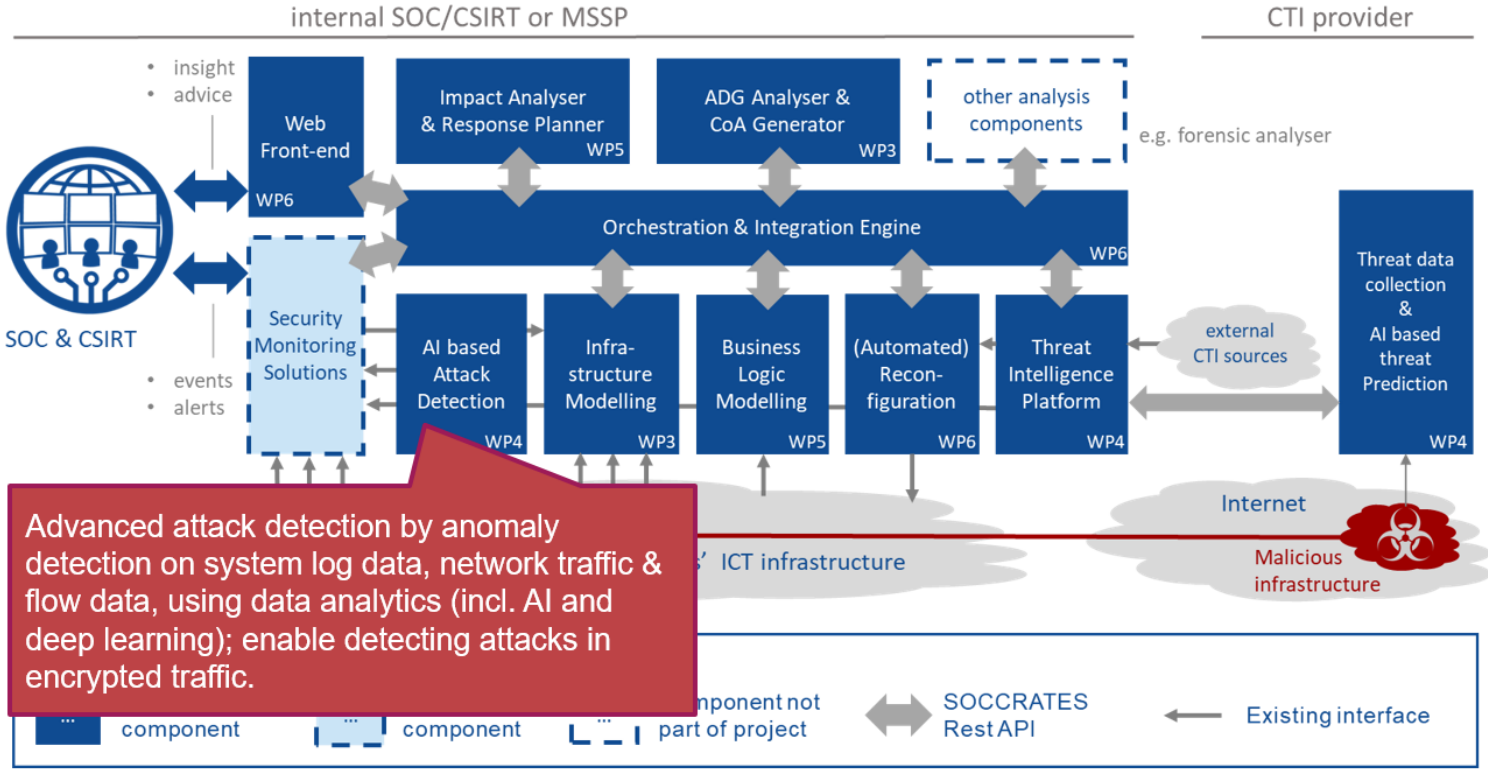
NETWORK-BASED ANOMALY DETECTION

DNS NINJA & ABC TOOL

Irina Chiscop

TNO innovation for life

RELEVANCE



Advanced attack detection by anomaly detection on system log data, network traffic & flow data, using data analytics (incl. AI and deep learning); enable detecting attacks in encrypted traffic.

