I forkant av svindleren
-med teknologien på din side

Christian Nordve
Systems Engineer
chnordve@cisco.com

The Security Problem

Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

Breach Statistics

It is a ***Community***
that hides in plain sight
avoids detection
and attacks swiftly

“There are two types of companies: Those who have been hacked, and those who don’t yet know they have been hacked.”

John Chambers
Chief Executive Officers of Cisco

Hvorfor?

Ville du gjort noe annerledes i dag *om du viste* at du kom til å bli angrepet i mogen?

Tekniske løsninger som antivirus og brannmur er ikke nok for å stoppe datainnbrudd, ifølge NorSIS. (Foto: Espen Zachariassen)

DATAINNBRUDDET HOS TELENOR

– Bedre opplæring kunne trolig avverget angrepet mot Telenor-ledelsen

Dataskurkene stoppes ikke av antivirus alene.

AV: ROALD RAMSDAL | ODD RICHARD VALMOTODD RICHARD VALMOT | IT | PUBLISERT: 18. MARS 2013 - 1

Facebook 0 Twitter

Denne helgen ble det kjent at sjefene i Telenor har blitt frastjålet store mengder sensitive data. For første gang politianmeldte selskapet industrispionasje,

JOBB

Jobbportalen for ing teknologer

2014, kl. 12:25

27 Million

illion citizens, up to 70

in 2013

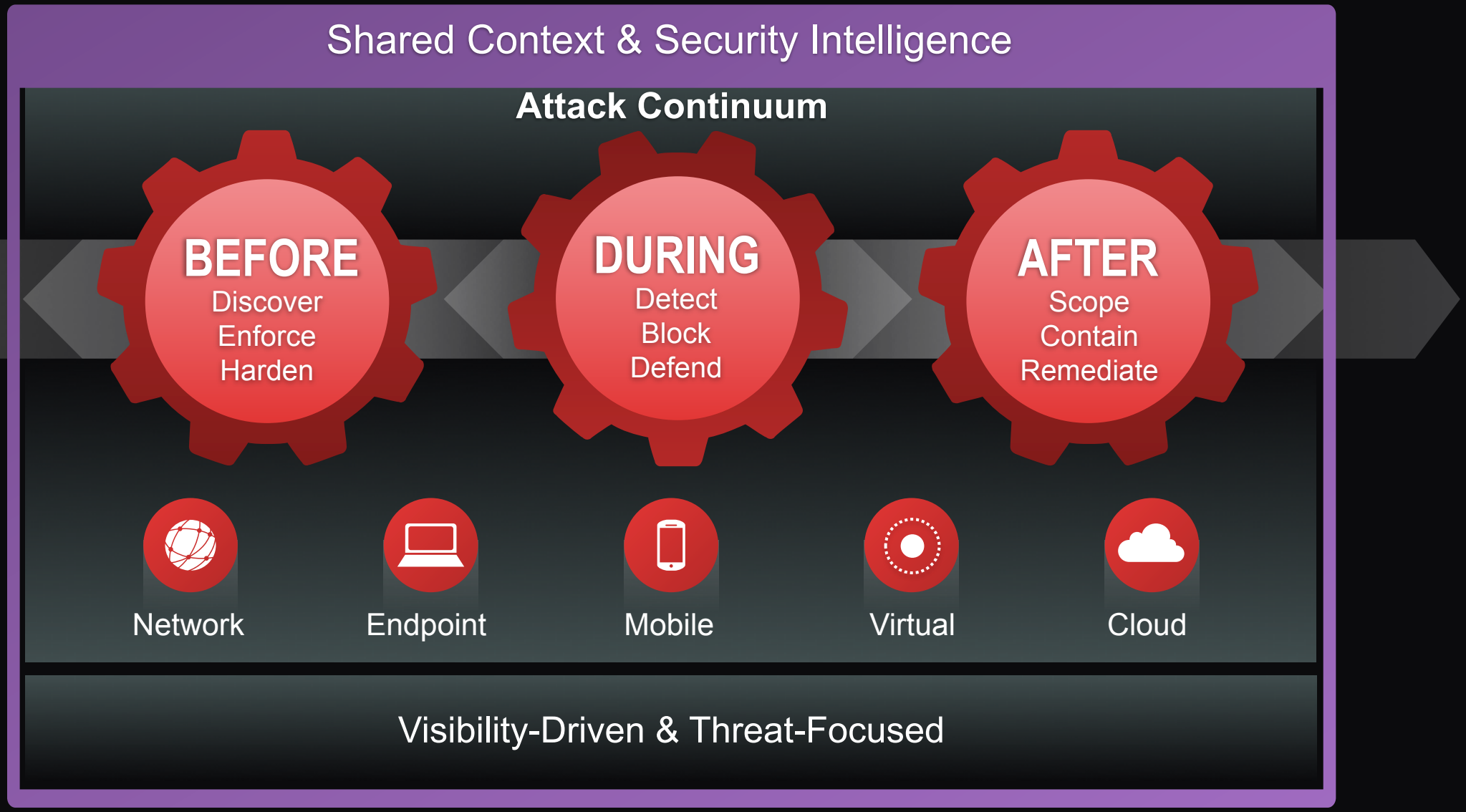
t year,

Når bygde Noha arken?

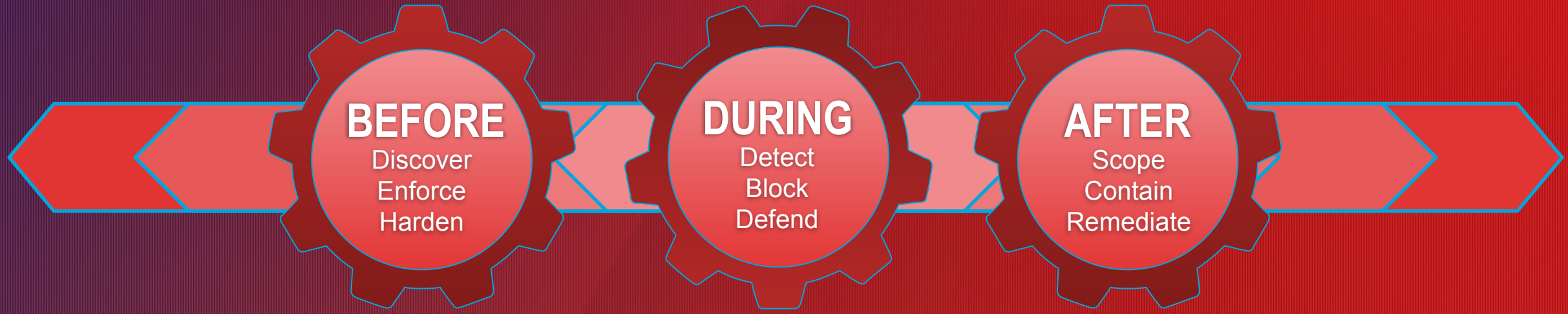
Før det begynte å regne!

