Using BRO to tattle on other tools

Patrick Cain

The Cooper-Cain Group. Inc.

pcain@coopercain.com

(@BC @APWG)

Using ~~BRO~~ ZEEK to tattle on other tools

Patrick Cain

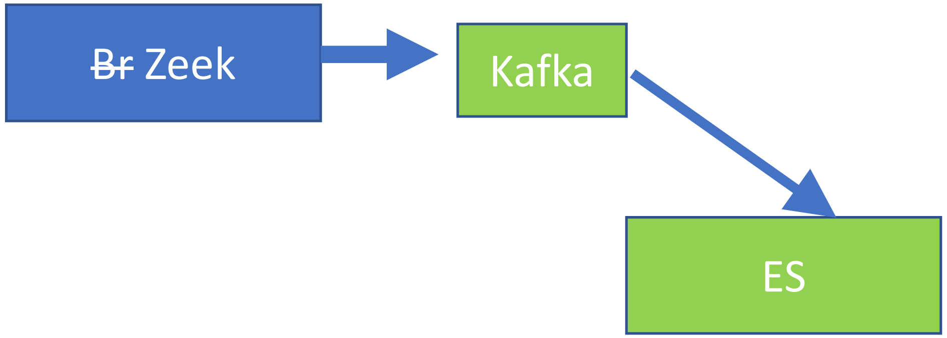
The Cooper-Cain Group. Inc.

pcain@coopercain.com

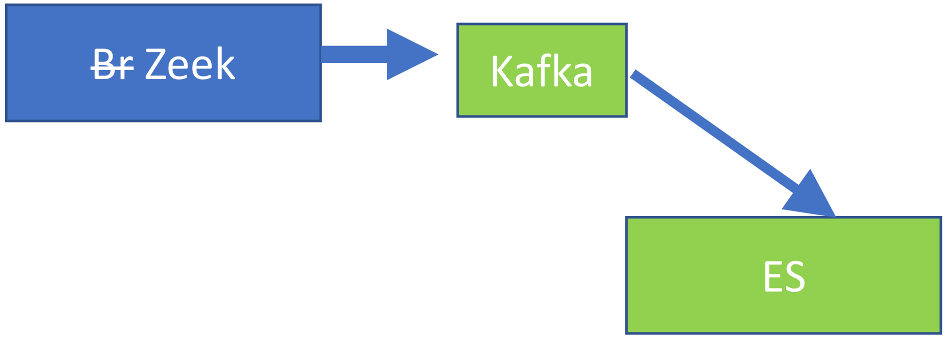
(@BC @APWG)

I don’t do BIG data, I do LARGE data!