FOCUS ON INTERNAL NETWORK PATTERNS IN COMBINATION WITH ANOMALY DETECTION

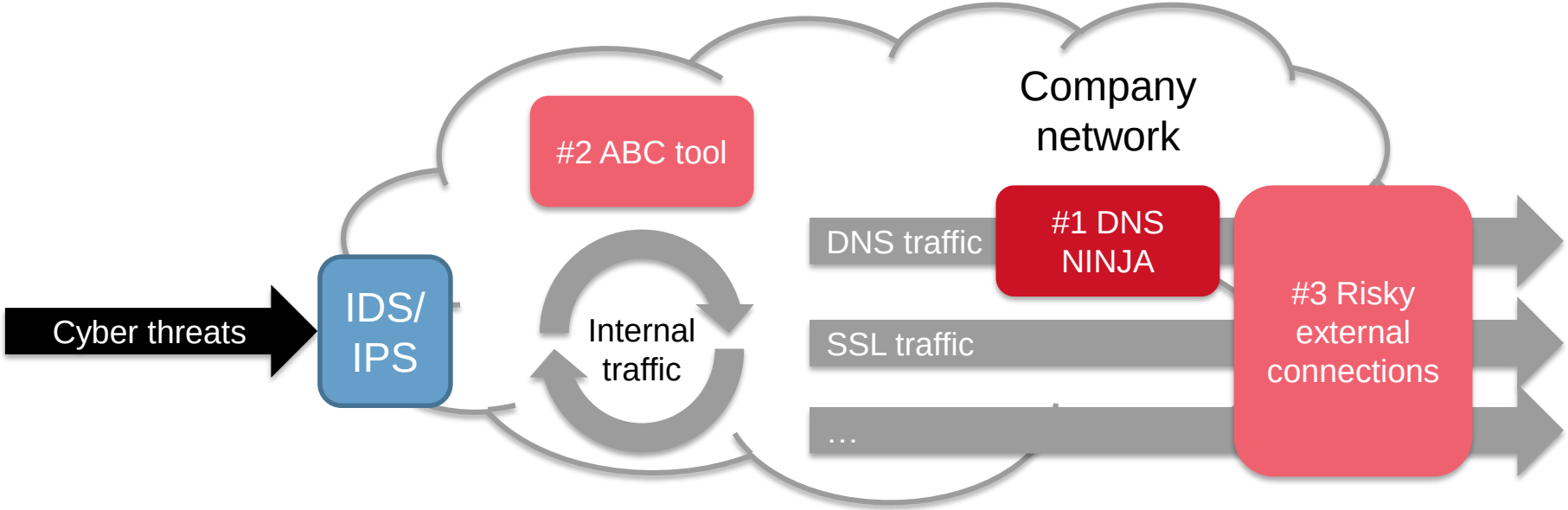
- Advanced targeted attacks typically consist of attack phases as shown in the lifecycle visualization
- Most commercial monitoring and detection products focus on inbound network traffic & rule-based detection
- Blind spot: analyzing internal network patterns in combination with anomaly detection

Signature Detection

Anomaly Detection

Dell SecureWorks attack lifecycle

ASSUMPTION: INTRUSION ALREADY TOOK PLACE

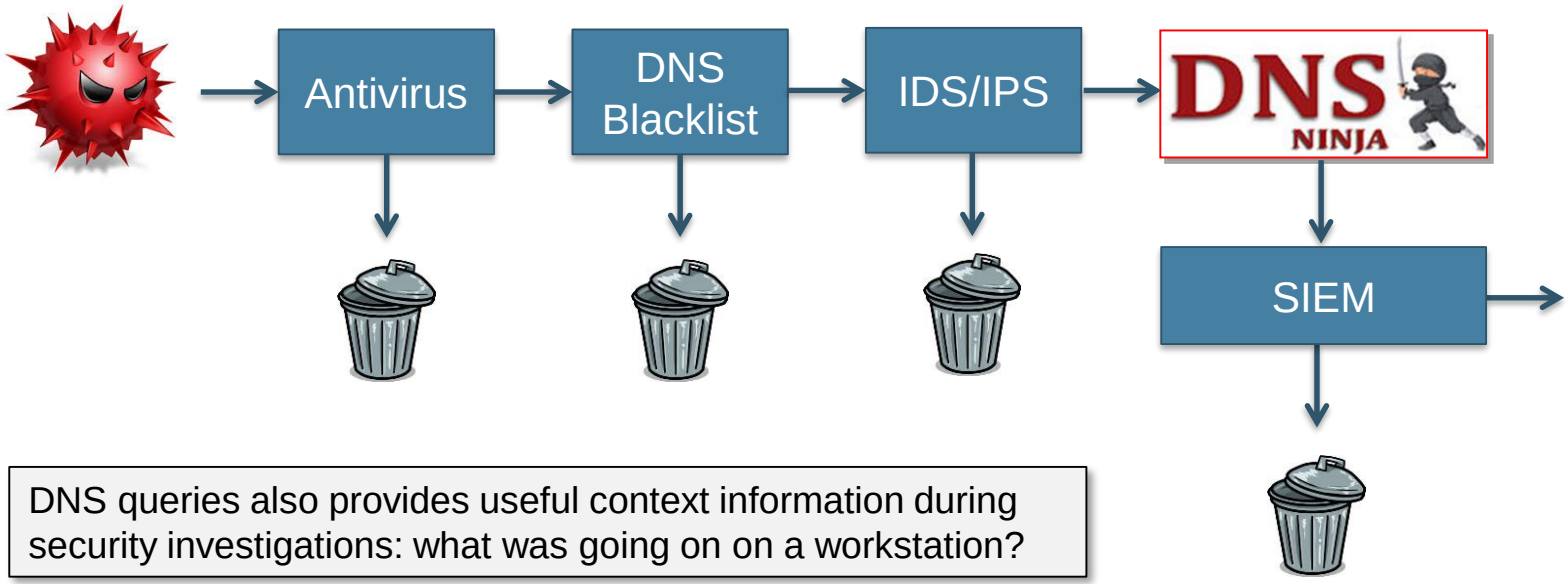


WHY DNS?

