TEMET
end-to-end IT security

Cyber Threat Defense

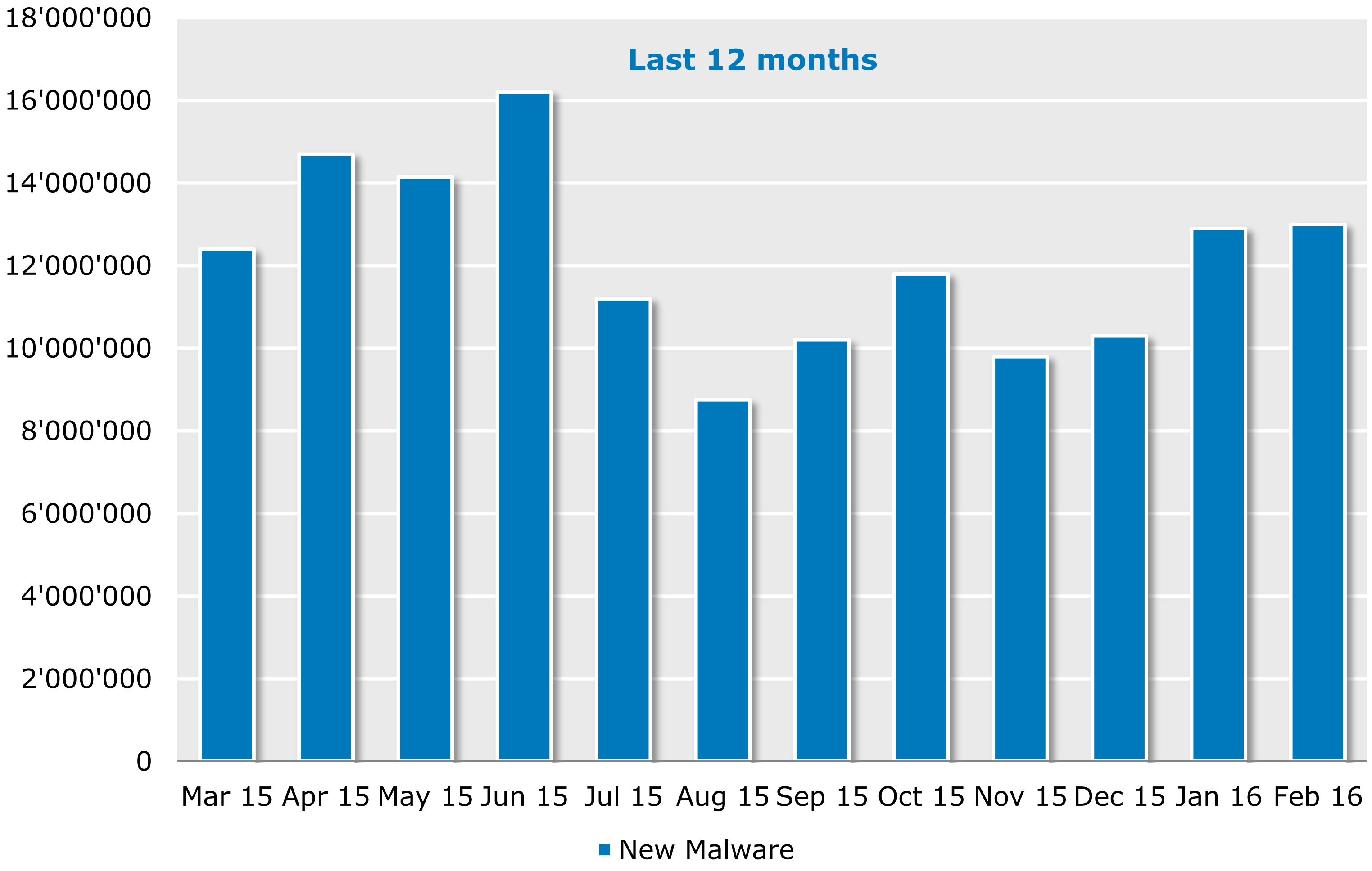
SIGS Afterwork, Basel

Dr. Alex Rhomberg, Partner TEMET AG

April 5, 2016

Cyber crime statistics

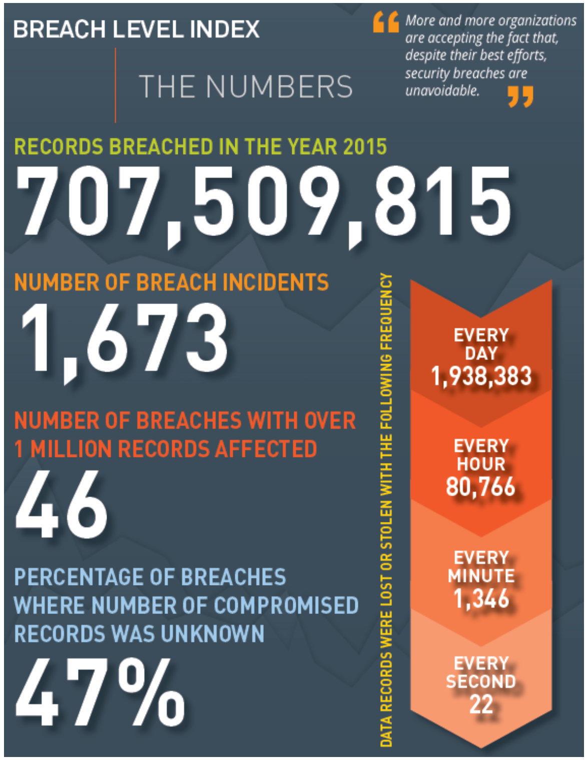
390’000 new malware samples every day!



Source: AV-Test GmbH, www.av-test.org

Cyber crime statistics

Breach Level Index 2015 (1/2)



BREACH LEVEL INDEX

THE NUMBERS

