STRATEGYTALKS

Aris Koios, Technology Strategist CEUR

CrowdStrike

XDR: What it is, What it isn't and What it should be!

CROWDSTRIKE

X D R

What it is.

Looking past the marketing hype.

An analysts opinion on XDR

Native

Tight integration with vendors own portfolio of products.

Hybrid

Relies on integrations with third-party vendors to collect new telemetry.

Security Analytics

Collects large data sets and provides security analytics over the collected dataset.

Looking past the acronym

Data

Access & leverage data from across the network

Detection

Use all the telemetry to identify and detect new threats

Response

Be able to interpret and determine true incidents and respond rapidly

The perceived solution

Application Logs

Event Logs

System Logs

Security Logs

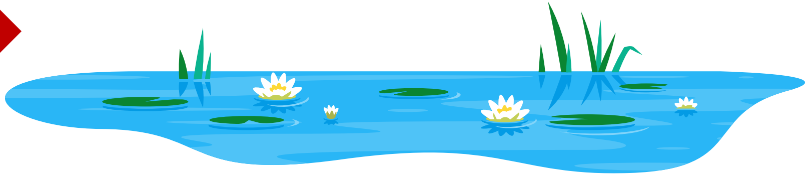
Web Service Logs

User Logs

Service Logs

DNS Logs

Log Logs Logs



The Data Pond

The perceived solution

Application Logs

Event Logs

System Logs

Security Logs

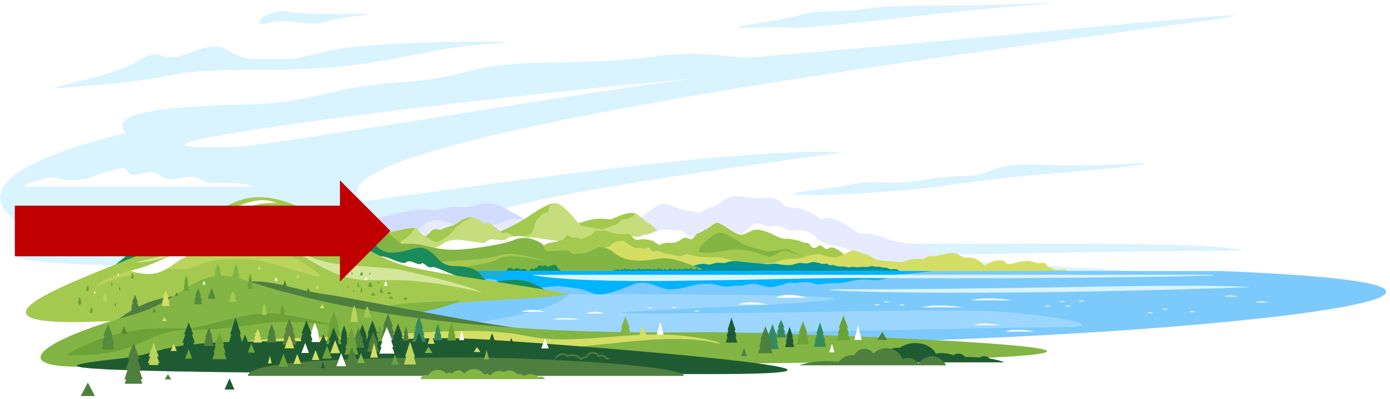
Web Service Logs

User Logs

Service Logs

DNS Logs

Log Logs Logs



The Data Lake

The perceived solution

Application Logs

Event Logs

System Logs

Security Logs

Web Service Logs

User Logs

Service Logs

DNS Logs

Log Logs Logs

The Data Dump

The data problem

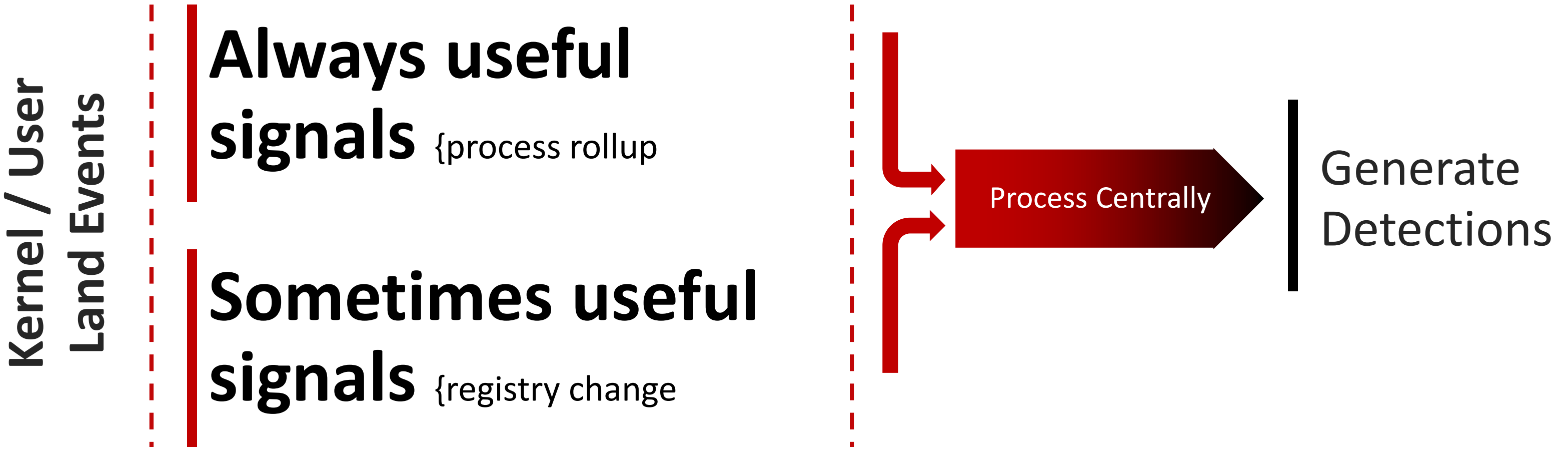
The right data is more important than all the data.

More data may help to introduce more relevance or usefulness.

