REFRACTED security
digital safety made accessible

HEB JE WEL EEN SOC?

Door Stijn Horemans en Karel Sels

INTRODUCTIE

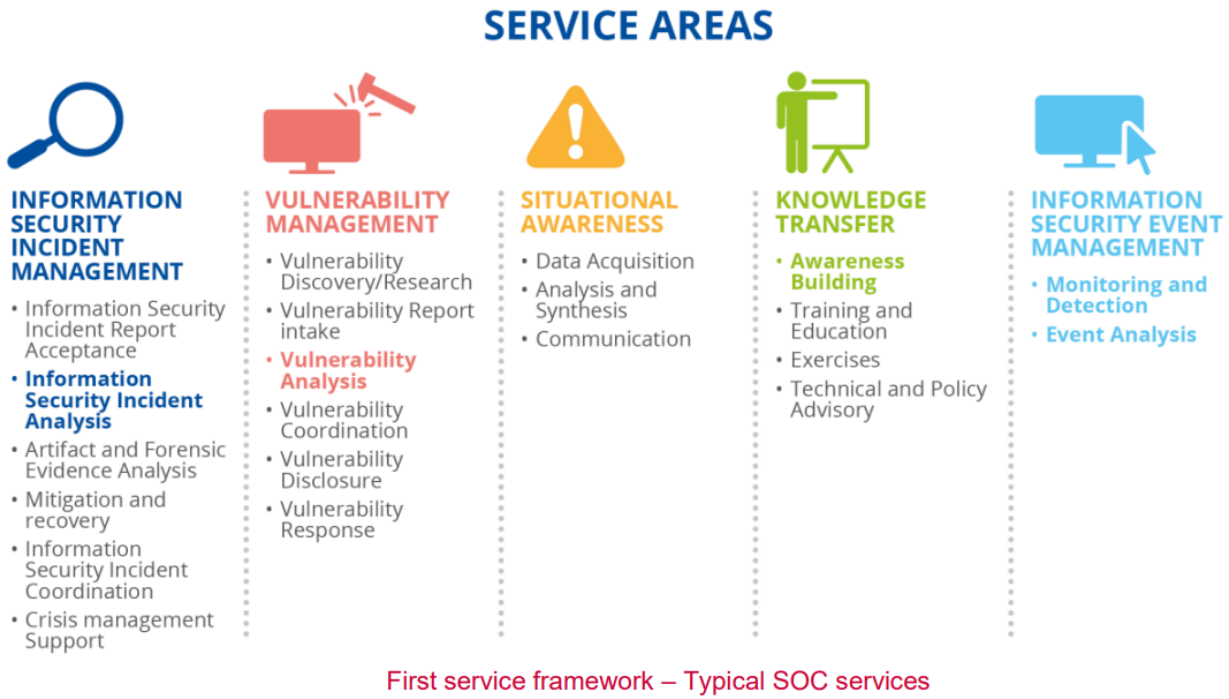
Karel Sels

_ Red Team / Penetration testing professional

Stijn Horemans

_ Red Team / Penetration testing professional

WAT IS EEN SOC?