A hypotethical environment…



An environment…

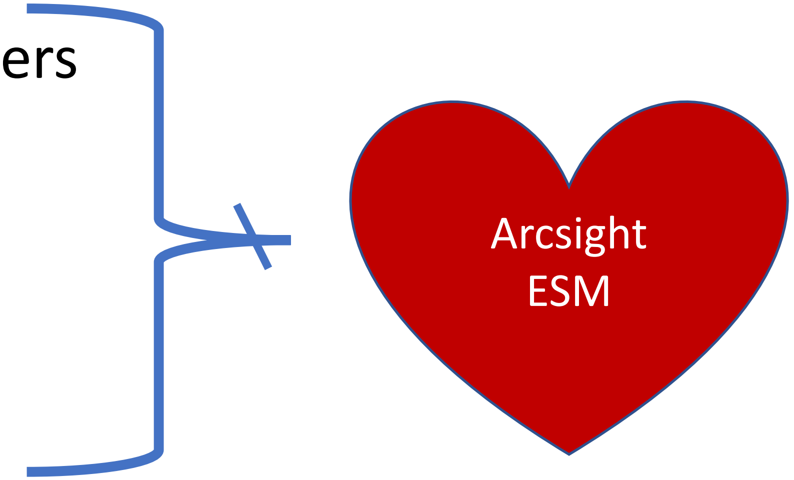


~~Br~~ Zeek

Kafka

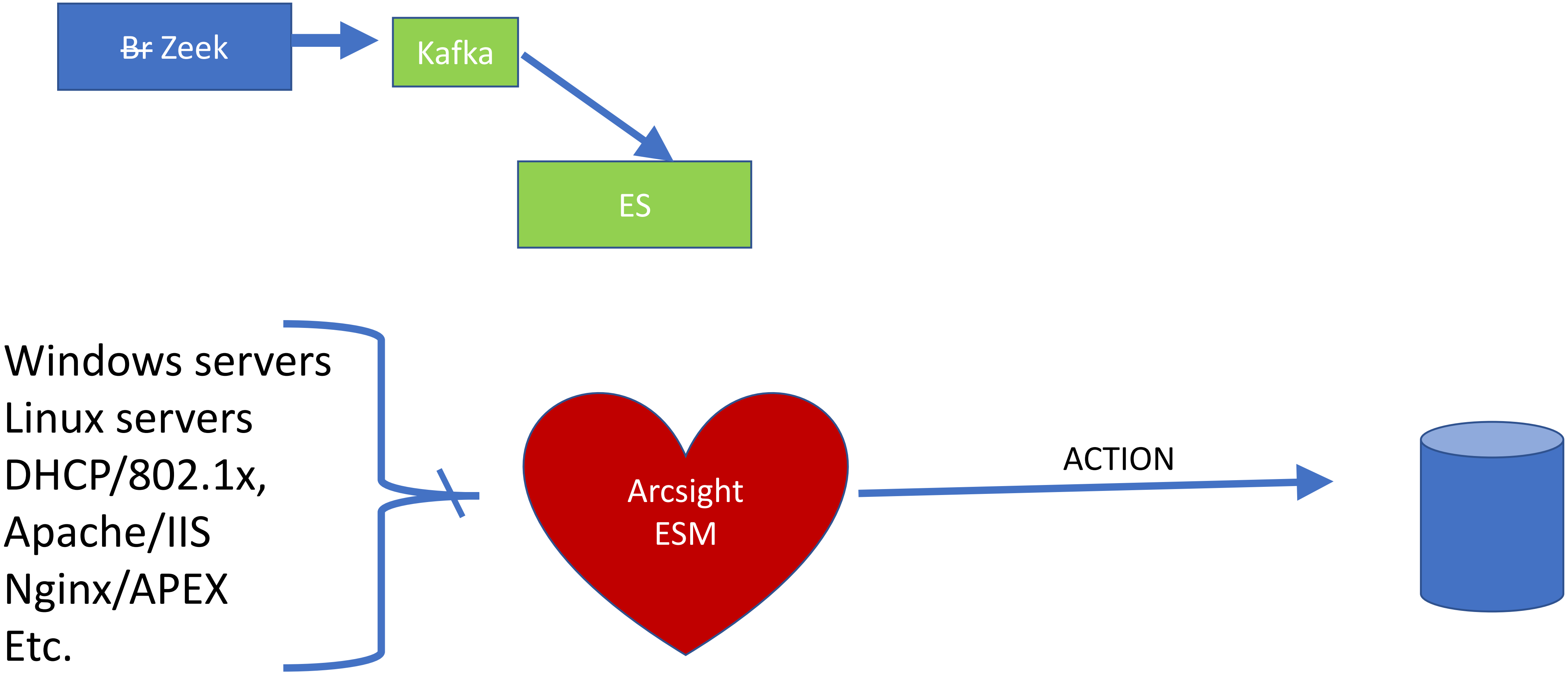
ES

Windows servers
Linux servers
DHCP/802.1x,
Apache/IIS
Nginx/APEX
Etc.