- Malicious software often tries to contact the outside world.

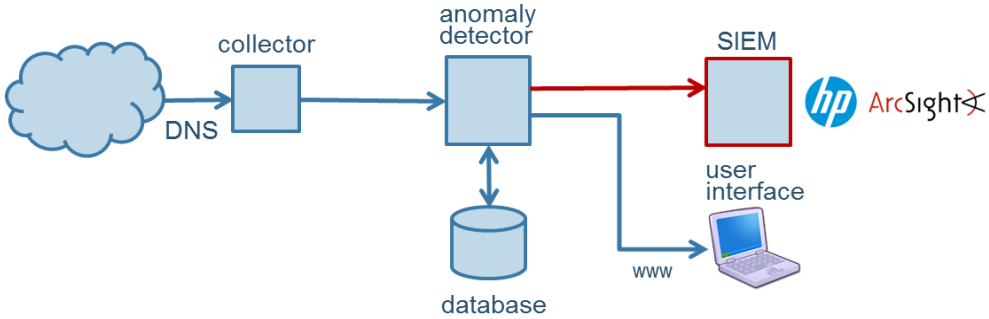
- DNS is commonly used for finding external servers ➔
- **Infections and attacks within a company network may be detected better / quicker if we take DNS queries into account**.
  - Examples: botnets, command and control traffic, ransomware, key loggers, DNS tunneling, …
    - Wannacry
      - Iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
        Ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

OUR SOLUTION: DNS NINJA
EXTRA LINE OF DEFENSE, SPECIALIZED IN DNS



DNS queries also provides useful context information during security investigations: what was going on on a workstation?

DNS NINJA OVERVIEW



Real-time filtering & classification of DNS queries

Real-time detection of “pseudo random” host and domain names (DGA) & puny code confusable

Alerts with “anomaly-scores” to ArcSight SIEM for correlation with other information/events

Web-based user interface for inspection and analysis of detected anomalies

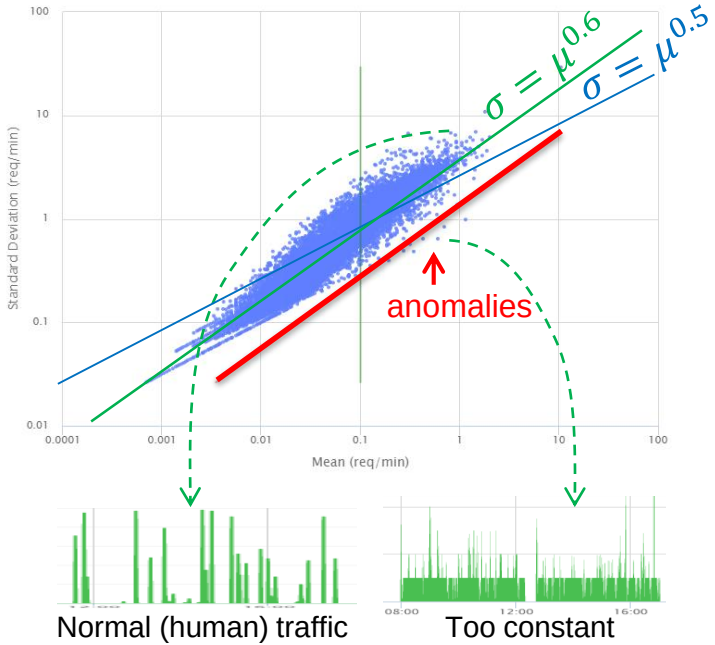
Detecting deviations in statistical properties of DNS traffic of individual hosts

HOW THE ANOMALY DETECTION WORKS (EX. 1/3)

- First the DNS queries of each machine are divided over 21 different (sub)classes: internal, whitelisted, reverse lookup, NXDOMAIN, DGA, MX, SOA, etc.

- Detector #1 detects computers of which the DNS traffic statistics deviate too much of normal random human behavior for one or more of the 21 classes.

Each dot in the graph represents the DNS queries of a computer over a number of hours.