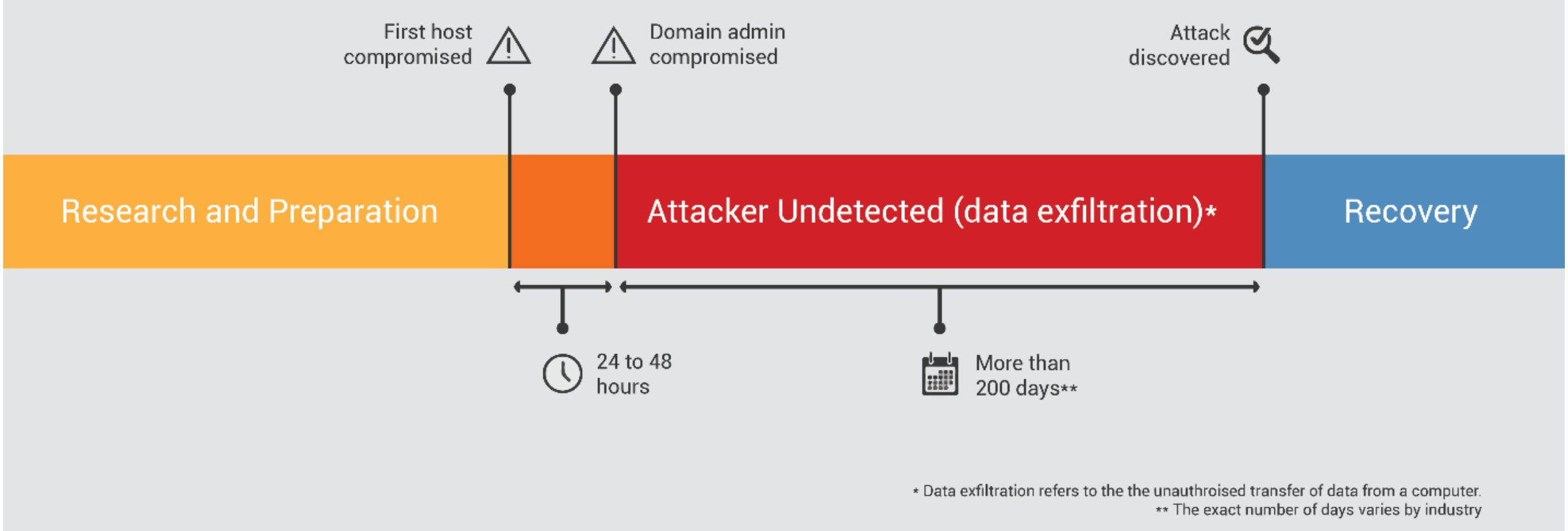


First service framework – Typical SOC services

- Assessments van SOC effectiviteit

- Focus
    - Incident Management
    - Netwerk Monitoring
    - Reactie op dreigingen

ANATOMIE VAN EEN DATA BREACH



Source: adminbyrequest.com

WAAROM DEZE TALK?

- Vals gevoel veiligheid
- Discussie stimuleren
- Awareness klant / SOC provider
- Security maturiteit verhogen

Gaten in de detectie

Vertraging response

False positives

False negatives

EVALUATIE VAN SOC MONITORING

Essentie van security monitoring en opvolging:

_ Incidenten tijdig waarnemen

_ Reactie initiëren

_ Nodige escalaties in gang zetten

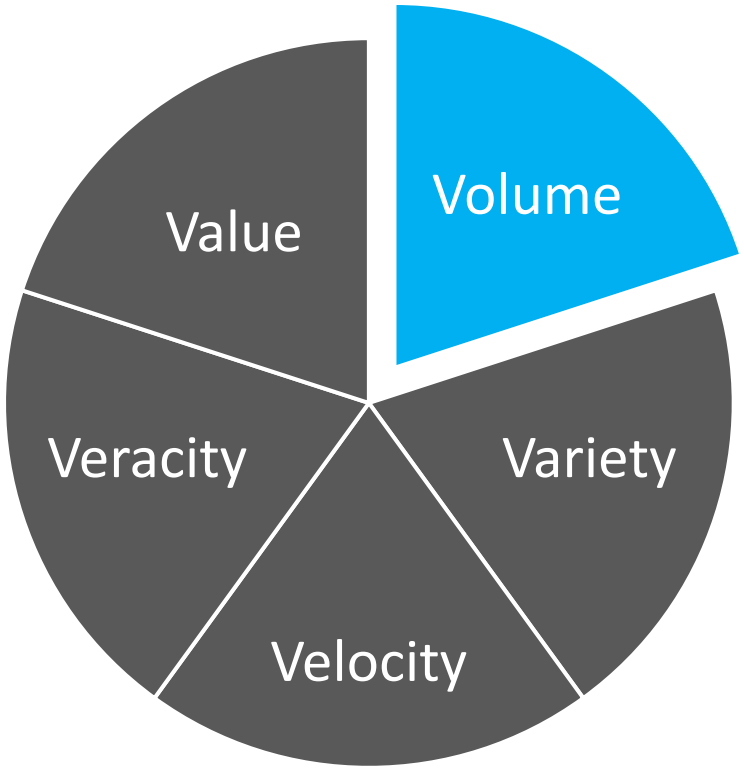
_ Informatieflow

5V model:

- _ **Volume**
- _ **Variety**
- _ **Velocity**
- _ **Veracity**
- _ **Value**

EVALUATIE VAN SOC MONITORING - VOLUME

Zien we van onze bronnen alle alerts?