En endring i vår forståelse og innstilling er i ferd med å endres

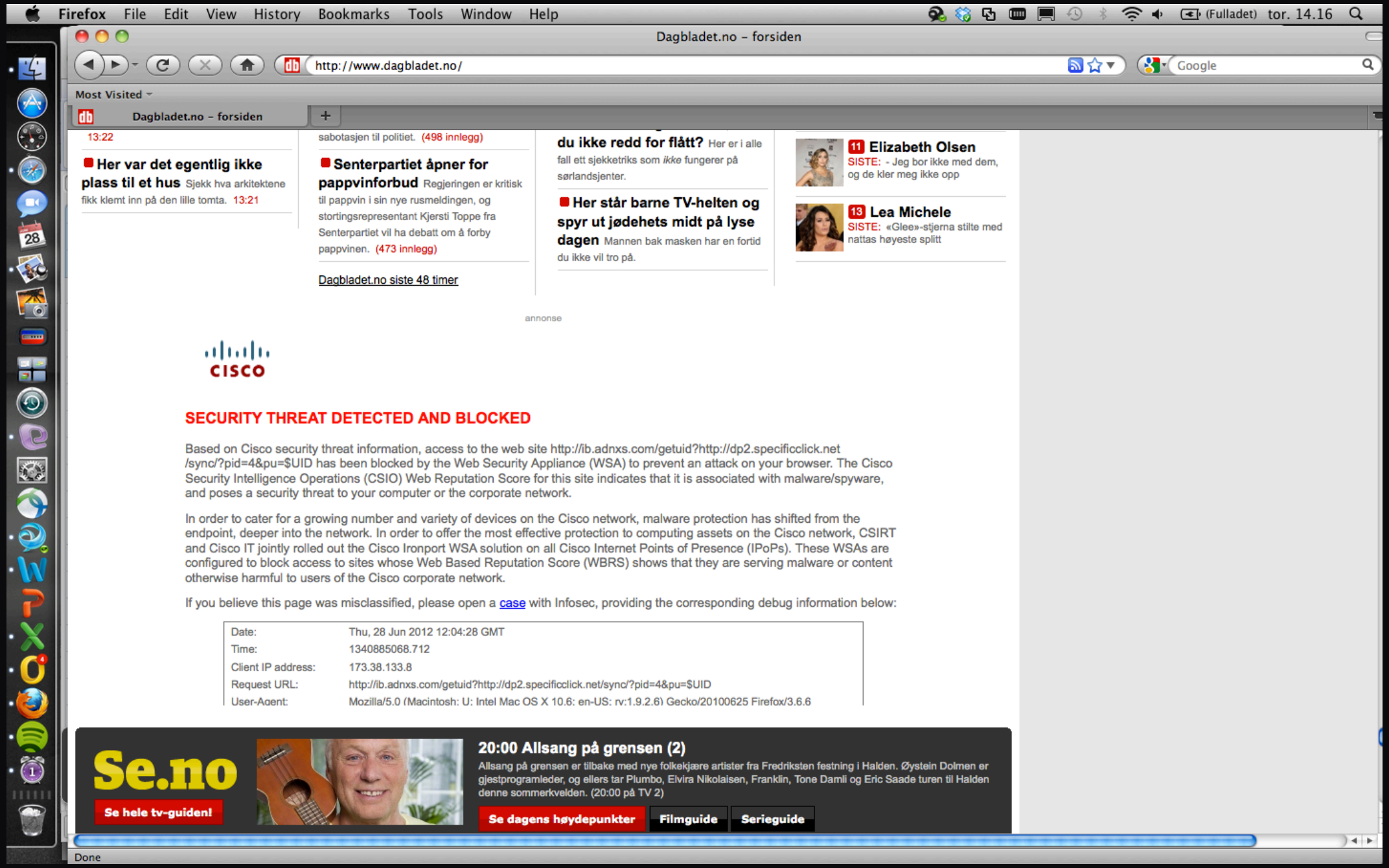
A Threat-Centric Security Model is Needed



Building a Threat-Centric Cisco Security Architecture



Attack Continuum



Se og forstå det sammensatte bilde!

Evne til å se ting i perspektiv og retroperspektiv

- Hvis noe kommer seg inn på nettet hos oss eller på en av våre maskiner forde vi ikke vet om det er farlig
- ...Fordi det er *helt nytt* og ingen har sette det før….
- Men, i morgen så vet vi mer og kan nå slå fast at det er et “virus”...
- Ville ikke du da helst vite om det?
  - Hvem lastet det?
  - Hvor er det nå? –Hvor har det spredd seg

Nettverket ser alt

Vi må integrere mer effektivt for å skape en virkningsfull sikkerhetsløsning.

Det krever arkitektur

Utfordringer

- Ikke noe av dette virker hvis alt må være på plass for at noe skal virke
- Hver enkel løsning/produkt må kunne “stå på egene ben” og være blandt de beste, hver for seg

Når Cisco løsningen settes sammen vil de skape mulighet for å bruke hverandres innsikt og innsyn til å berike hverandre

“Our fundamental job is to reduce complexity and increase capability”