Arcsight
ESM

An environment…



~~Br~~ Zeek

Kafka

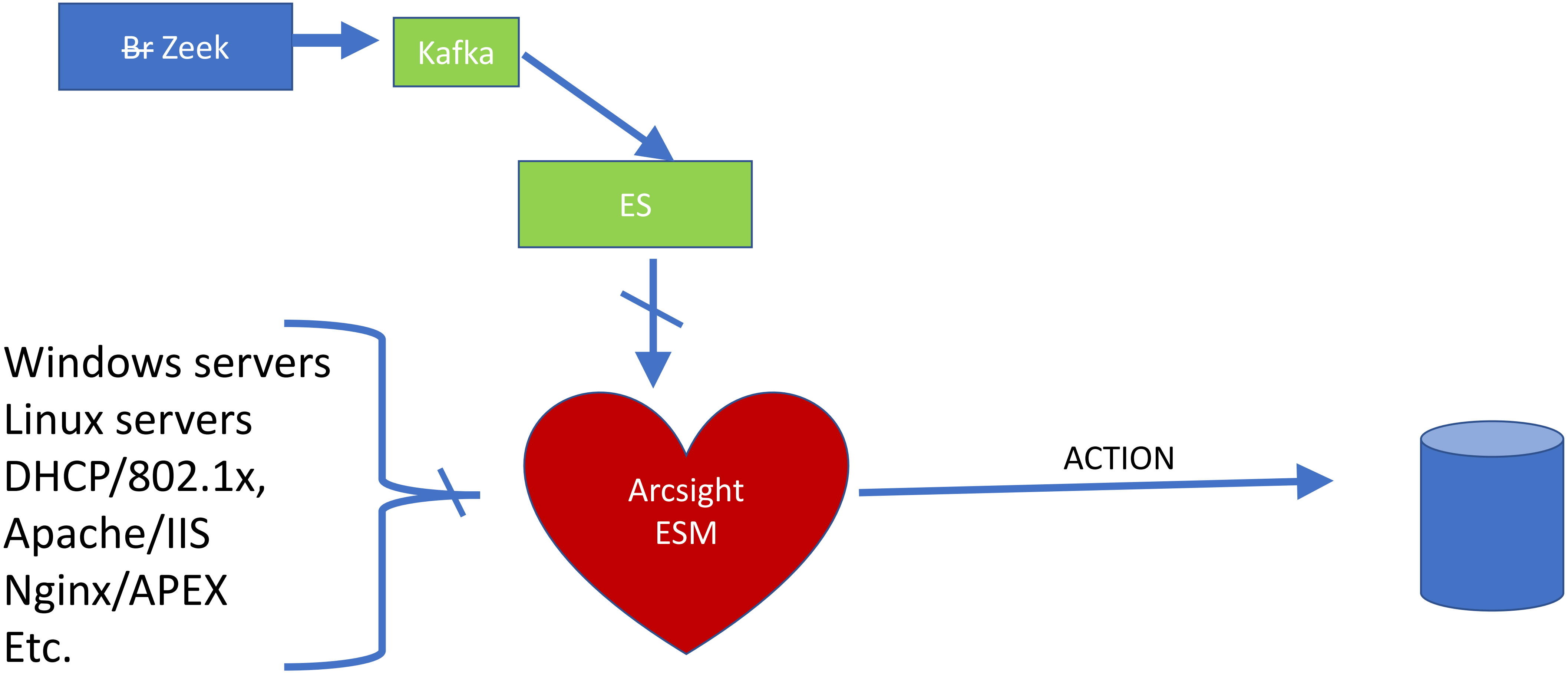
ES

Windows servers
Linux servers
DHCP/802.1x,
Apache/IIS
Nginx/APEX
Etc.