The wrong balance will decrease our outcomes.

How real EDR vendors solved the data problem

- First rule of building an EDR solution, don’t build a log collector!



Kernel / User Land Events

Always useful signals {process rollup

Sometimes useful signals {registry change

Process Centrally

Generate Detections

So what is XDR?

Its an evolution of EDR.

XDR

Definition | **Extended Detection Response**

Built on the foundation of EDR, XDR extends enterprise-wide visibility across all key security domains (native & third-party) to speed and simplify near real-time detection, investigation, and response for the most sophisticated attacks

X D R

What it isn't!

eXtra, eXtended, MDR, SIEM, NDR …

What XDR is not

- EDR + NDR != XDR
- SIEM + EDR != XDR
- EDR + API’s != XDR
- EDR + Firewall Logs != XDR
- SIEM + SOAR != XDR
- EDR + Log Management != XDR

Questions to ask when looking for an XDR solution

- What data is the solution looking at?
- Does the data get collected, stored and then queried?
- Is the solution a collection of point solutions via a single/multiple UI?
- Do you have to add your own integrations or is it out of the box?
- How much configuration / people do you need to make it work?
- Is it on-premise or cloud based?

X D R

What it should be!

CROWDSTRIKE

Evolving EDR to XDR

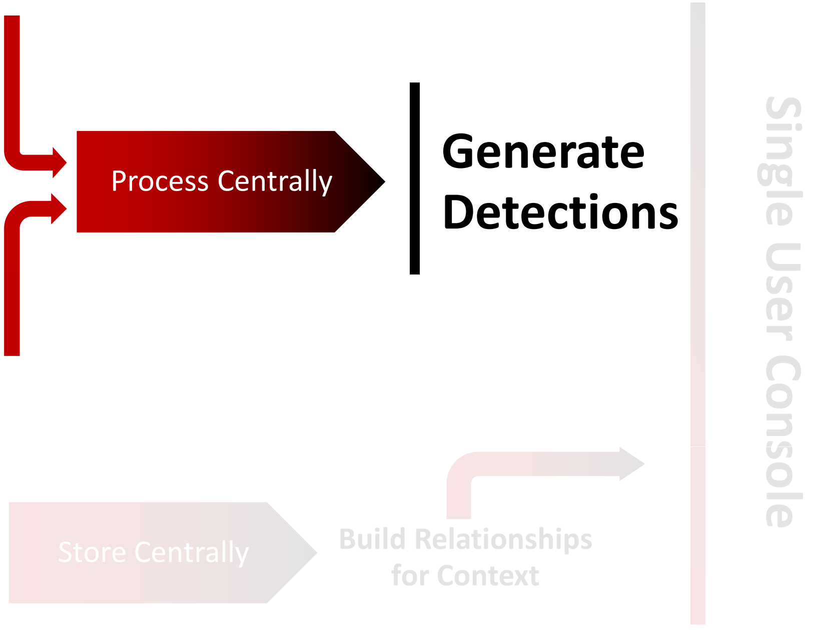
Any data event (Cloud, Identity, Endpoint, IOT, Network ...)

