

Detectie verdachte activiteit in je netwerk

Ontwikkeling van het Intermax SOC 2.0

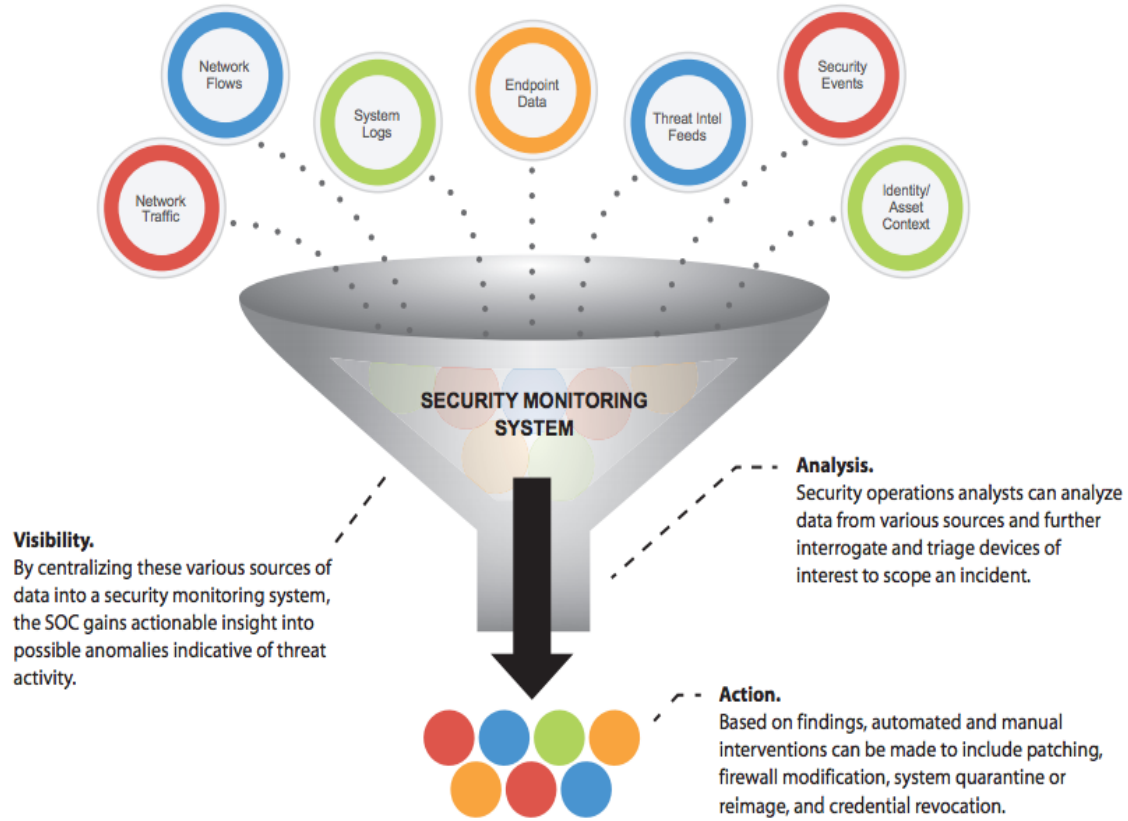
donderdag 5 december 2019

Doelstellingen

- Real-time detectie
- Multi-tenant
- Horizontaal schaalbaar
- Inzichtelijk voor de klant
- Kosten effectief