“More and more organizations are accepting the fact that, despite their best efforts, security breaches are unavoidable.”

RECORDS BREACHED IN THE YEAR 2015

707,509,815

NUMBER OF BREACH INCIDENTS

1,673

NUMBER OF BREACHES WITH OVER 1 MILLION RECORDS AFFECTED

46

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

47%

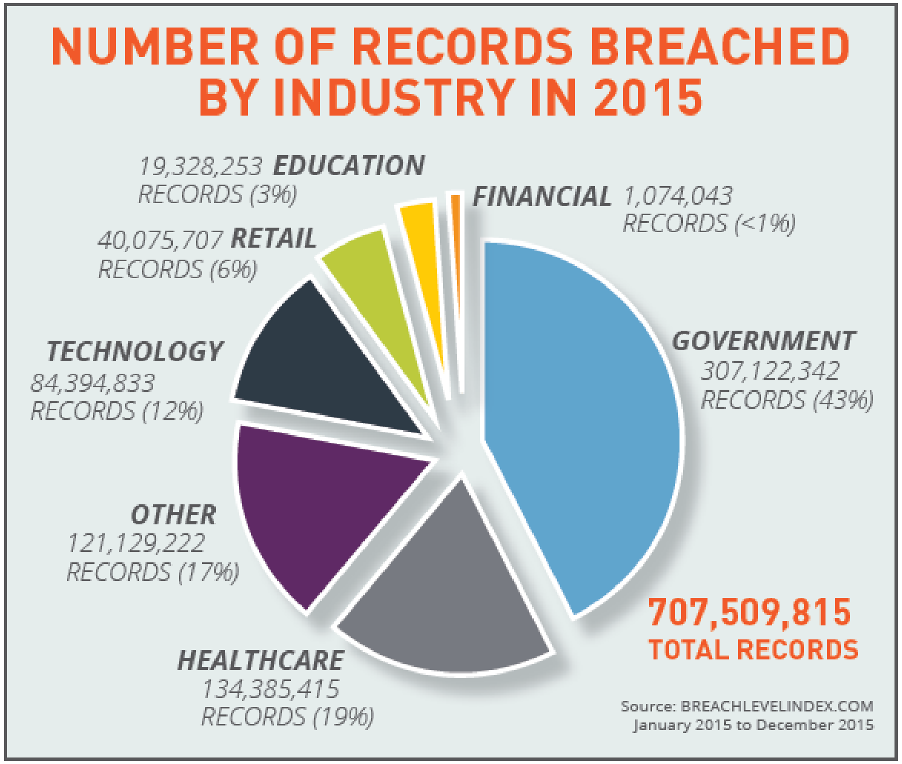
DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY 1,938,383