Always useful signals {process rollup

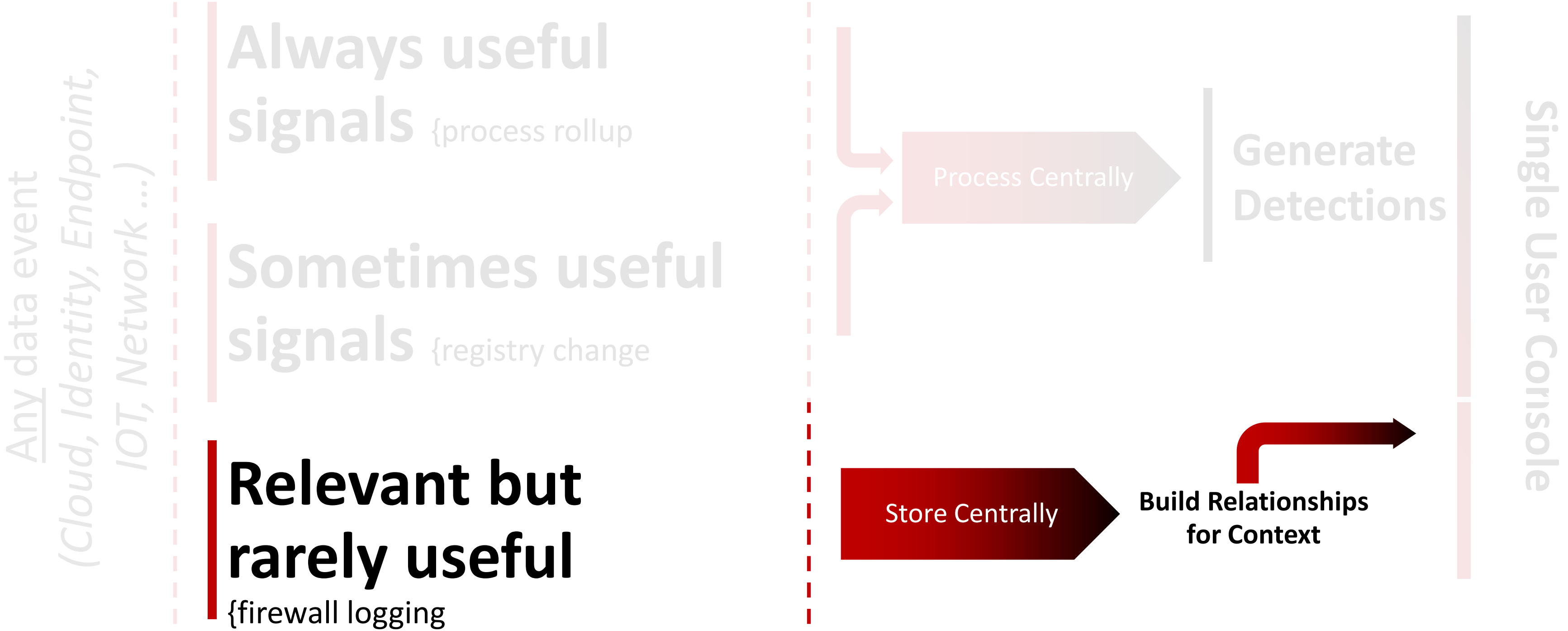
Sometimes useful signals {registry change

Relevant but rarely useful

{firewall logging



Evolving EDR to XDR



Any data event (Cloud, Identity, Endpoint, IOT, Network ...)

