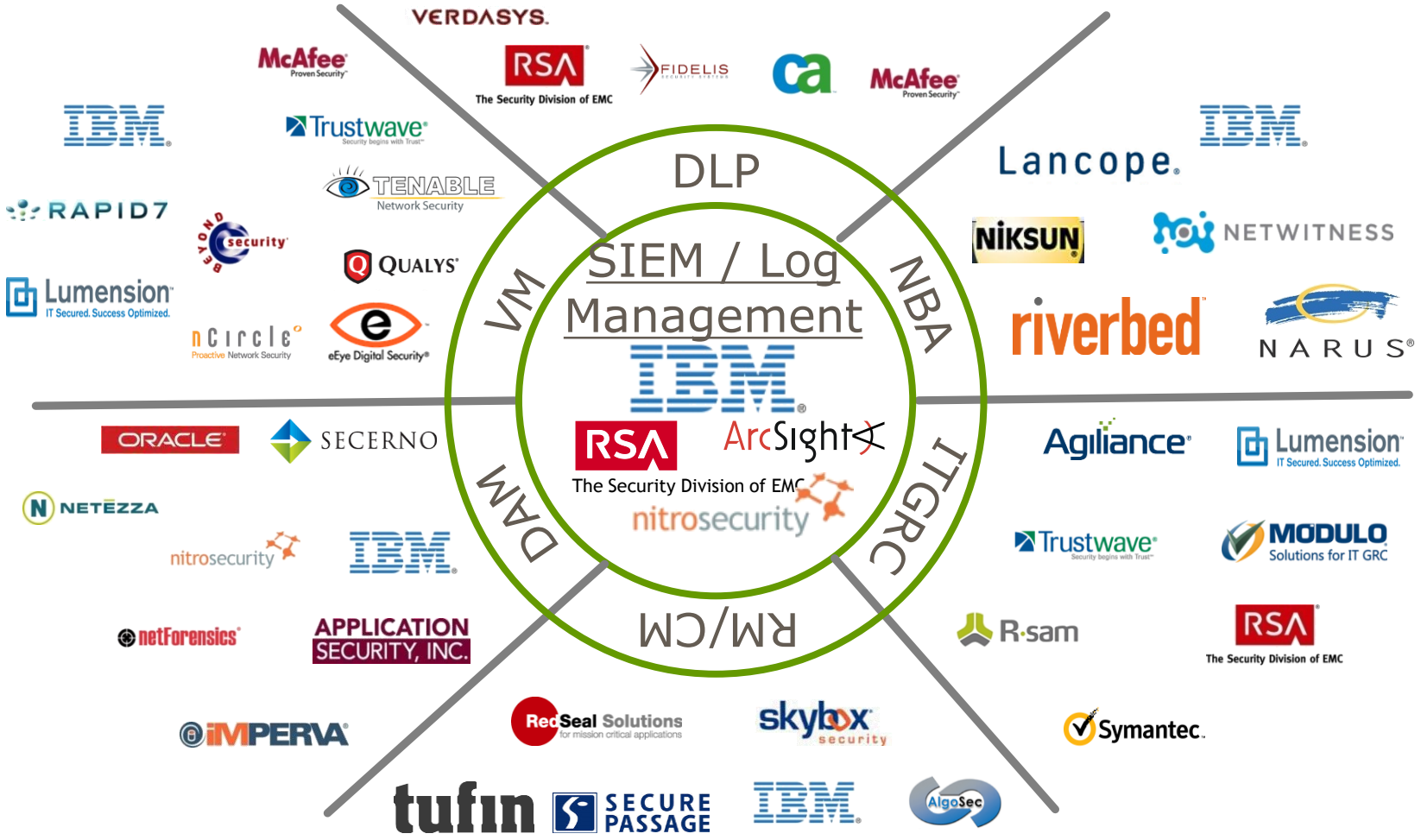
IT-Sikkerhet

For viktig for IT-avdelingen alene?

Paul-Christian Garpe CISSP CISA CCSK
pcg@pedab.no, 48 01 89 03
Pedab Norway

Til tross for mye teknologi...