Arcsight
ESM

ACTION

An environment…



~~Br~~ Zeek

Kafka

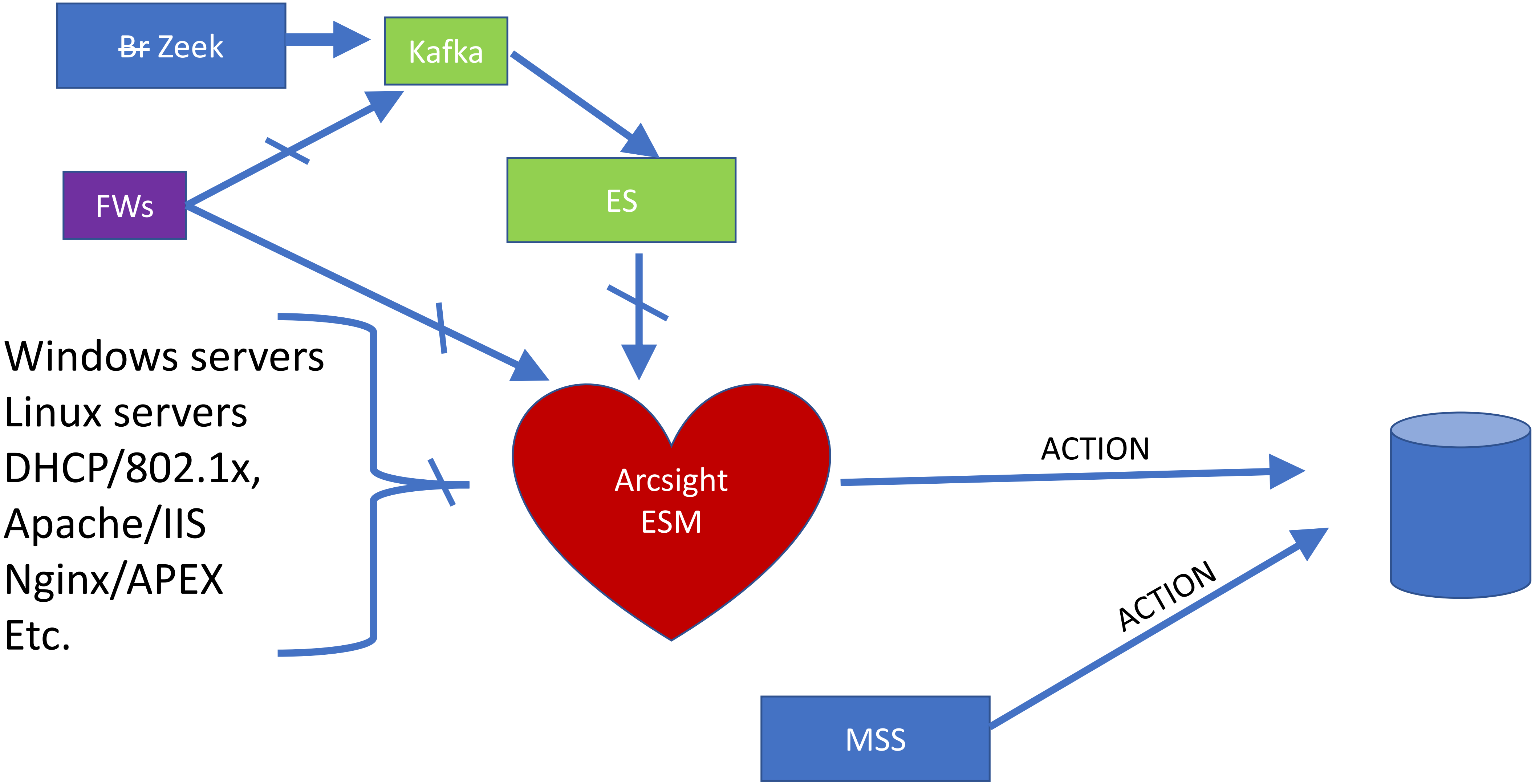
ES

Windows servers
Linux servers
DHCP/802.1x,
Apache/IIS
Nginx/APEX
Etc.