Typische problemen:

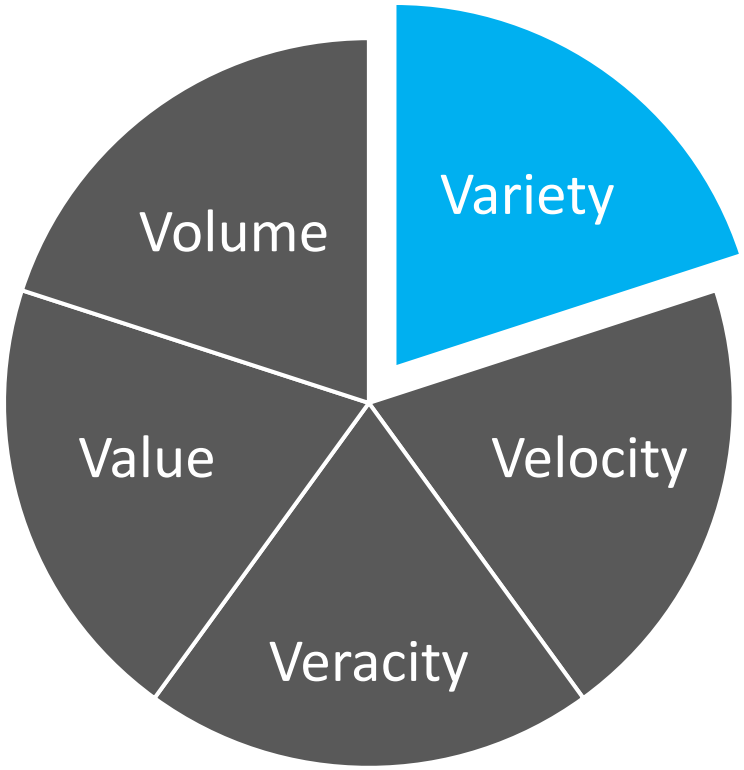
_ Ontbrekende alerts door sampling

_ Queues die vol zitten

_ Slechte afstelling van alerts (teveel false positives)

EVALUATIE VAN SOC MONITORING - VARIETY

Zien we alerts uit voldoende bronnen?



Niet alle systemen

Log sources niet geconnecteerd

Prijs

Oorzaak

Gaten in visibiliteit

Tragere response

Compliance issues

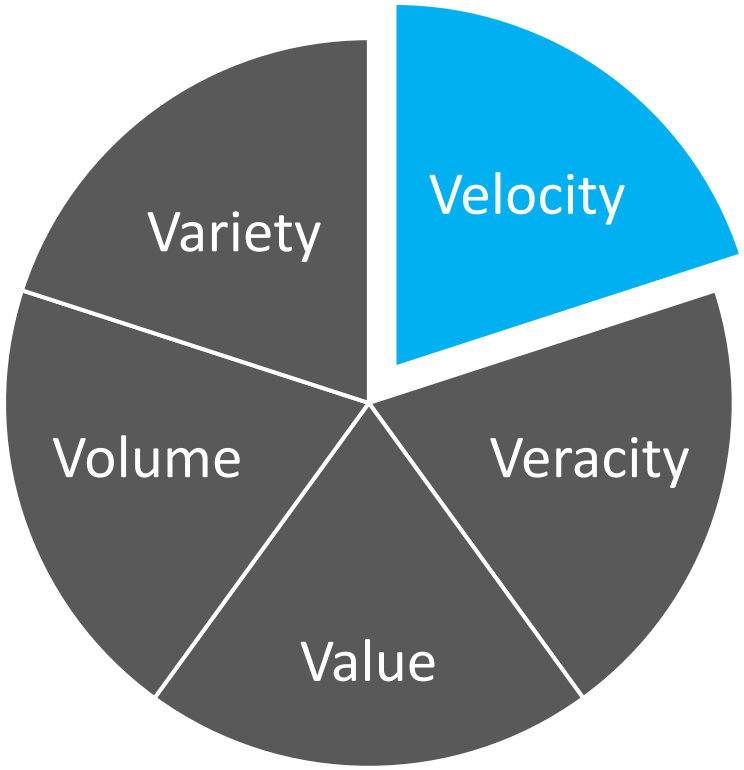
Gevolg

Welke wel?

- Active directory
- Anti-virus / EDR
- Basic network logs
- Powershell / commandline

EVALUATIE VAN SOC MONITORING - VELOCITY

Worden de alerts voldoende snel behandeld?