...er knapt problemet løst

Hackere tok over Gje
nettsider
det

bedrifter har opplev
- Bare fem pr

til angrep mot
og Swedbank

Næringsministeren
sette i gang en felle

ANNE MELLINGSÆTER
24 | PUBLISERT: 07.NOV. 2015 13:13

Tapr
d

Statoil «kriget» med
hackere i tre dager

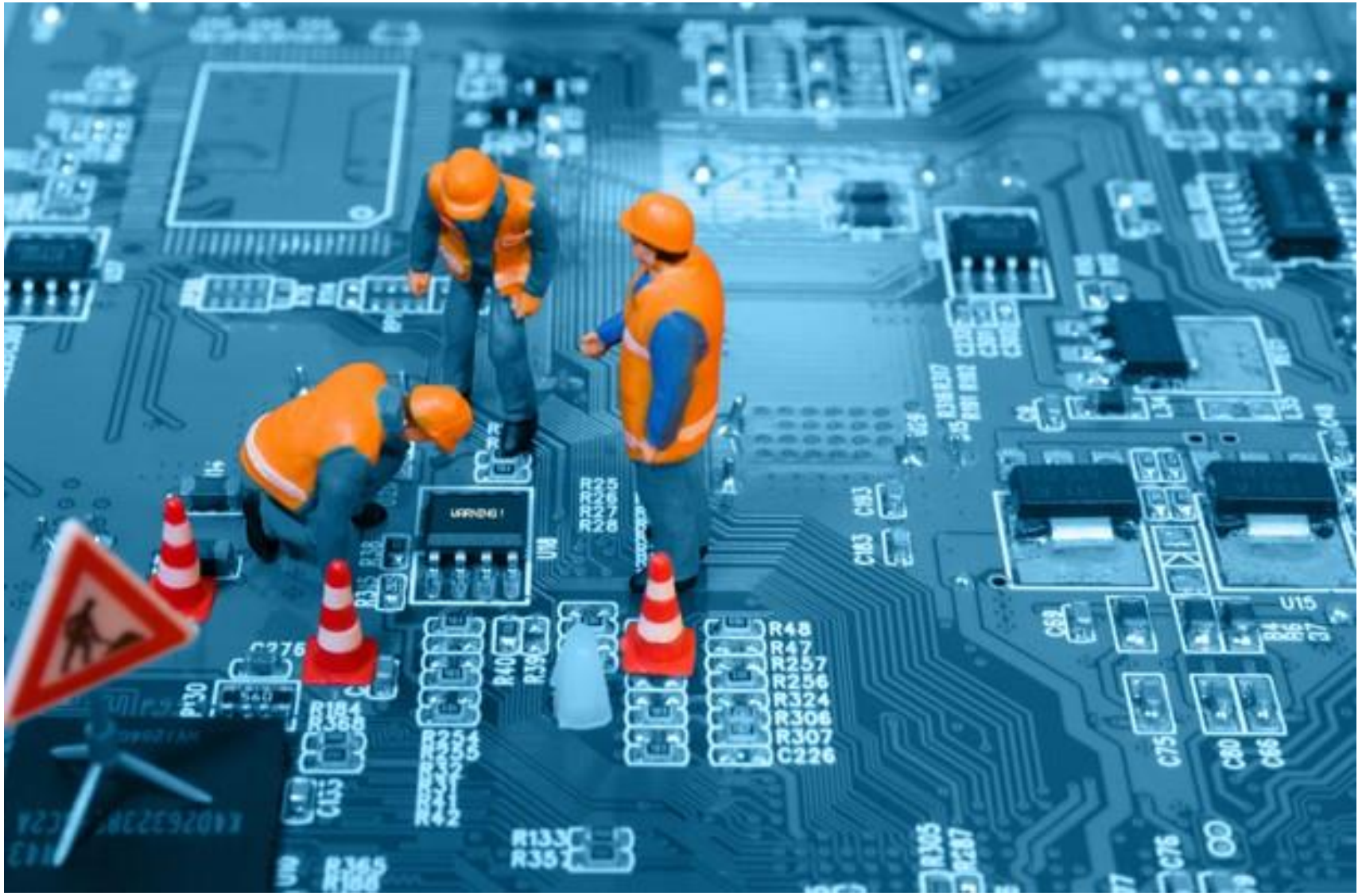
I tre dager ble Statoil utsatt for et av de mest alvorlige cyberangrepene noensinne.