18

Superior Intelligence to battle Advanced Threats

Cisco® SIO

Talos
Cisco Collective
Security Intelligence

Sourcefire VRT®

1.8 million
global sensors

100 TB
of data received per day

180 million+
deployed endpoints

600+
engineers, technicians, and researchers

35%
worldwide email traffic

13 billion
web requests

24x7x365
operations

40+
languages

Pervasive across Portfolio

200,000+ File Samples per Day

FireAMP™ Community, 3+ million

Advanced Microsoft and Industry Disclosures

Snort and ClamAV Open Source Communities

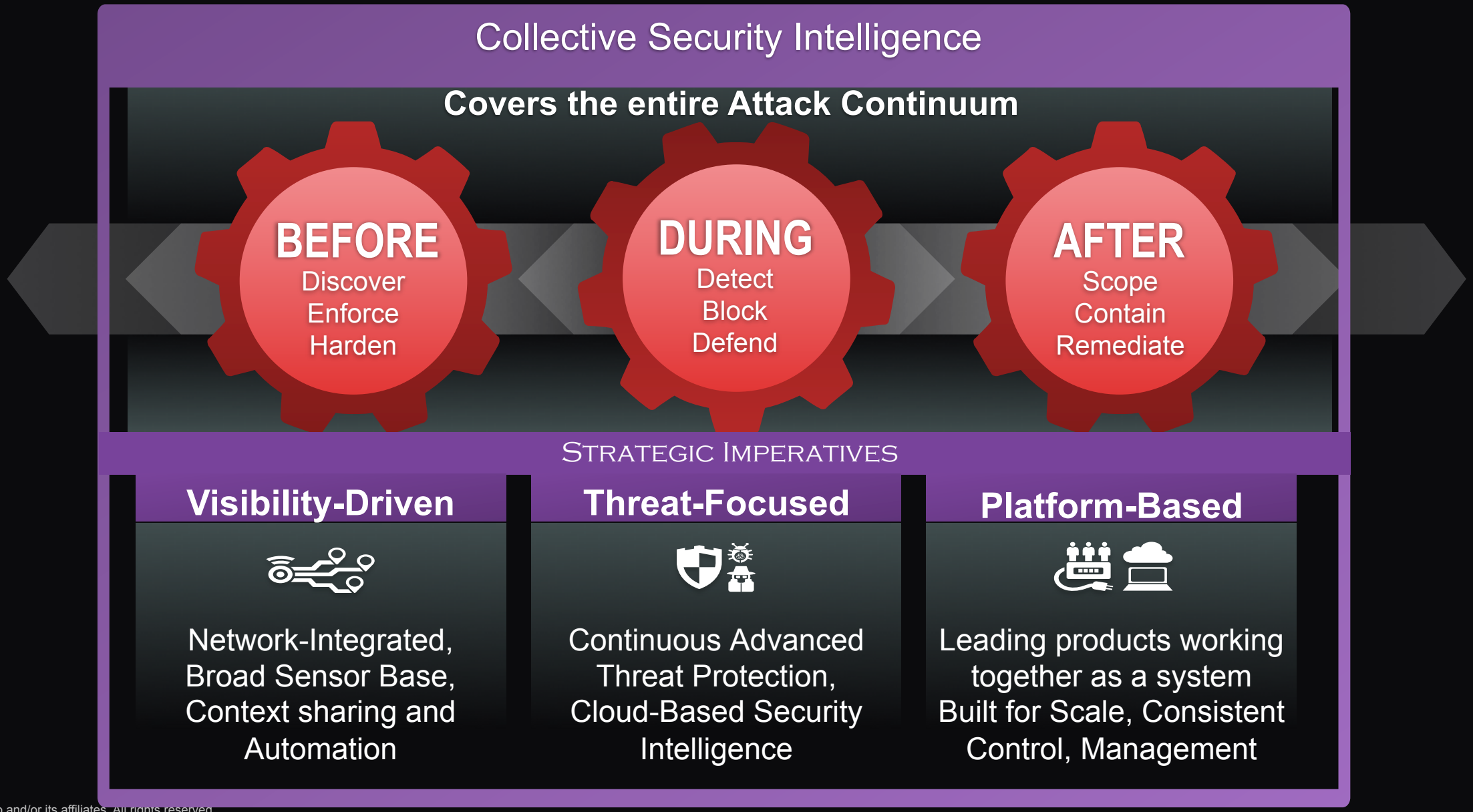
Honeypots

Sourcefire AEGIS™ Program

Private and Public Threat Feeds

Dynamic Analysis

Oppsummert



Takk for meg!