EVERY HOUR 80,766

EVERY MINUTE 1,346

EVERY SECOND 22

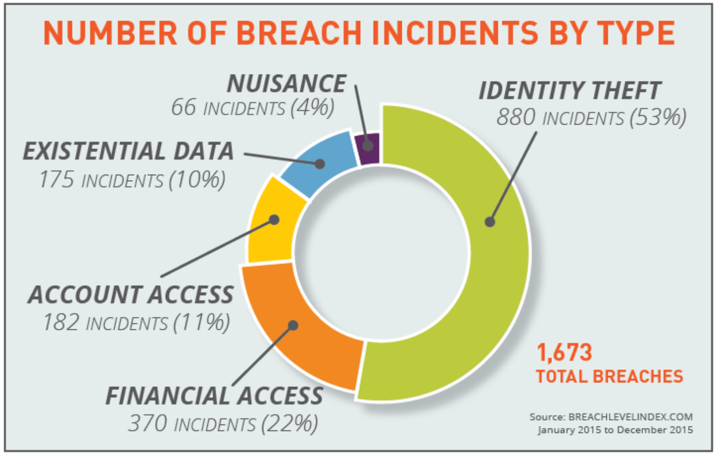


http://fr.sitestat.com/gemalto/gemalto/s?ent-Breach_Level_Index_Annual_Report_2015&ns_type=pdf

Source: Gemalto Breach Level Index Annual Report 2015

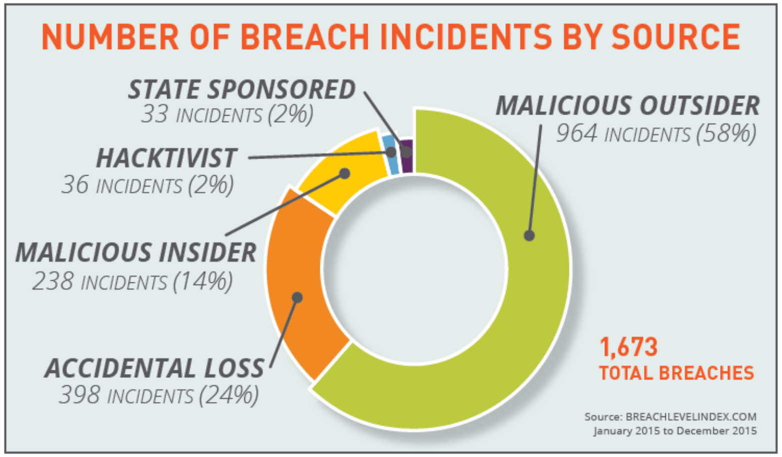
Cyber crime statistics

Breach Level Index 2015 (2/2)