e mot norsk
strigigant

DNB angrepet av hackere

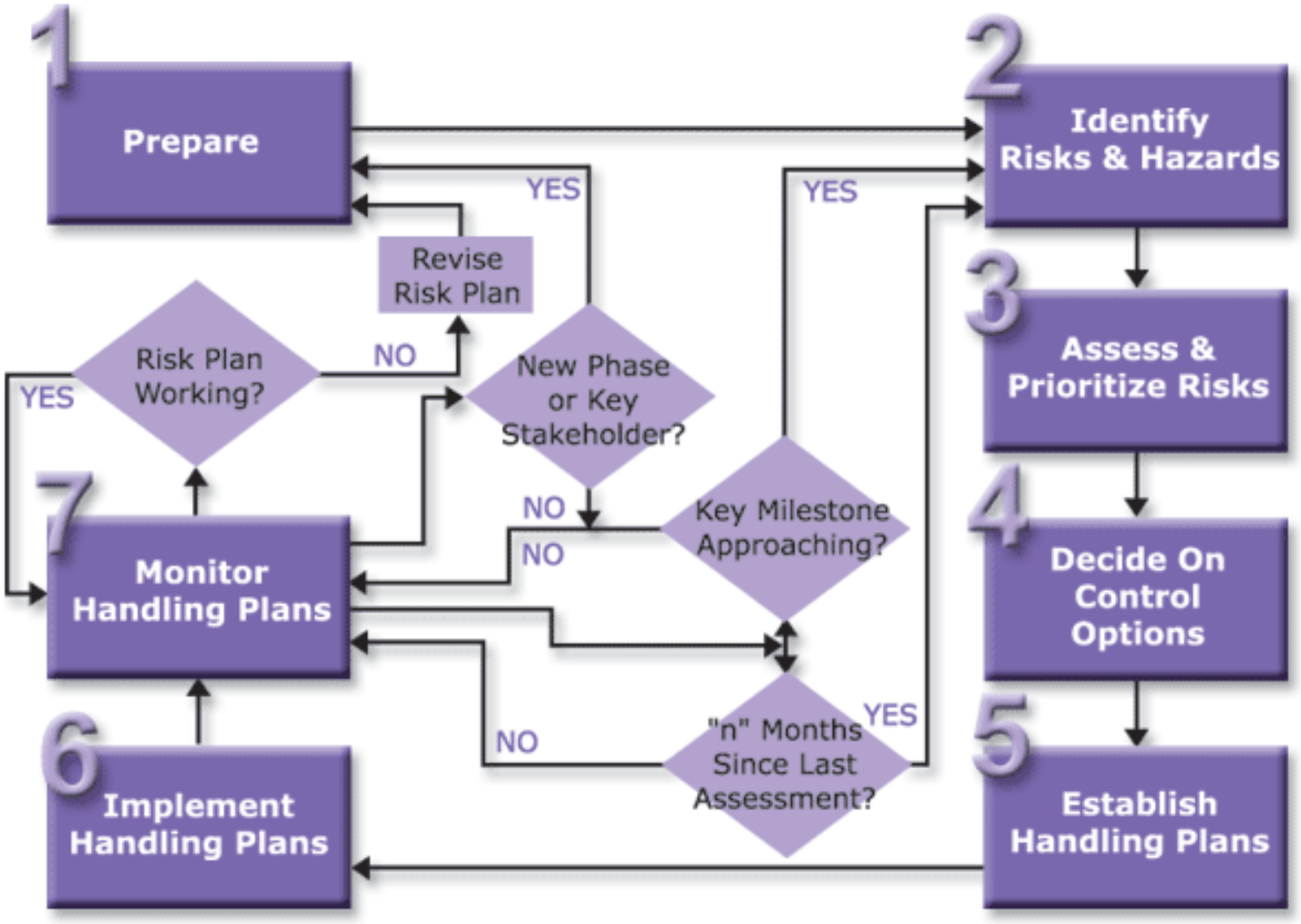
FELLES FRONT: Arne Røed Simonsen, fungerende direktør i Næringslivets Sikkerhetsråd, møtte næringsminister Monica Mæland tirsdag. Nå vil de få norske bedrifter til å våkne opp og beskytte seg mot dataangrep.

Konsekvenser for IT-avdelingen

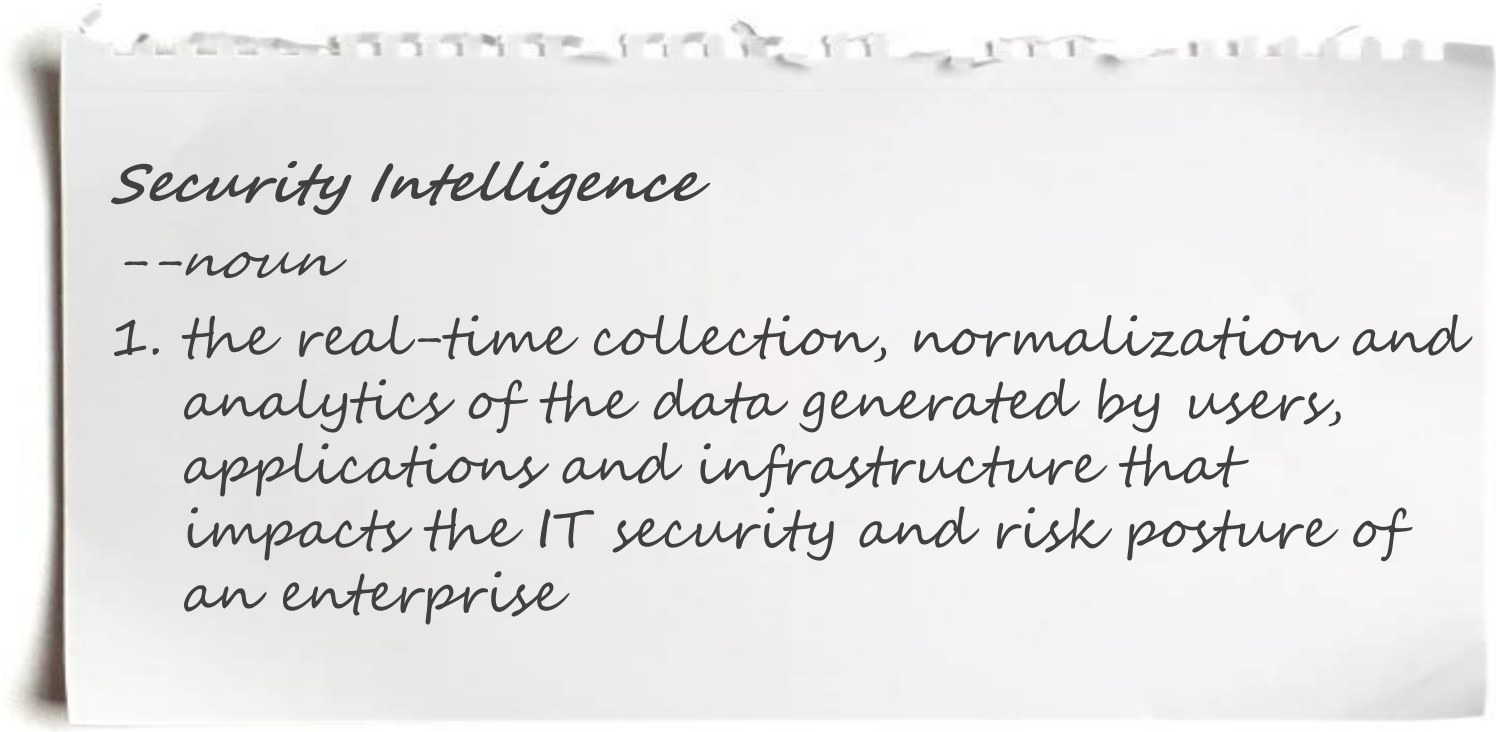


Risikoeier

Risiko- og sårbarhetsanalyse



Hva er Security Intelligence?



Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

“Hvorfor mer kontekst”

Organizations are failing at early breach detection, with more than 85% of breaches undetected by the breached organization.*

(…)

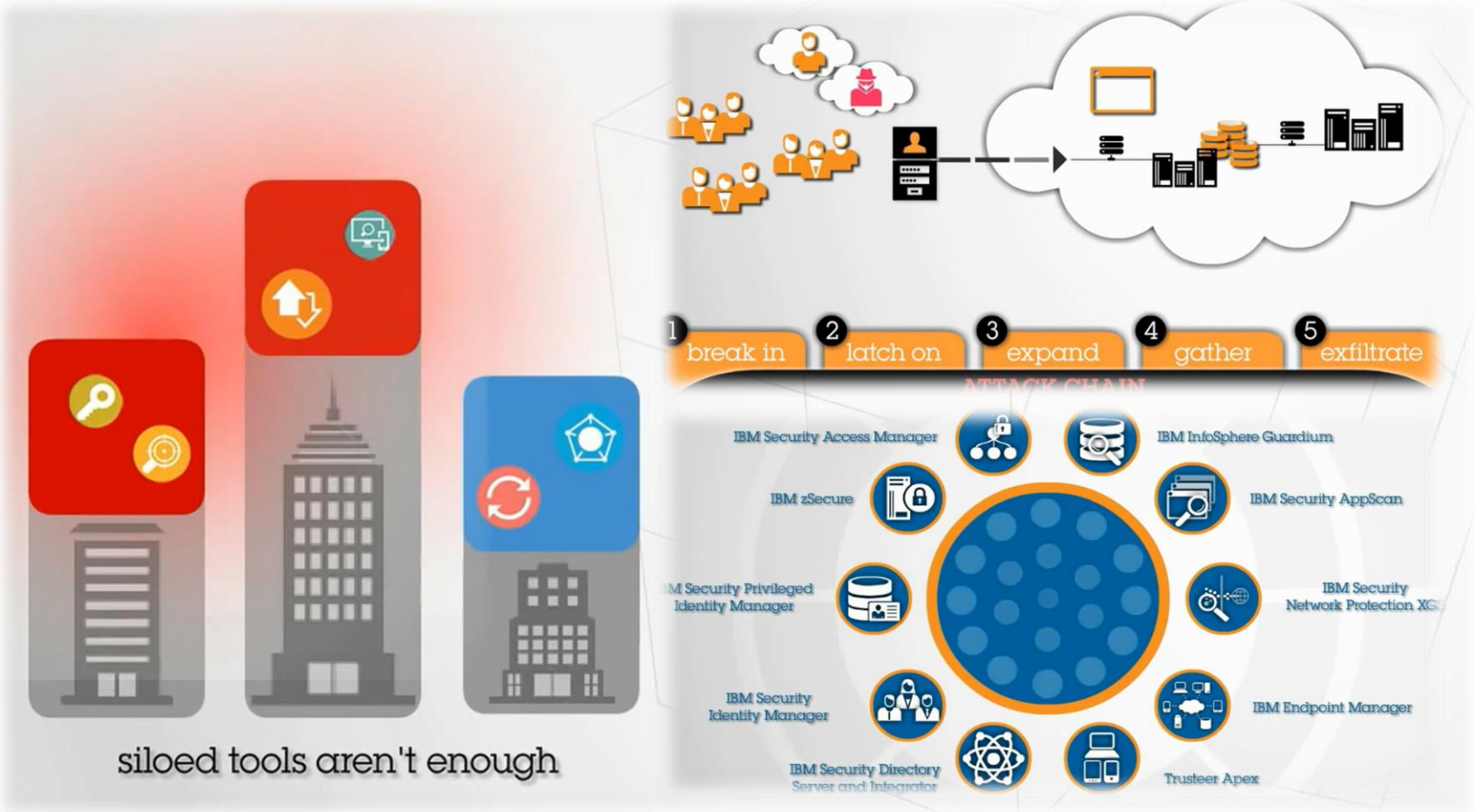
It is the **combination** of **real-time security monitoring**, **context** (threat, vulnerability, user, asset, data and application) and **"smart eyeballs"** on dally activity reports that will improve your chances of early breach detection beyond the current 15% success rate.

Gartner “Using SIEM for Targeted Attack Detection” (March 2012)

* 2011 Data Breach Investigations Report — Verizon Business Systems.

«Mer kontekst» betyr **integrasjon**

IBMs sikkerhetsløsninger tilbyr tett integrasjon og høy automatiseringsgrad. Dette utnyttes av kundene som driver bedre og mer effektivt sikkerhetsarbeid med mindre manuelt arbeid.