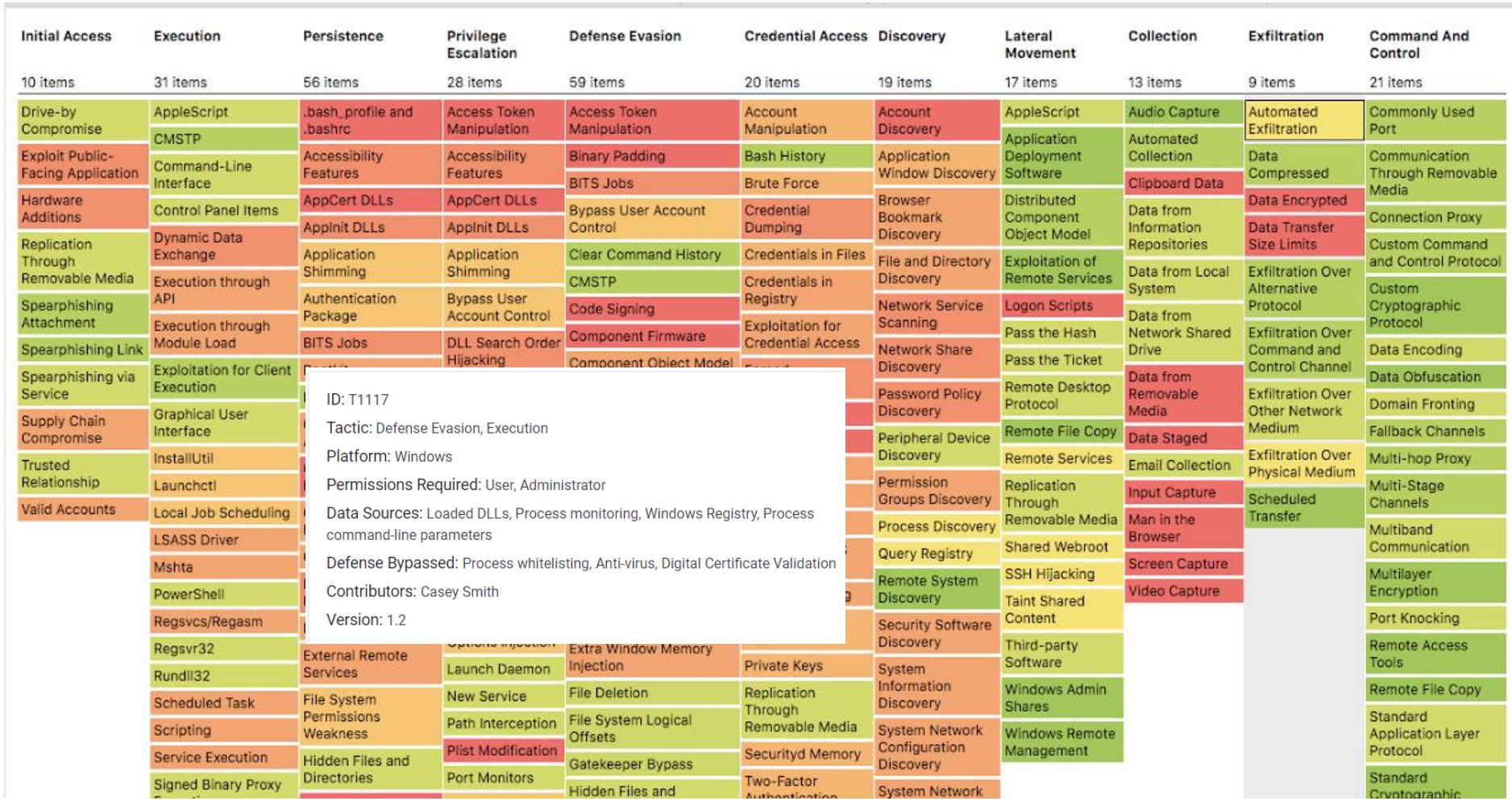
Uitdagingen

- Geen tooling op de endpoints
- Beperkte mogelijkheden voor detective in het netwerk
- Contractuele verplichtingen voor data vernietiging
- Niet iedere klant heft dezelfde risk appetite



intermax

Mitre Att&ck Map



intermax

Detectie door middel van statische regels

- Detecteert op basis van de inhoud van logs
- Ook op samenhang tussen log regels
- Alleen vooraf bekende risico's
- 300+ regels beschikbaar