HOW THE ANOMALY DETECTION WORKS (EX. 2/3)

- Detector #2 detects unlikely domain names (based on length, frequencies of letter combinations, and dictionaries)

Time	Type	Domain
08:47:15	A	rgtryhbgddtyh.biz
08:49:53	A	wertdghbyrukl.ch
10:06:40	A	wertdghbyrukl.ch
11:35:19	A	wertdghbyrukl.ch

Real malware

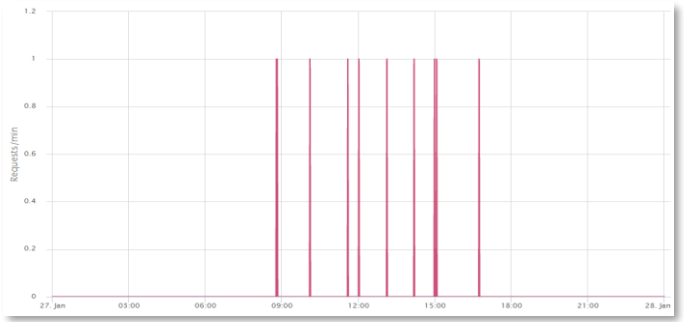
50	jifrdjsqbll3.com	422	A
52	lofofzznjtmyapyng.com	420	A
53	nkklnfupmihl.net	418	A
55	zihovualrnic.com	415	A
56	pwrbjasbrcdobyab.com	415	A
59	pmrrvdzpboio.com	411	A
60	auwnnfqqrsha.com	410	A
62	hl2l7z454.utedxzhpphsbo.com	406	A
64	stjlyttveprknqtcs.com	401	A
65	grmtjauzbliyzd.com	401	A
66	y-xh1xc1vc5.scpfrcjrsrrmzo.com	401	A
69	xishzaukglfojc.com	397	A
73	8i68ap5gvq-m.rluplti4l-woj.com	393	A
74	rqmgnwdeucwiod.com	391	A
75	xontuwlhbttsydv.com	391	A
78	qihnlbnyxgrwpawi.com	387	A
79	mqscvyyszicrbfiovy.com	385	A

Example domain names and anomaly scores

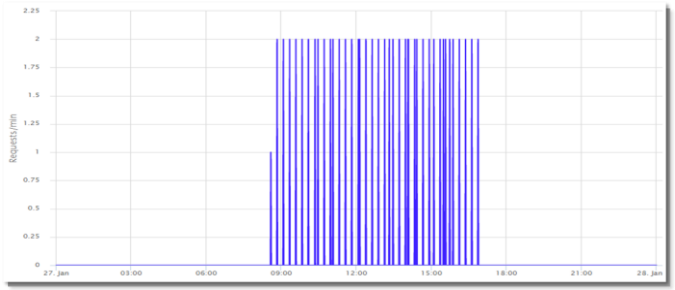
HOW THE ANOMALY DETECTION WORKS (EX. 3/3)

- Detector #3 detects computers of which the DNS queries show a too regular pattern for one or more of the 21 classes.

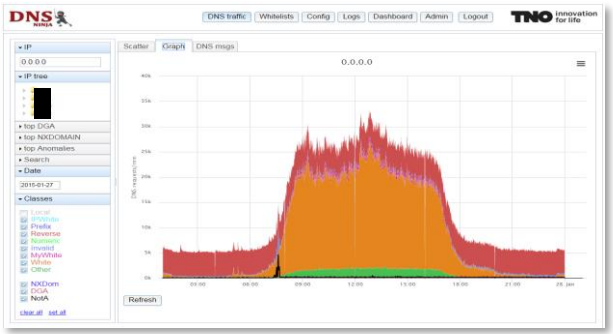
Periodic (class: DGA) – Real malware

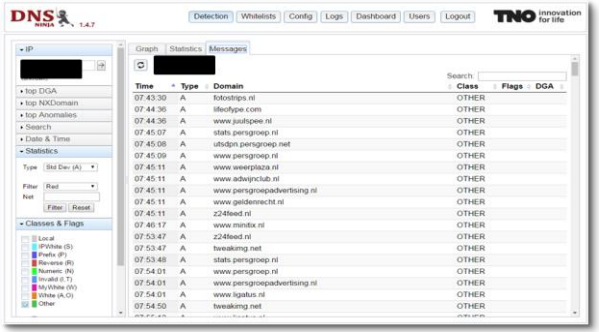


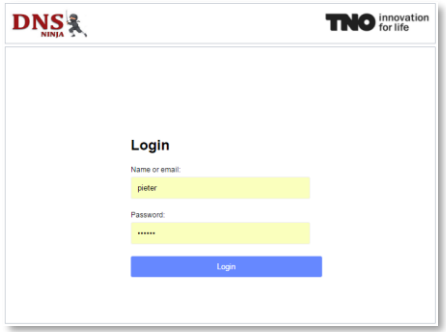
Highly periodic (class: NXDOMAIN)