«Integrasjon» betyr **enklere** og **mer helhetlig**

Sikkerhetskompetanse og –bemanning henger etter:

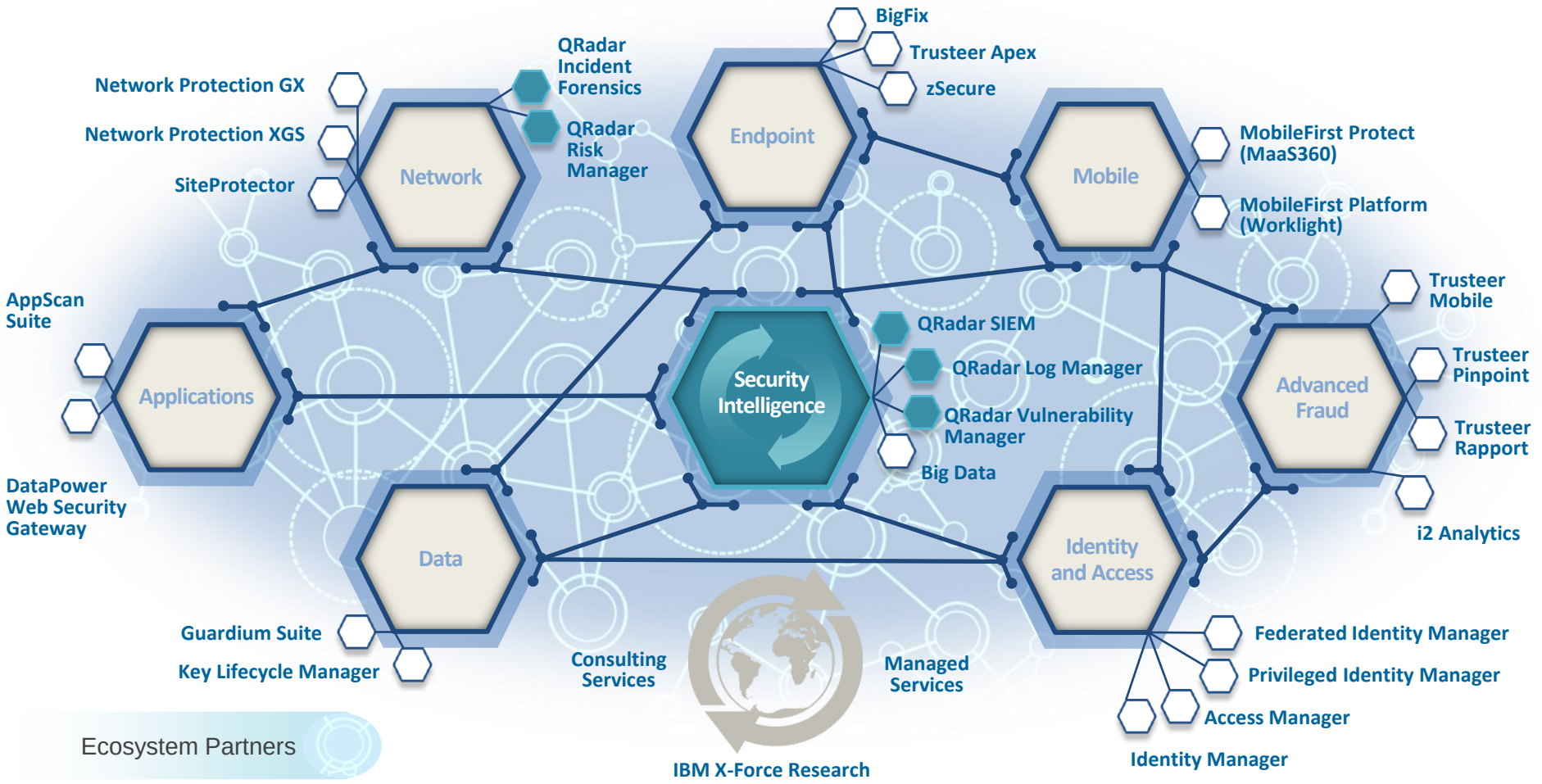
- *30% of organizations say that the network security skills of the infosec staff are inadequate in some, most, or all cases.*
- *44% of organizations say that the number of networking/security staff with strong knowledge in both security and networking technology is inadequate in some, most, or all cases.*
- *38% of organizations say that the ability of the security staff to keep up with network security changes is inadequate in some, most, or all cases.*
- *37% of organizations say that the ability of the security staff to keep up with the threat landscape is inadequate in some, most, or all cases.*
- *47% of organizations say that the number of employees dedicated to network security is inadequate in some, most, or all cases.*

Store virksomheter har segmentert nettverk, filtrert pakker, administrert brannvegger, IDS/IPS, nettverksproxies og ulike gateways i årevis. Til tross for denne erfaringen har de forblitt mer sårbare enn de burde vært, grunnet mangel på sikkerhetskompetanse.

Source: ESG research report “Network Security Trends in the Era of Cloud and Mobile Computing”

Etablèr sikkerhet som et system

IBM QRadar er midtpunktet



Løsninger for hele tidslinjen

Hva er de eksterne og interne truslene?

Er vi konfigurert for å beskytte mot disse truslene?

Hva skjer akkurat nå?