Nadelen

- Generiek, geen detectie op gedrag
- Detecteerd geen onbekende technieken

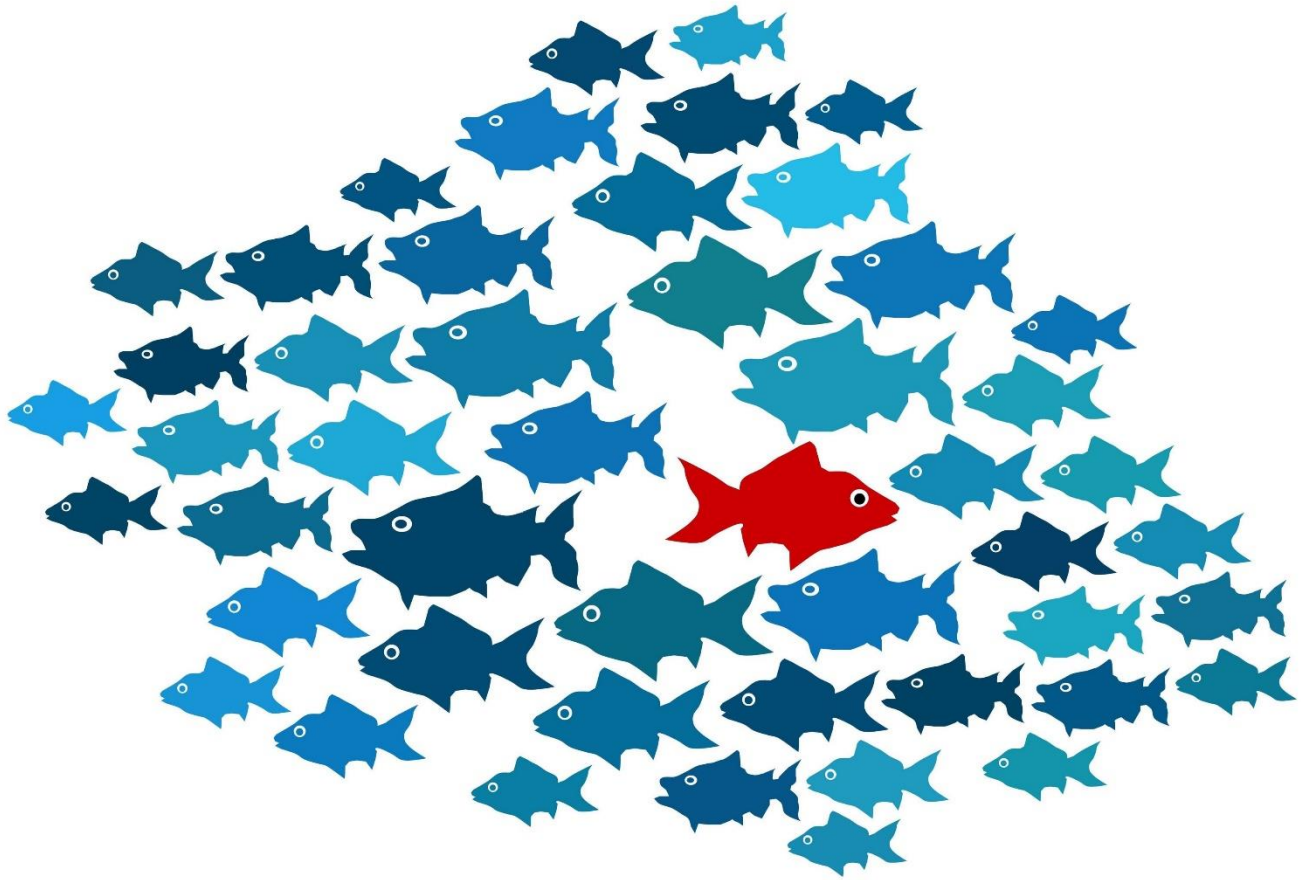
win_susp_failed_logons_single_source.yml | win_susp_security_eventlog_cleared.yml | win_susp_lsa

```yaml
title: Multiple Failed Logins with Different Accounts from Single Source System
description: Detects suspicious failed logins with different user accounts from a single source system
author: Florian Roth
logsource:
    product: windows
detection:
    selection:
        EventLog: Security
        EventID:
            - 529
            - 4625
            - 4776
        UserName: not null
        SourceWorkstation: not null
    timeframe: last 24h
    condition: selection | count(UserName) by SourceWorkstation > 3
falsepositives:
    - Terminal servers
    - Jump servers
    - Other multiuser systems like Citrix server farms
    - Workstations with frequently changing users
level: medium
```

Dynamische detectie

- Nog onbekende technieken
- Profilering

- DGA (Domain Generation Algorithms)
- Process execution chain
- TLS Certificaat eigenschappen
- Layer 3 en 4 communicatie

