clear advice with a hacker mindset

Marc Smeets

+31 6 5136 6680
marc@outflank.nl
www.outflank.nl/marc

@MarcOverIP

Stan Hegt

+31 6 1188 5039
stan@outflank.nl
www.outflank.nl/stan

@StanHacked