Hvilken skade skjedde?

Vulnerability — PREDICTION / PREVENTION PHASE — Exploit — REACTION / REMEDIATION PHASE — Remediation

Pre-Exploit

Post-Exploit

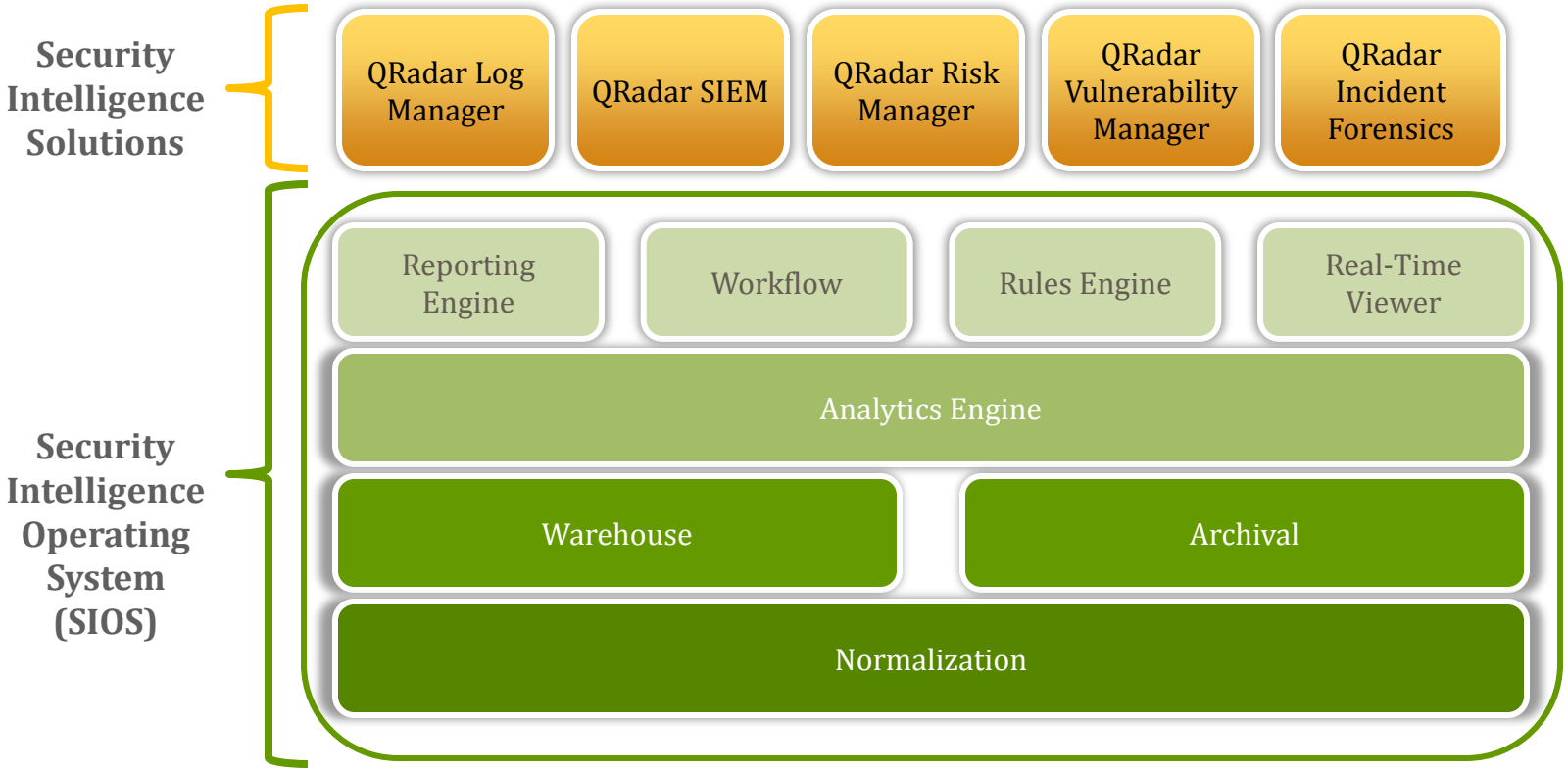
Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management.
Reporting and Scorecards.