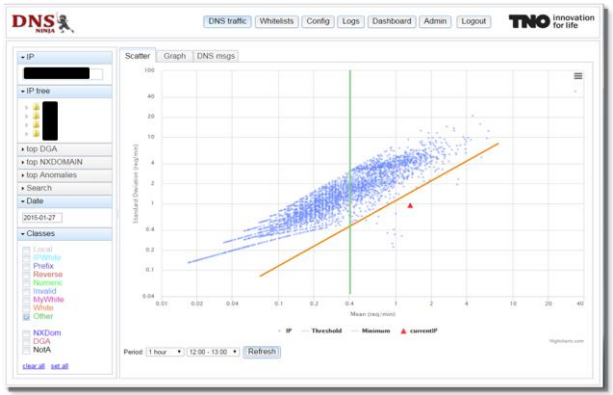


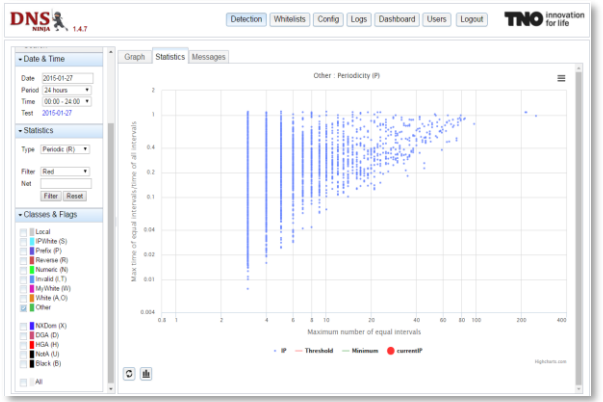
WEB-BASED USER INTERFACE

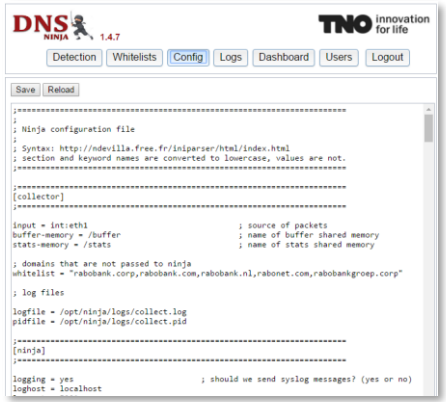




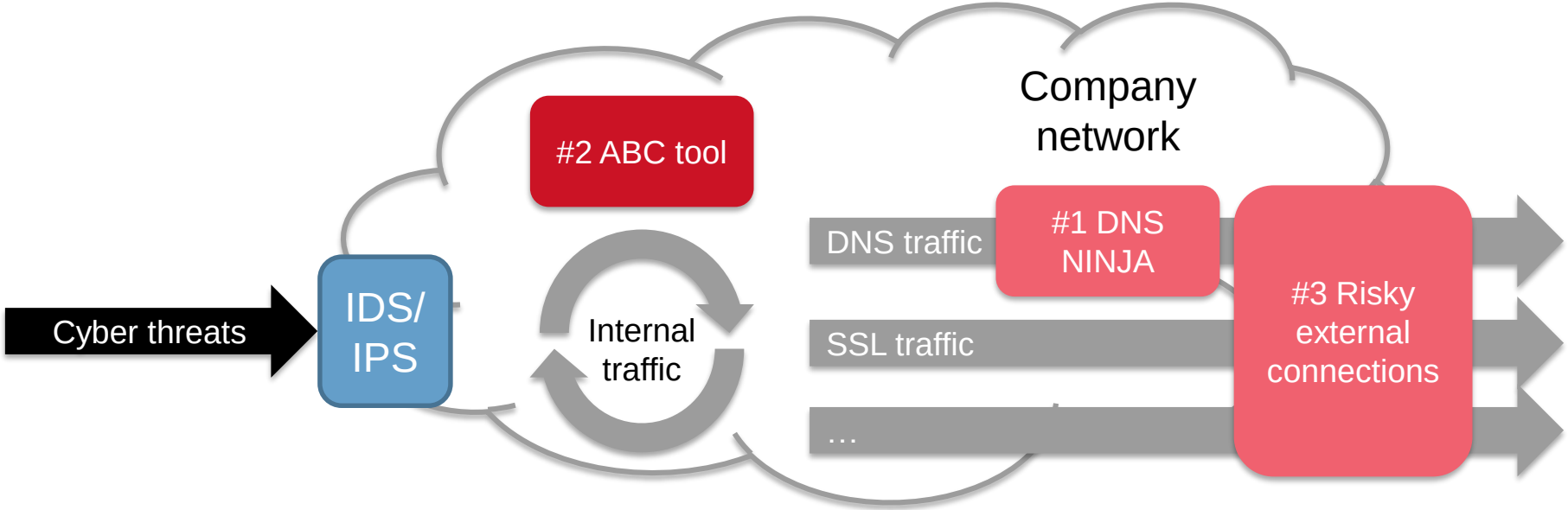








ASSUMPTION: INTRUSION ALREADY TOOK PLACE



INTERNAL NETWORK PATTERNS CAUSED BY TARGETED ATTACKS

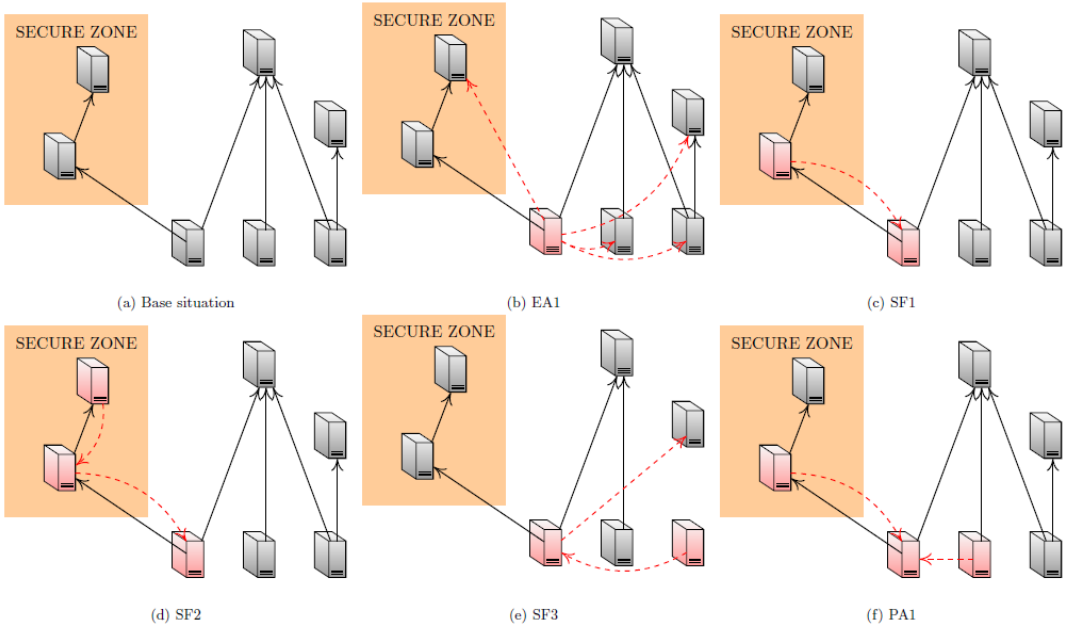
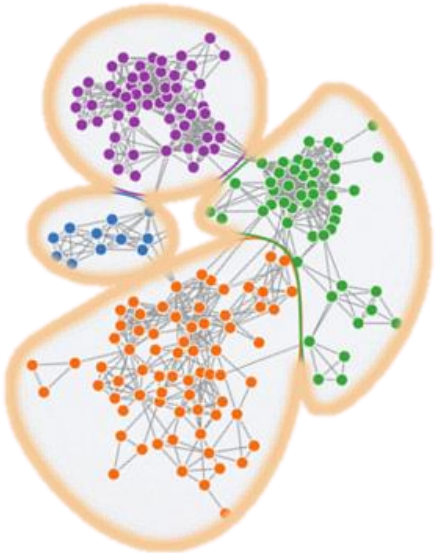


Figure VII.3: Examples of how internal network structures may change. Hosts in the secure zone do not have external Internet access, hosts