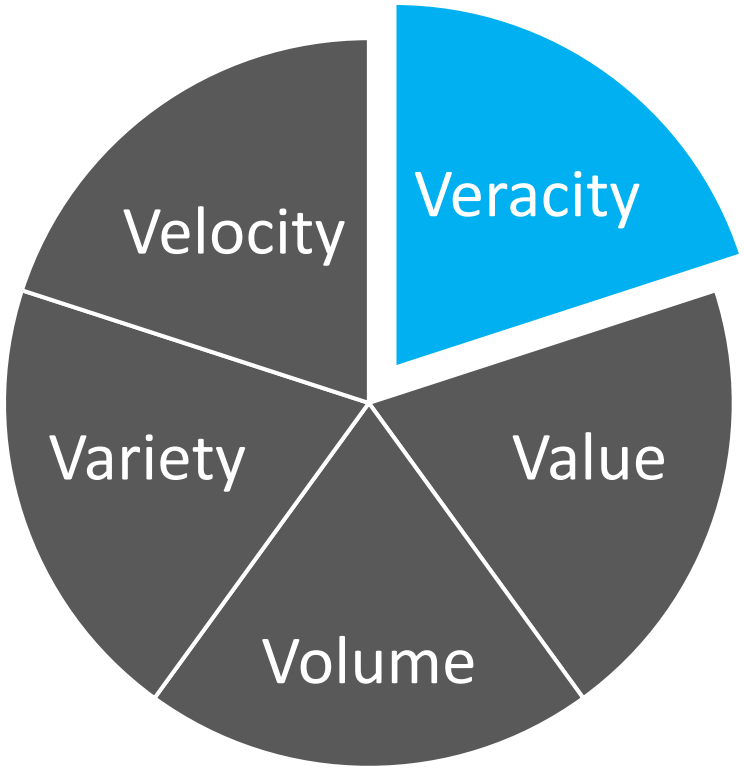
Oorzaak	Gevolg
Weinig alerts	Aanvallen negeren
Te veel false positives	Verminderde efficientie
Repeditieve onderzoeken	Compliance issues
	Governance vergeten

Wat wel?

- Nakijken SOC response
- SOC – Klanten workshops
- Offensive security assessments

EVALUATIE VAN SOC MONITORING - VERACITY

Is de informatie correct?



Verkeerde data

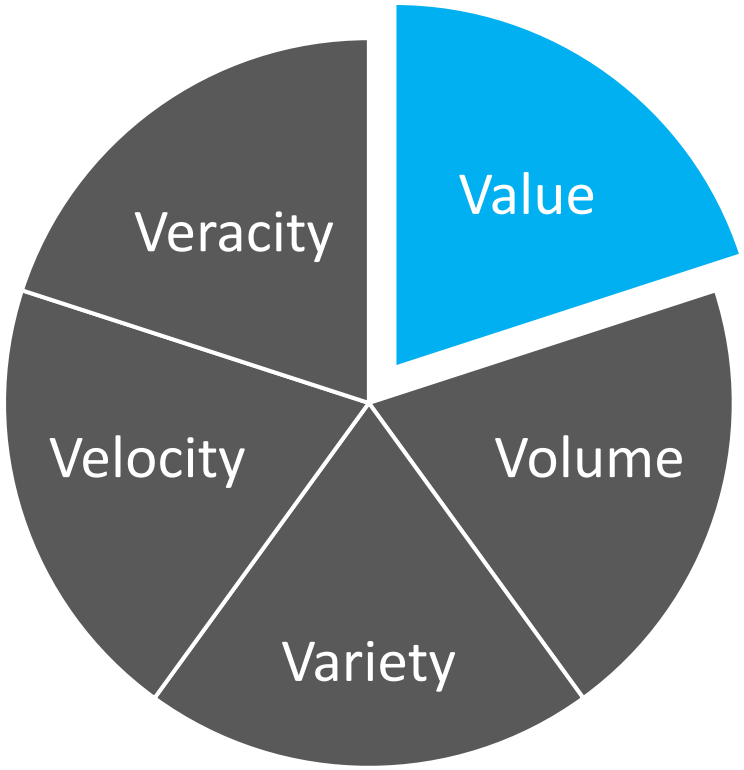
- Enrichment vanuit verkeerde bron
- Tickets gelinkt aan verkeerde alerts

Verkeerde analyse

- Verkeerde prioritisatie (bv ikv SLAs)

EVALUATIE VAN SOC MONITORING - VALUE

Kunnen we hierop actie ondernemen?



Slechte prioritisatie

Misverstanden rond normale trafiek

Te weinig context

Communicatie problemen

Link naar Playbooks

GEEN INCIDENT RESPONSE PLAYBOOKS GEDEFINEERD

- Niet voorbereid op een incident
- Paniek
- Slechte response
- Te aggressieve response
- Vertraagde opvolging van security incidenten
- Geen efficiente response
- Reputatie schade
- Compliance problemen

VALUE

Gebruikelijke Playbooks

- Malware infectie
- Databreach
- Denial of service
- Insider threat
- Inbraak
- Mobiele device compromise
- Cloud environment compromise
- Compromised accounts
- Ransomware

CONCLUSIE: CONTINU VERBETERING

CONCLUSIE: ESSENTIEEL

Definieer specifieke use cases

Verifier of alle data bruikbaar is

Frequent testen van use cases

Open en eerlijk communicatie met SOC

Aankoop process is essentieel

Playbooks zijn levende documenten

We want to be the power-food for your digital safety

Refracted Security
by 42secure BV