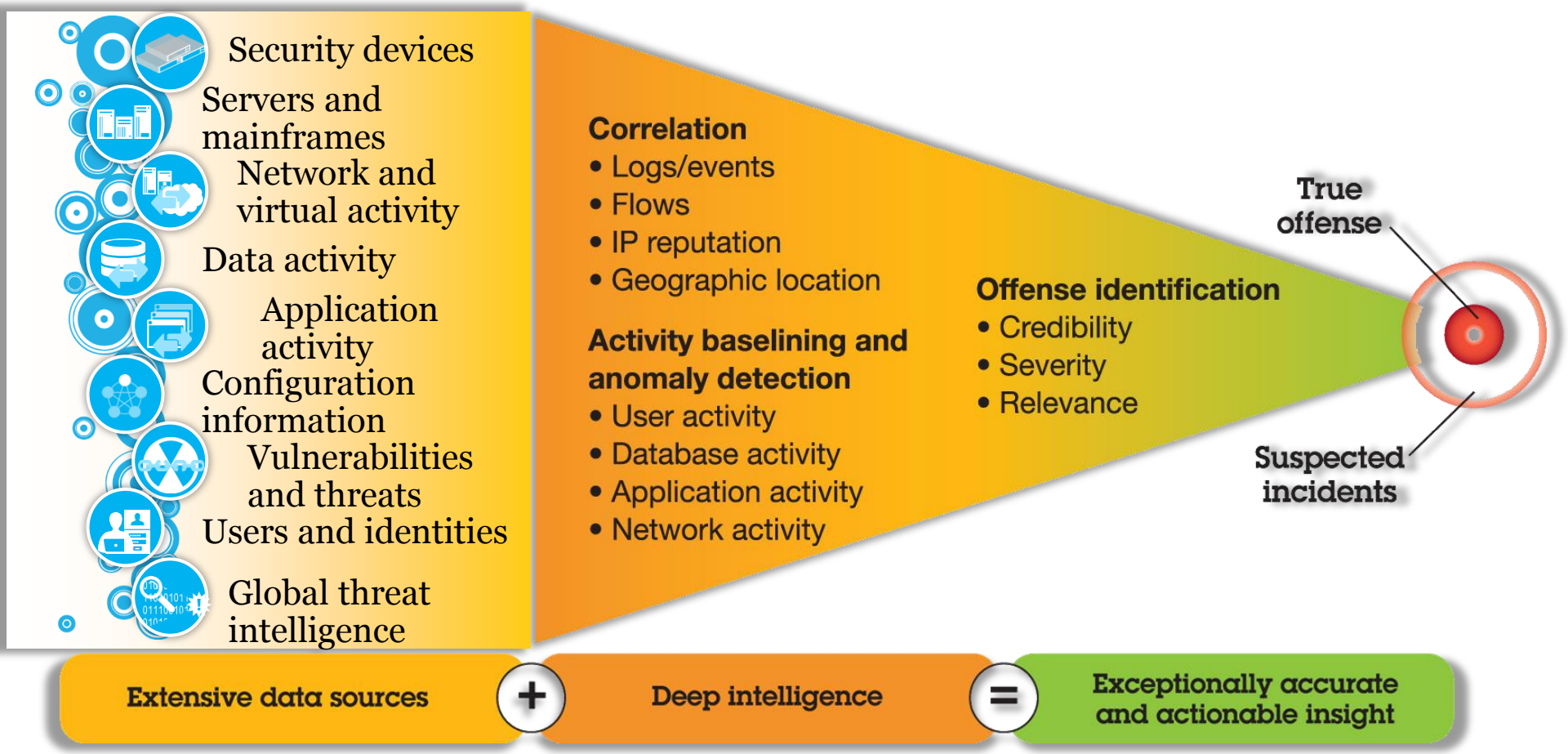
Reaction & Remediation

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
Security Information and Event Management.
Log Management. Incident Response.