outside the secure zone have. Red hosts indicate infected hosts, red arrows indicate observable, changed behaviour caused by the corresponding APT characteristic.

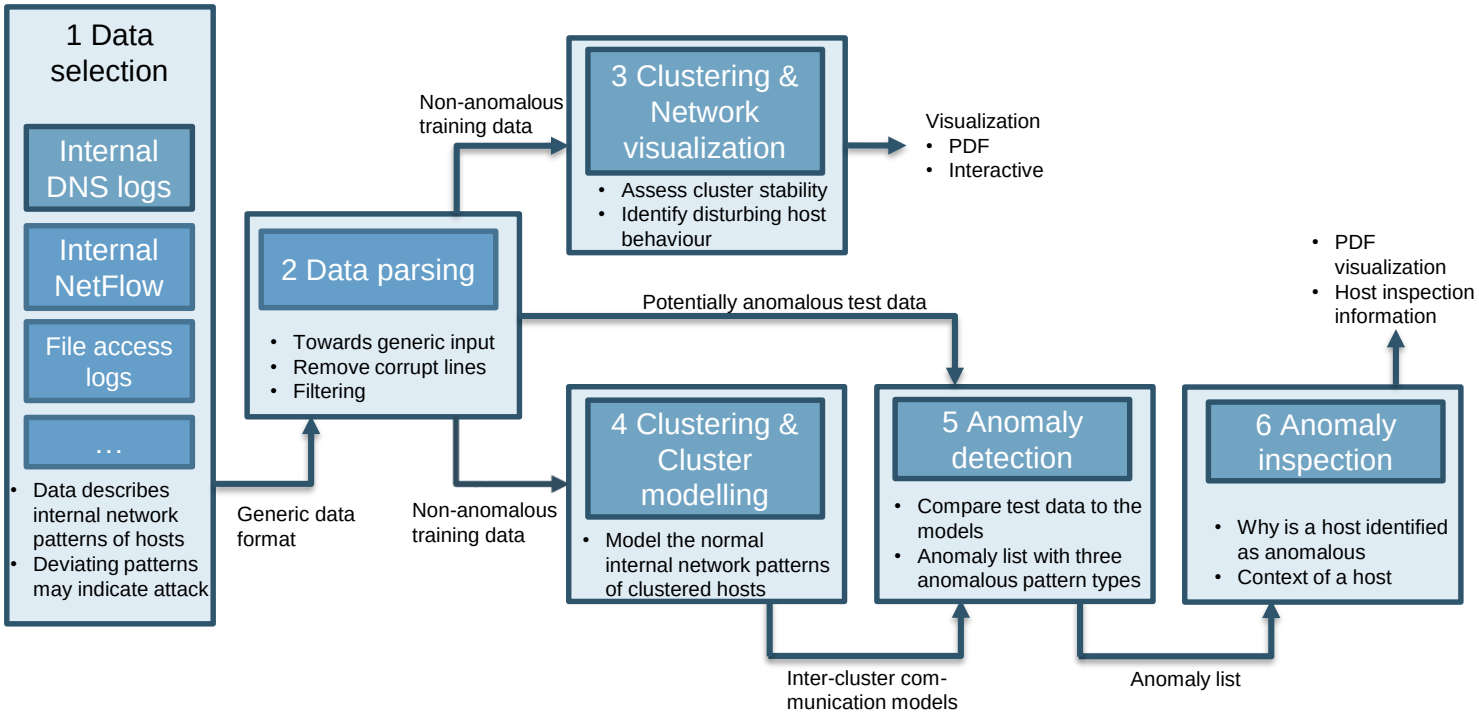
Img	Type of intrusion
(b)	**Probing hosts for vulnerabilities** Seen in Flame, Duqu, Stuxnet
(c)	**Peer-to-peer C&C channel** Seen in Duqu
(d)	**Peer-to-peer threat update** Seen in Stuxnet
(e)	**Local proxies to steal intelligence** Seen in Flame
(f)	**Staging server (gathers intelligence)** Seen in Duqu