NUMBER OF BREACH INCIDENTS BY TYPE

Source: BREACHLEVELINDEX.COM
January 2015 to December 2015



NUMBER OF BREACH INCIDENTS BY SOURCE

Source: BREACHLEVELINDEX.COM
January 2015 to December 2015

Source: Gemalto Breach Level Index Annual Report 2015

Know your adversaries

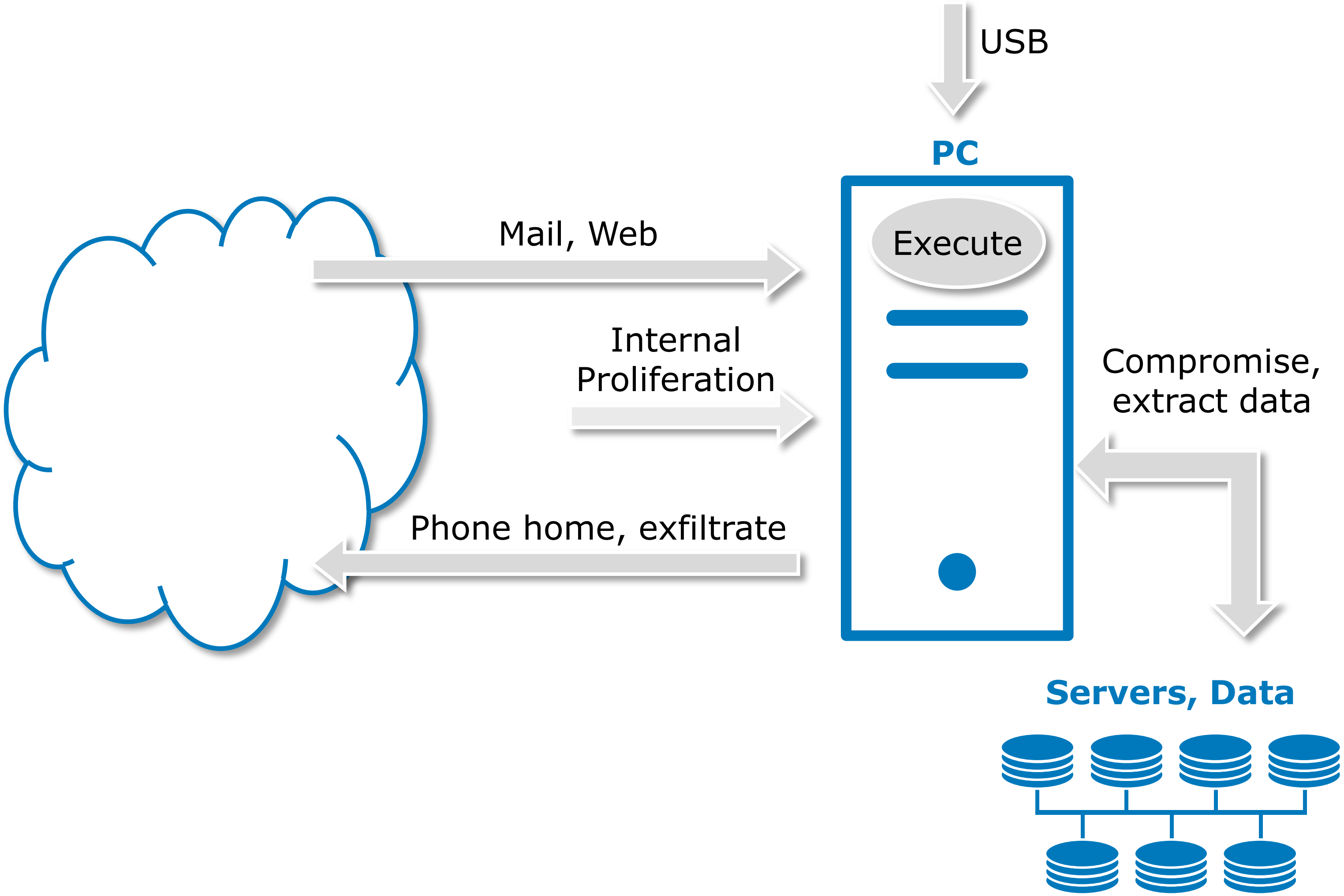
Cyber criminals: looking for a profit

- Extortion
- Selling data
- Money transfers
- Use processing power & bandwidth

Government agencies: Aiming for disruptive or military technology

Hacktivists: Avenge a perceived wrongdoing

Anatomy of an attack



Close the front door

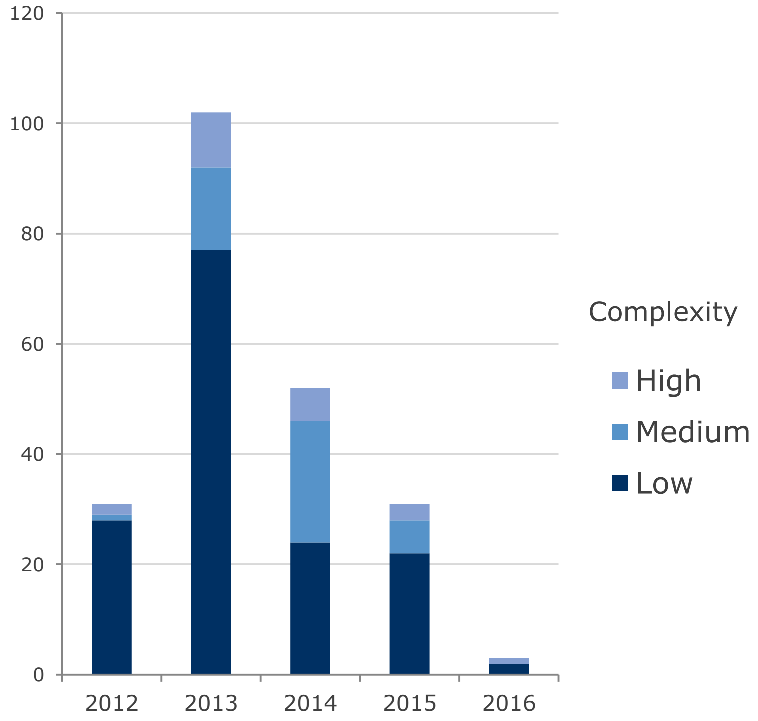
Lock down on file types

- Who needs to download executables?
- What are the common sources?
- What kind of mail attachments are really needed

Lock down on outdated technologies

- Java (in the browser) is obsolete and a constant source of pain. Why expose everyone?
- Examine and restrict other obsolete technologies, e.g. Silverlight, Flash in the near future

Java CVE score > 7



Close the front door

Examine your anti-virus strategy

- is your set-up up to speed?
- Does it incorporate new technologies your provider includes?
- Does the configuration follow best practice?