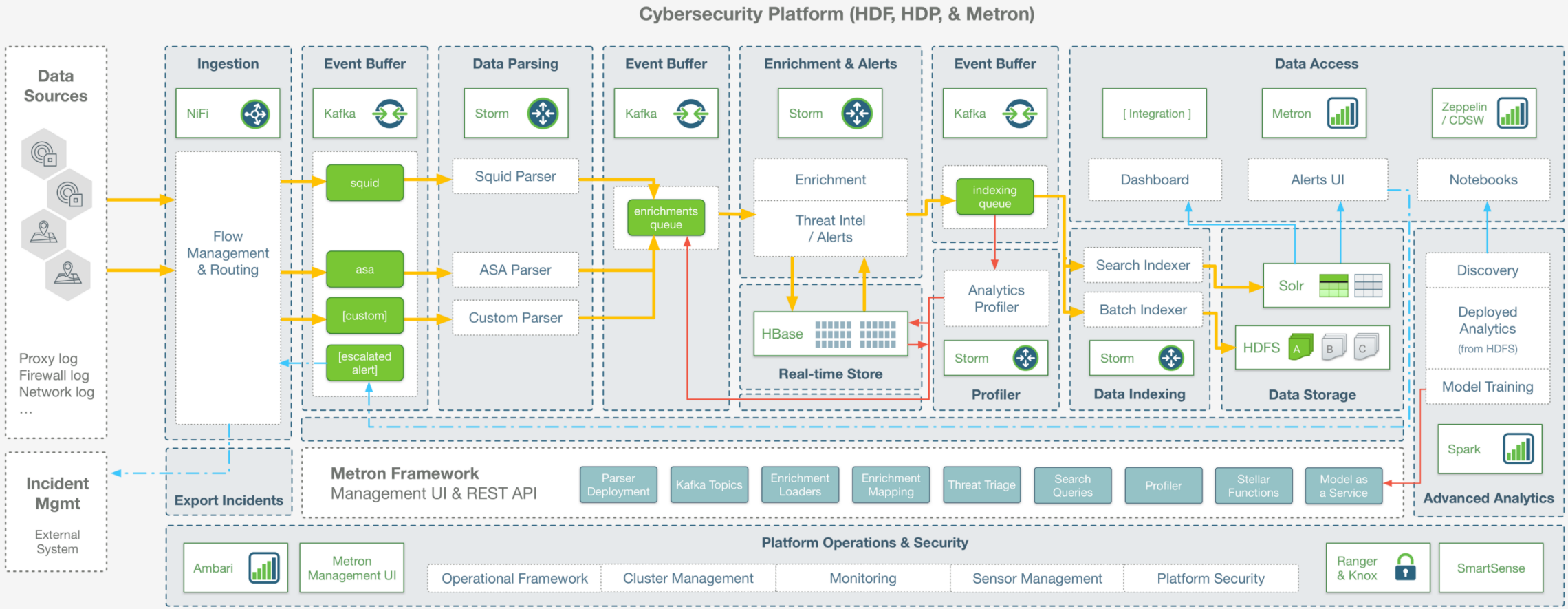


Nadelen

- Black-box
- Adveserial attacks
- Risico op hoog percentage false-positives en false-negatives

intermax

Apache Metron – Streaming Analytics



SOC Anomaly detectie

- Risico profiel verschilt per medewerker en server
- Risico profiel verschilt per moment van de dag

Intermax SOC

- Stelt risico profiel op per medewerker en systeem
- Alerts op basis van afwijking in het risico profiel
- Alerts op basis van afwijking t.o.v. directe collega's



intermax

Meer informatie:

- Anatomy of a Streaming Data Engineering Pipeline
  https://medium.com/@laurencedaluz/anatomy-of-a-streaming-data-engineering-pipeline-c13c0211067e
- Getting Started with ATT&CK: Detection and Analytics
  https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0
- Real Time Threat Detection Through Network Analysis
  https://www.researchgate.net/publication/336680779_Real_Time_Threat_Detection_Through_Network_Analysis

- https://attack.mitre.org/
- https://metron.apache.org/
- https://github.com/Neo23x0/sigma