IDEA: LOOK AT CLUSTERS OF HOSTS

- Individual host behave relatively unpredictable
- Groups of hosts often behave similarly
- Determine normal behaviour per cluster
  - Observe when individual host deviates
- Group hosts that often communicate with each other using
  community clustering
  - **More robust to minor changes**
  - **More efficient**



PROCESS STEPS OF ANOMALY BASED CLUSTERING

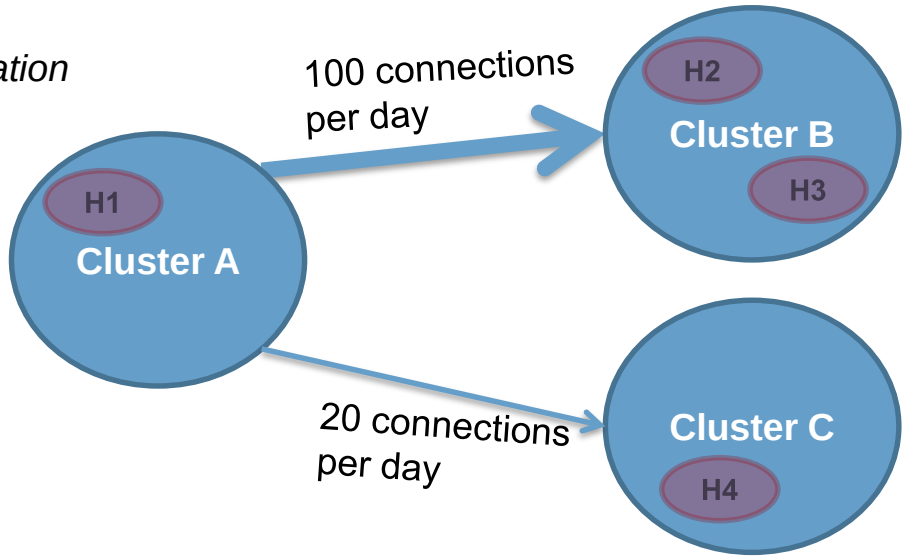


CLUSTERING & CLUSTER MODELLING

MODELLING THE INTER-CLUSTER COMMUNICATION BEHAVIOUR

- After community clustering, each host is within a cluster
- Cluster modelling:
  Each cluster has its own *inter-cluster communication model* based on a statistical analysis
  - Communications within a community cluster are considered normal
  - Communications between different community clusters are modelled