Additional technology?

- The baseline is the attack patterns you see, not the ones the product was built for
- Perform a PoC after closing the cheap vectors

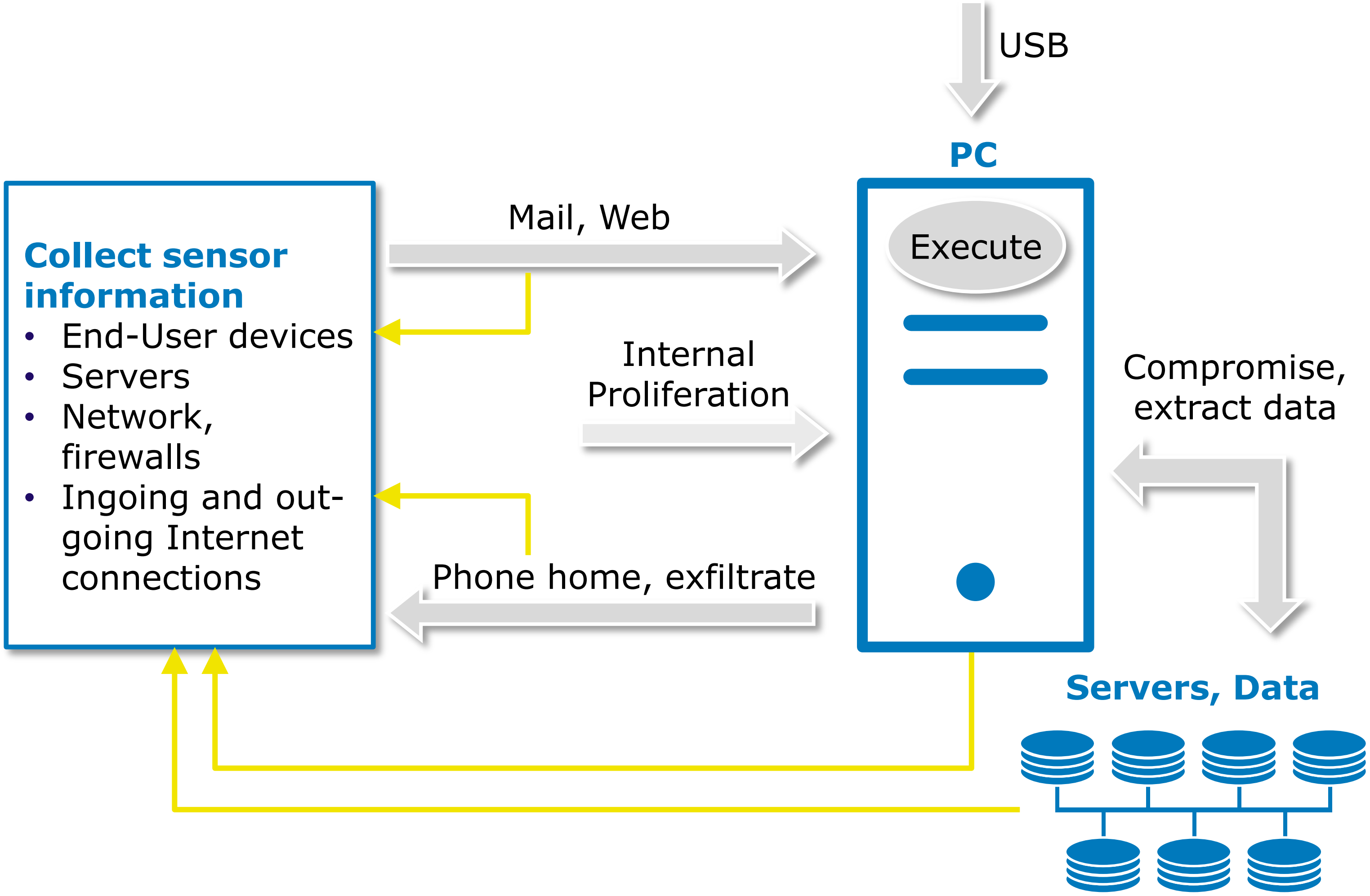
Minimize impact

Contain execution

Protect your assets

- Check your backups
- Check your recovery procedures
- Implement Access Management for end-user data
  - Implement access control on your file servers
- Implement Privileged Access Management
  - Need to do for privileged access
  - Use different credentials form admin rights