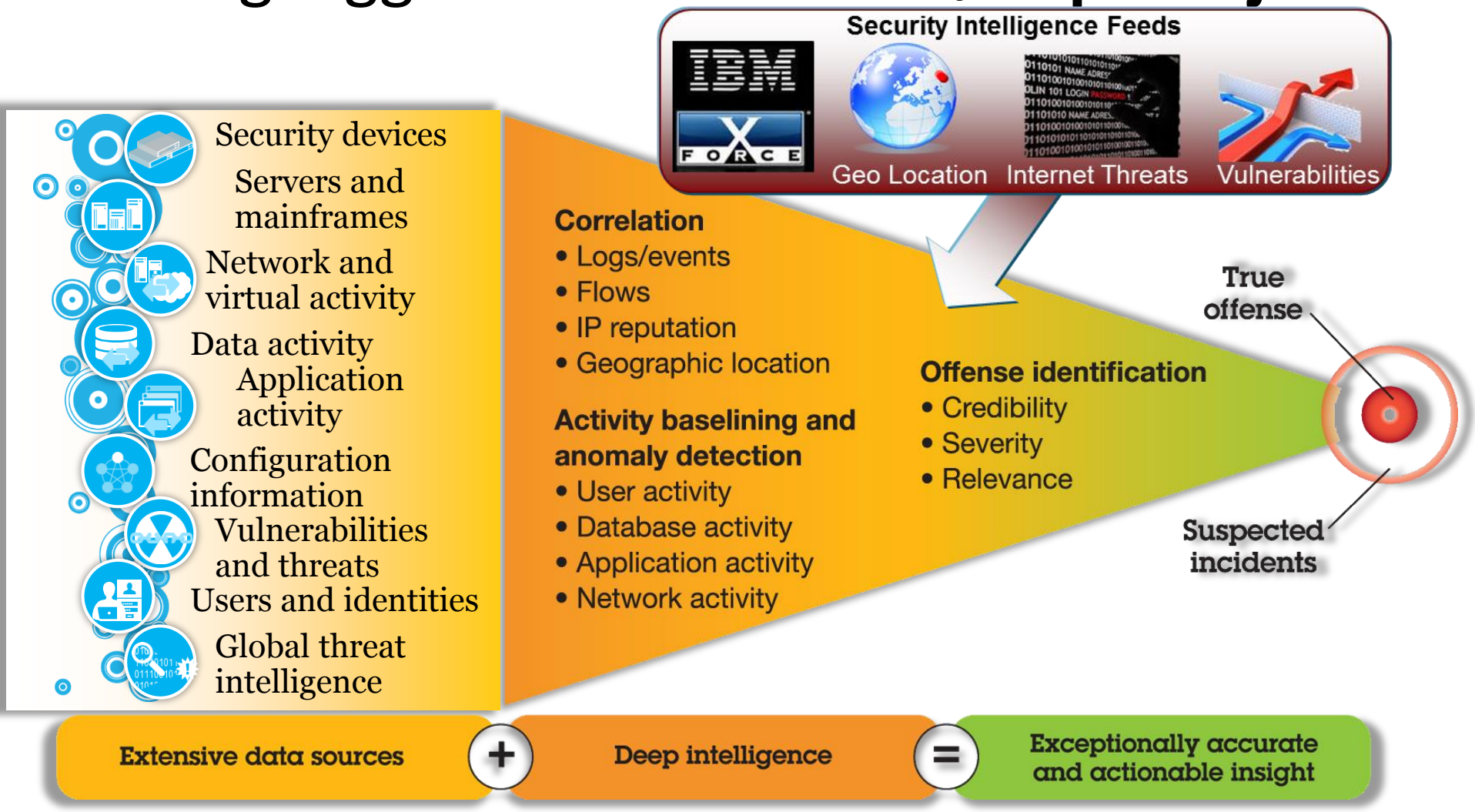
Bygget på fellesplattformen QRadar SIOS



Tar inn data fra et bredt **spekter av kilder**…



… og legger til **kontekst** for **økt presisjon**



Eksempel (1)

- Ny maskin kommer på nett
  - Oppdages umiddelbart og logginnsamling startes
  - Flowinnsamling begynner, og også profiling av maskin (mtp anomalideteksjon)
  - Sårbarhetsskanning startes automatisk
  - Resultat mates automatisk til risikomodul, som starter evt avvikshåndtering – risikobasert
- Resultat: Risikosituasjon avklart umiddelbart. Ingen «løse kanoner på dekk»

Eksempel (2)

- Malwareangrep
  - Varsel fanges opp fra ulike sikkerhetssystemer
  - Hendelser korreleres mot annen informasjon
    - Konfigurasjonsinfo for brannvegg
      - Avdekker at visse mål er beskyttet av brannvegg, men ikke alle
    - Sårbarhetsinfo
      - Avdekker at visse mål er sårbare, men ikke alle
    - Logger fra antivirus etc
      - Avdekker at antivirus har beskyttet noen mål, men ikke alle
  - Anomalibeskyttelse avslører mistenkelig trafikk fra system
  - Løsning varsler fortløpende om faktisk hendelsesomfang
- Resultat: Angrep fanget opp og håndtert, med lite manuell inngripen

Eksempel (3)

- Spørsmål – «er vi sårbare for x?»
  - Løsningen sammenstiller sårbarhetsinformasjon, policyinformasjon mm
    - Gir svaret ift reelle sårbarheter
      - Har man virtuell patching?
      - IPS?
      - Brannvegg?
- Sårbarhetssituasjon raskt avklart

Eksempel (4)

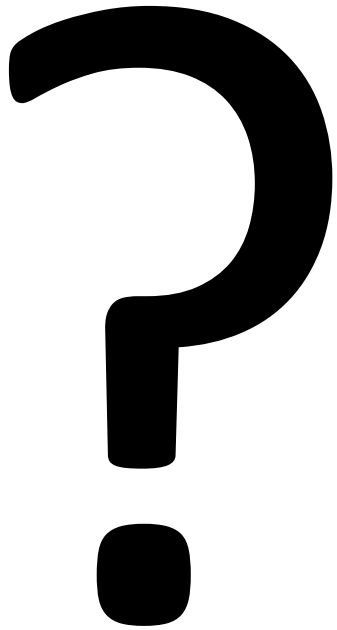
- Angrep
  - Informasjon fra sikkerhetssystemer monitoreres og sammenstilles kontinuerlig – ingen av dem har oppdaget noe mistenkelig
  - Korreleres mot IBMs trusselinformasjon – avdekker at maskiner har kommunisert med kjente angrepsnoder.
  - Analyse og opprydning foretas
- Resultat: Angrep avdekket og håndtert, igjen med lite manuelt arbeid

Eksempel (5)

- Angrep
  - Informasjon fra sikkerhetssystemer monitoreres og sammenstilles kontinuerlig – ingen av dem har oppdaget noe mistenkelig
  - Korreleres mot IBMs trusselinformasjon – gir intet mistenkelig resultat
  - En standard anomaliregel ser på nettverkstrafikk, og oppdager at en mailserver plutselig er aktiv på FTP. Forholdet varsles, og sikkerhetspersonell analyserer forholdet gjennom løsningen og konkluderer:
    - Målrettet, avansert angrep
  - Analyse og opprydning foretas
- Resultat: Angrep avdekket og håndtert


The Software Experts
Crayon


PEDAB
FINDS YOUR
NEXT BUSINESS



The Software Experts Crayon

PEDAB FINDS YOUR NEXT BUSINESS

Takk for oppmerksomheten!

Vi snakkes gjerne på stand i pausen.

Paul-Christian Garpe CISSP CISA CCSK
pcg@pedab.no, 48 01 89 03
Pedab Norway