Always useful signals {process rollup

Sometimes useful signals {registry change

Relevant but rarely useful
{firewall logging

Process Centrally

Generate Detections

Store Centrally

Build Relationships for Context

Single User Console

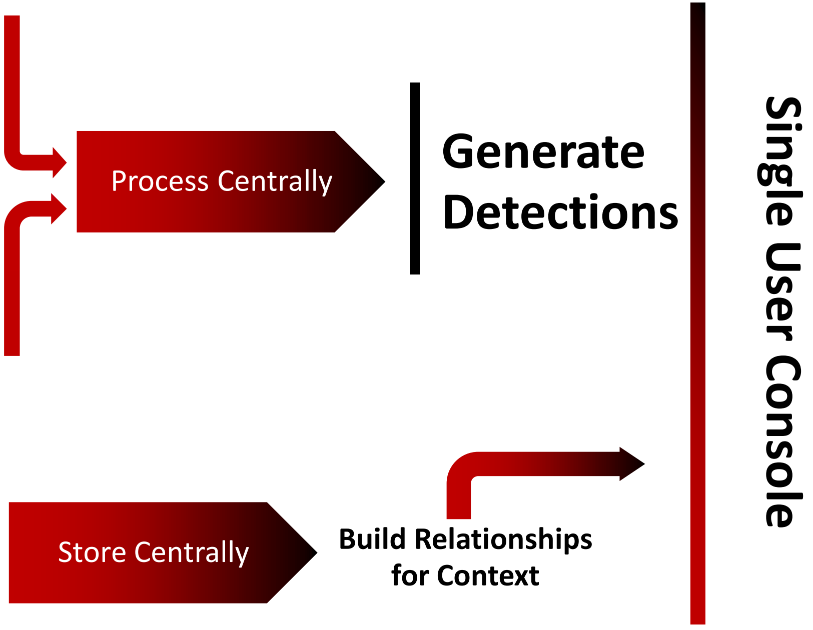
Evolving EDR to XDR

Any data event
(Cloud, Identity, Endpoint,
IOT, Network ...)

Always useful signals {process rollup

Sometimes useful signals {registry change

Relevant but rarely useful {firewall logging



Process Centrally

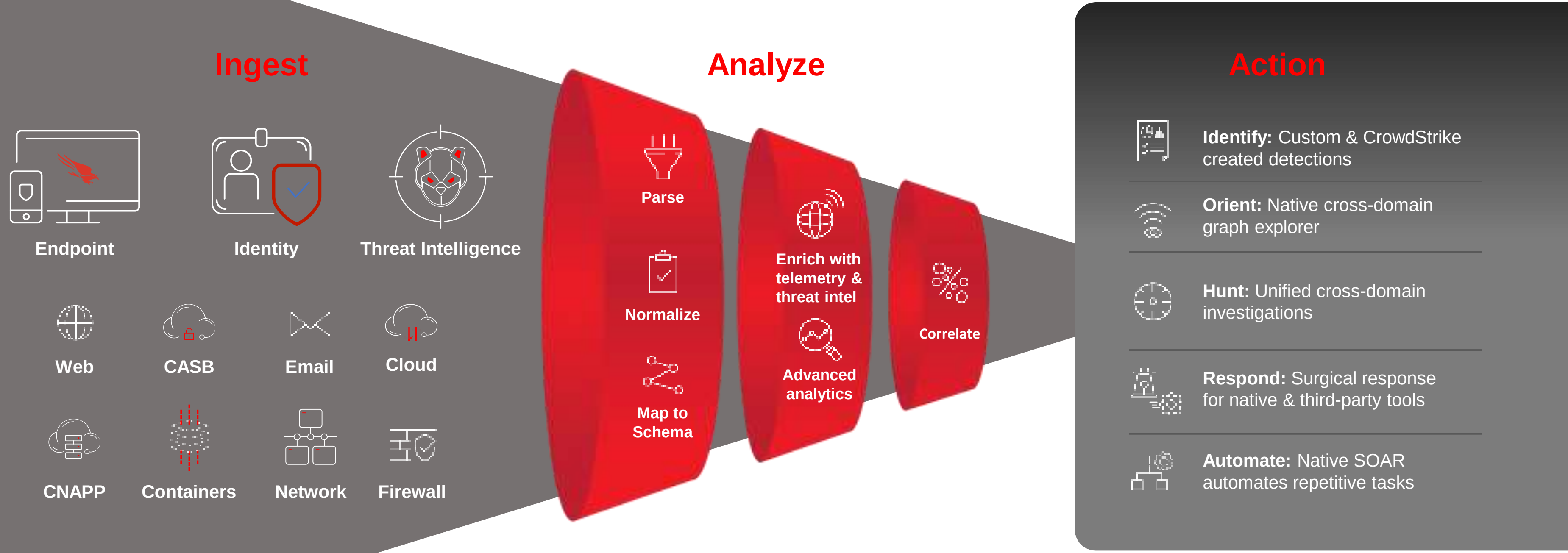
Generate Detections

Store Centrally

Build Relationships for Context

Single User Console

Detect: Unify signals to find the most sophisticated attacks across the entire enterprise



Ingest

- Endpoint
- Identity
- Threat Intelligence
- Web
- CASB
- Email
- Cloud
- CNAPP
- Containers
- Network
- Firewall

Analyze

- Parse
- Normalize
- Map to Schema
- Enrich with telemetry & threat intel
- Advanced analytics
- Correlate

Action

Identify: Custom & CrowdStrike created detections

Orient: Native cross-domain graph explorer

Hunt: Unified cross-domain investigations

Respond: Surgical response for native & third-party tools

Automate: Native SOAR automates repetitive tasks

So what did we learn?

Remember the main problem we are solving – stopping breaches!

Security is a data problem.

Remember to look past the acronym.

Ask your vendors how they are solving this problem!

The future of XDR, here today

Reduce complexity, supercharge SOC efficiency and Stop Breaches!

Thank You!