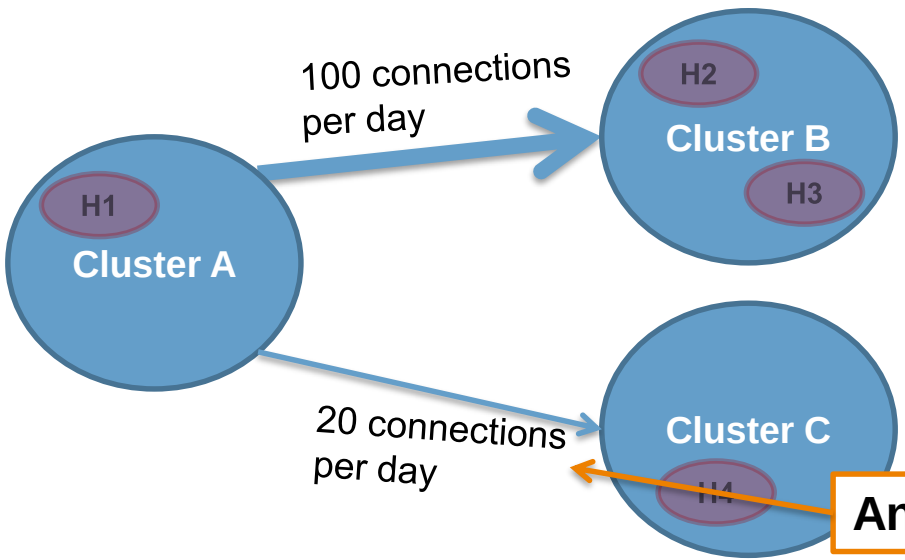
Example of a simplified inter-cluster communication model



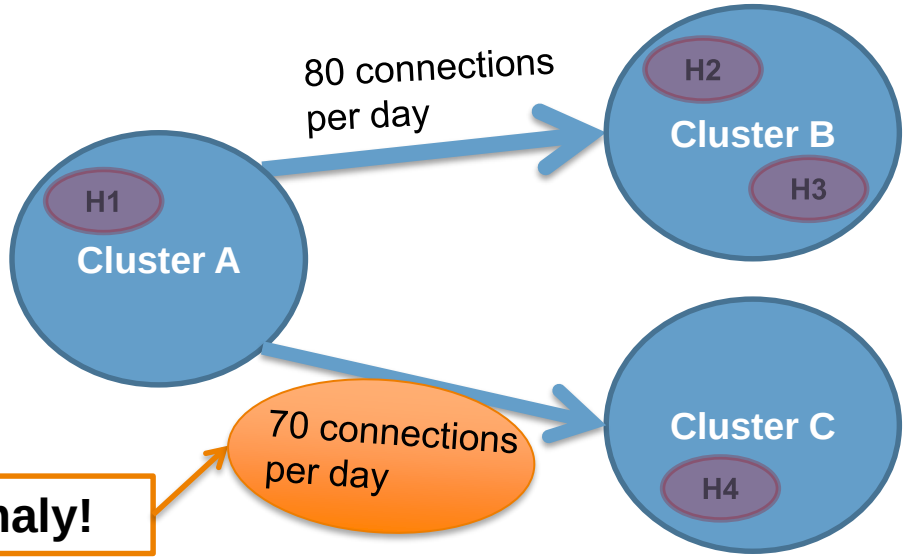
CLUSTERING & CLUSTER MODELLING

MODELLING THE INTER-CLUSTER COMMUNICATION BEHAVIOUR

Example of a simplified inter-cluster communication model



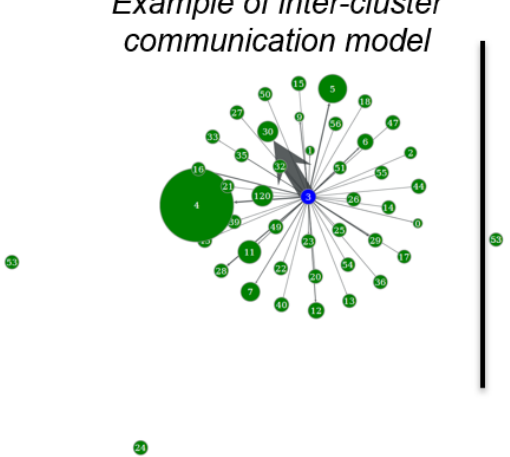
Example of anomalous host behaviour



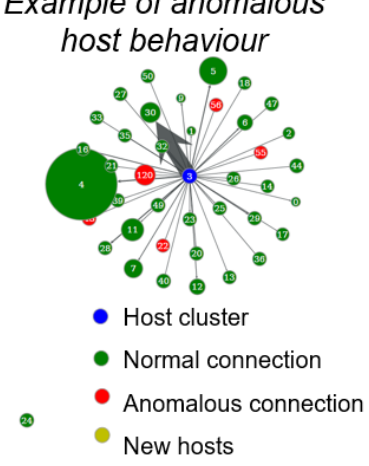
ANOMALY INSPECTION
ZOOMING INTO BEHAVIOUR OF AN ANOMALOUS HOST

- Visualizations of the cluster communication model and the behaviour of the anomalous host indicate **why the host is identified as anomalous**

Example of inter-cluster communication model



Example of anomalous host behaviour



CONCLUSIONS AND TAKEAWAYS

- **Internal network traffic:**
  - Valuable source of information for targeted attack detection
- **Behavioural based clustering techniques:**
  - Improve anomaly detection algorithms

THANK YOU FOR YOUR ATTENTION

TNO innovation for life

Contact:
Irina Chiscop, Scientist Innovator
irina.chiscop@tno.nl