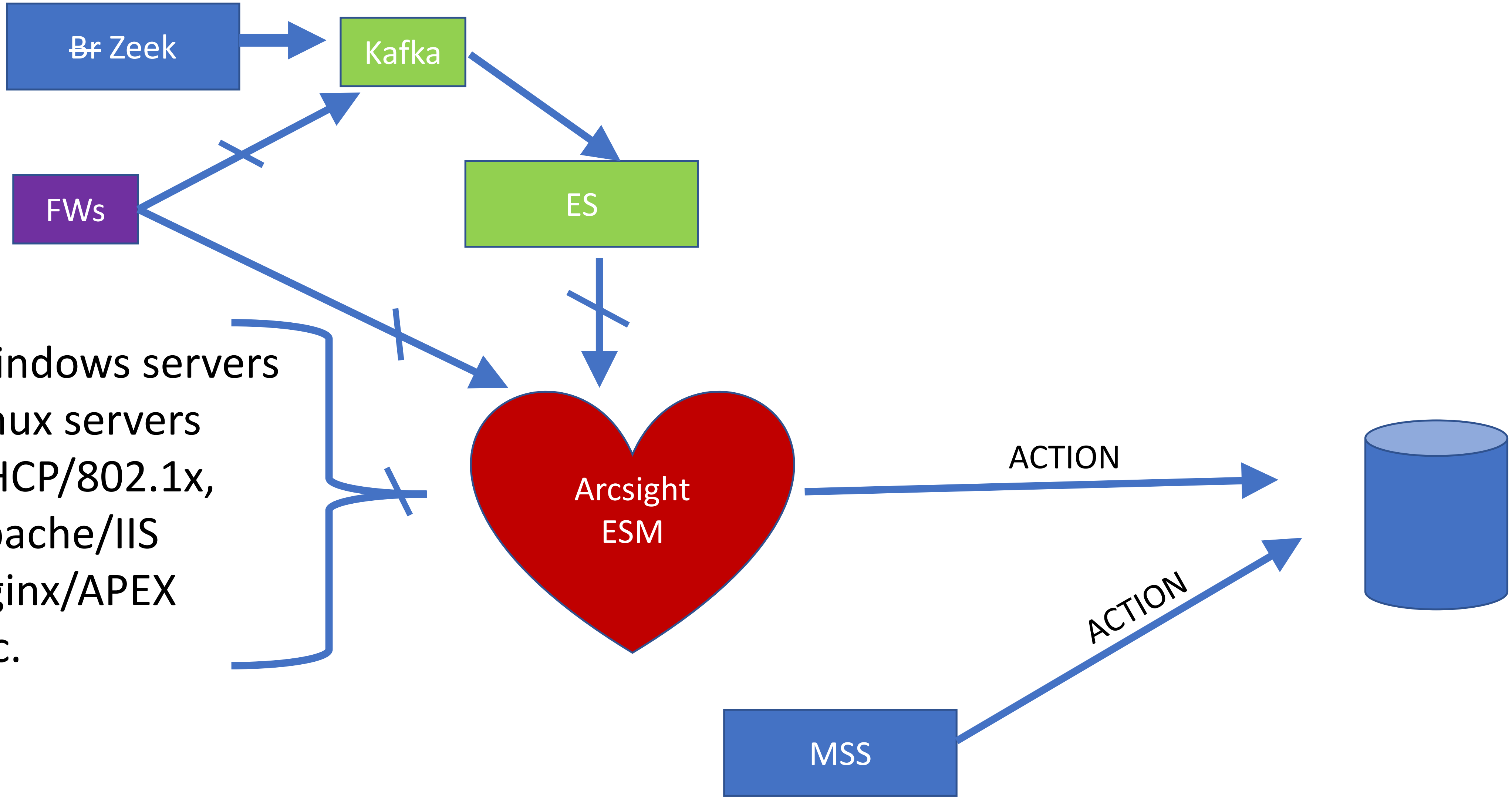
Arcsight
ESM

ACTION

An environment…



An environment…



Normal Event ‘flow’

- Taps feed ~~br~~ zeek
- Zeek feeds elasticsearch (ES) via a kafka buffer
- Analyst can search in ES using kibana
- ES sends filtered things to the SIEM
- SIEM does correlation, add user detail, etc
  - No sense in rebuilding the SIEM
- SIEM alerts on “bad things” and sends alert to tix

We have an MSSP, too

- “they will watch stuff as we sleep” ☹
- They run snort; we get tickets when they see “stuff”
- Snort is uni-directional; there are a lot of false positives in “stuff”