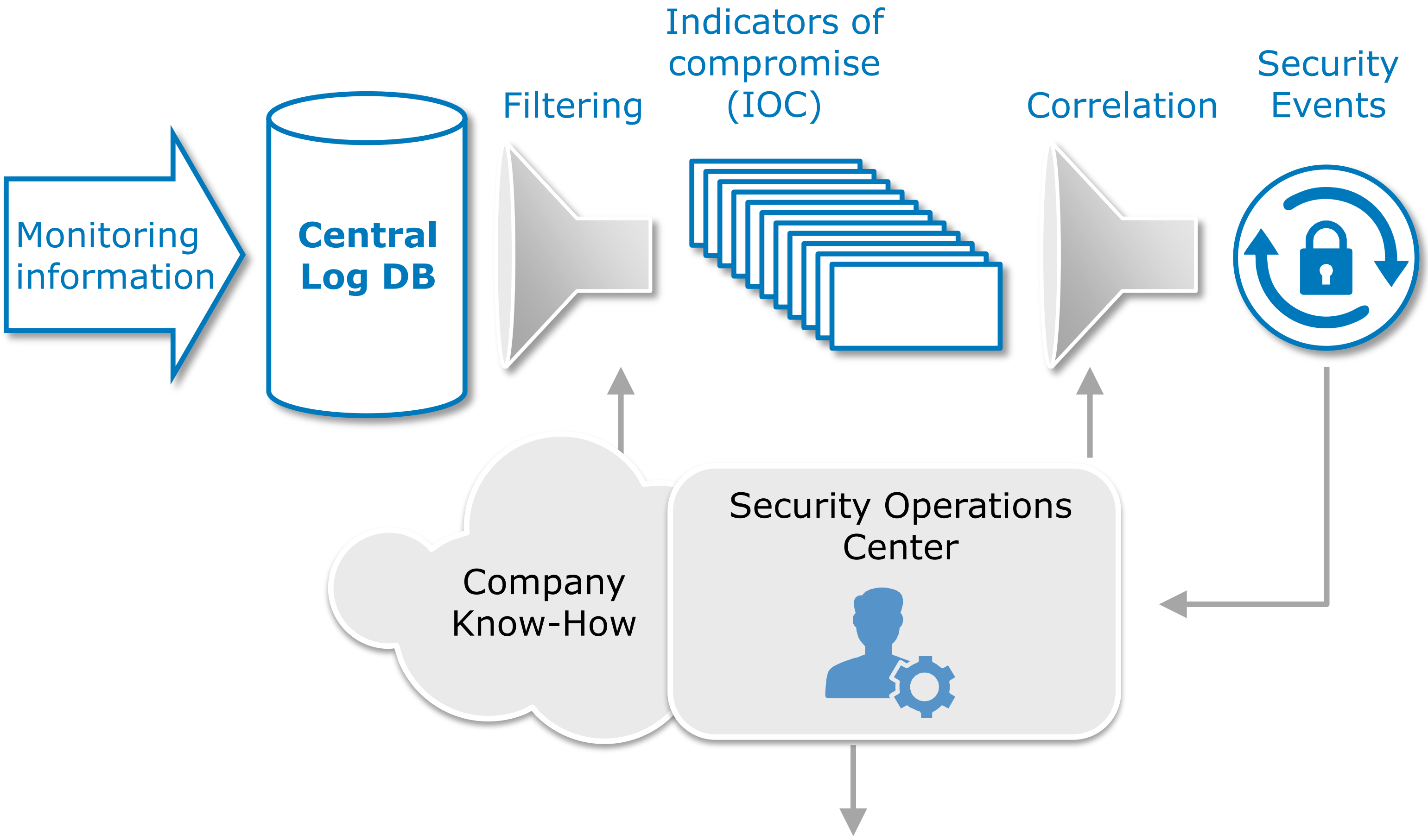
Monitor anomalies



Collect sensor information

- End-User devices
- Servers
- Network, firewalls
- Ingoing and out-going Internet connections

Monitor anomalies


Monitoring information

Central Log DB

Filtering

Indicators of compromise (IOC)

Correlation

Security Events

Company Know-How

Security Operations Center

- Analyze
- Respond
- Recover
- Improve filters

Summary

- Check your maturity in all areas
  - Infiltration
  - Execution
  - Containment
  - Monitoring

- Invest where maturity is lowest

- Did you close the simple stuff?