We have an MSSP, too

- “they will watch stuff as we sleep” ☺
- They run snort; we get tickets when they see “stuff”
- Snort is uni-directional; there are a lot of false positives in “stuff”
- We wrote a script to log into their ticketing system:
  1. Grab IP, port, timestamp
  2. Search ES for the zeek conn log
  3. If connection not blocked -> generate a ticket for us.
  4. If port is 80 and http_resoonse is 200 -> generate a ticket to us.
  5. Else, close vendor ticket

We have an MSSP, too

- “they will watch stuff as we sleep” ☺
- They run snort; we get tickets when they see “stuff”
- Snort is uni-directional; there are a lot of false positives in “stuff”
- We wrote a script to log into their ticketing system:
  1. Grab IP, port, timestamp
  2. Search ES for the zeek conn log
  3. If connection not blocked -> generate a ticket for us.
  4. If port is 80 and http_resoonse is 200 -> generate a ticket to us.
  5. Else, close vendor ticket

We have an MSSP, too

- “they will watch stuff as we sleep” ☺
- They run snort; we get tickets when they see “stuff”
- Snort is uni-directional; there are a lot of false positives in “stuff”
- We wrote a script to log into their ticketing system:
    1. Grab IP, port, timestamp
    2. Search ES for the zeek conn log
    3. If connection not blocked -> generate a ticket for us.
    4. If port is 80 and http_response is 200 -> generate a ticket to us.
    5. Else, close vendor ticket

We have an MSSP, too

- “they will watch stuff as we sleep” ☺
- They run snort; we get tickets when they see “stuff”
- Snort is uni-directional; there are a lot of false positives in “stuff”
- We wrote a script to log into their ticketing system:
  1. Grab IP, port, timestamp
  2. Search ES for the zeek conn log
  3. If connection not blocked -> generate a ticket for us.
  4. If port is 80 and http_response is 200 -> generate a ticket to us.
  5. Else, close vendor ticket

We’re slowly adding new things

- Hey! We run snort, too!
- Let’s verify other snort alerts
    - Did the RDP actually succeeed? (Nope -> blocked at FW)
    - Was the remote shell attempt successful? (# bytes in conn.log)
    - Did the exploit actually succeed?

We’re slowly adding new things

- Hey! We run snort, too!
- Let’s verify other snort alerts
  - Did the RDP actually succeeed? (Nope -> blocked at FW)
  - Was the remote shell attempt successful? (# bytes in conn.log)
  - Did the exploit actually succeed?
- Put zeek behind the F5 (SSL-decryptor)
  - Did bad stuff seen in decrypted traffic hit other servers encrypted?
    - Zeek to the rescue.

We’re slowly adding new things

- Hey! We run snort, too!
- Let’s verify other snort alerts
  - Did the RDP actually succeeed? (Nope -> blocked at FW)
  - Was the remote shell attempt successful? (# bytes in conn.log)
  - Did the exploit actually succeed?
- Put zeek behind the F5 (SSL-decryptor)
  - Did bad stuff seen in decrypted traffic hit other servers encrypted?
    - Zeek to the rescue.

We’re slowly adding new things

- Hey! We run snort, too!
- Let’s verify other snort alerts
  - Did the RDP actually succeed? (Nope -> blocked at FW)
  - Was the remote shell attempt successful? (# bytes in conn.log)
  - Did the exploit actually succeed?
- Put zeek behind the F5 (SSL-decryptor)
  - Did bad stuff seen in decrypted traffic hit other servers encrypted?
    - Zeek to the rescue.
- Can we skim 10% off the coin miner traffic?
    - Keep tuition low ☺

We’re slowly adding new things

- Hey! We run snort, too!
- Let’s verify other snort alerts
  - Did the RDP actually succeed? (Nope -> blocked at FW)
  - Was the remote shell attempt successful? (# bytes in conn.log)
  - Did the exploit actually succeed?
- Put zeek behind the F5 (SSL-decryptor)
  - Did bad stuff seen in decrypted traffic hit other servers encrypted?
    - Zeek to the rescue.
- Can we skim 10% off the coin miner traffic?
    - Keep tuition low ☺

Always looking for more ideas ☺

Pat Cain

pcain@coopercain.com