Endpoint Detection and Response (EDR) Extension

Suggested path forward.

02-03-2022

Update

2nd Track – “Longer Term Detection and Response Schema Extension” (LTDRSE?) - What problem? (subset of asset forensics, not including CASE?)

- Plausible EDR/NDR/XDR/MDR normalization for all threats, across all technologies?
  - Agent telemetry is not normalize-able across products in the same enterprise
    - Different *DR products detect the same mal-behaviors in using very different behaviors/indicators
    - Different *DR products expose detection at very different architectural loci (some at the controller, some at an analytics feed (from cloud), some from the agent.
    - Different *DR products consume response commands at different architectural loci (some at the controller, some at the agent) using different asset identifiers.
  - But almost all *DR products can map their detections into an ATT&CK identification, TTP vector. As Mitre demonstrated by focusing on attack behavior (TTPs), That approach is highly comparable across products,
  - … but still highly variable across products for almost every attack.
  - Also, almost all *DR products have a mapping to some reconcilable Asset Identifier, also variable across products.

2nd Track – Proposed first normalizations?

1. I think we need both identification and behavior normalization, but maybe more (connectivity?)
2. Interacting with *DR at the right place for a specific product (controller, cloud, asset instrumentation, …) => flexible discovery, registration, collection, correlation , analysis
3. Resilient asset identifier (tolerates normal operational dynamics)
   - Probably endpoint GUID or GUID tuple (e,g, Container GUID, Service GUID, …) which can always be mapped to other proxies (e.g. IP current associated with an invariant GUID, generates a, IP trajectory over time)
   - The inverse mapping (e.g. IP-> GUID is not unique (multi-homing , load balancing (IPS), durable (temporally)), enough, not complete (progressive apps), provide no glue to dev/supply chain/context across invocations).
   - On AWS , ARNs solve all of these issues handily, and can always get at other proxies (IP, MAC SSID, other GUIDs) via logs.
   - Normalize for other platforms (cloud , premise, edge, …)
   - Normalize across platforms (multi-cloud (see new NIST MCSWG) and ZT (see NCCoE use case 5))
   - *** Normalize across existing conventional tuple structures ?
     - Ex. (IP, MAC, FQDN, SSID, NetBIOS/DN, (replicated for VMs and their movement)…) - https://www.ibm.com/support/pages/individual-assets-merging-one-asset-many-ip-addresses-mac-addresses-or-hostnames
     - VMware , Greg Frascadore (example for VM dynamics using crypto): https://patents.google.com/patent/US9098318B2/en
     - Microsoft (example for cloud (Azure) asset /abstraction mgmt): Define your naming convention - Cloud Adoption Framework | Microsoft Docs
     - * the motivation for using GUIDs in all cloud platforms becomes clearer … ☺
4. Normalized detections (only unify-able at the attack level (different product TTPs -> same attack), so use ATT&CK ? Or enhanced ATT&CK? Or … (any other candidates/levels of normalization)?
5. Normalized response (ATT&CK TTP action mitigations (product))? Or D3FEND?

2nd Track

Suggestion 1: We should drive to a decision and scoping of a sub project, prior to engaging with external orgs, so that appropriate governance and rules of engagement are in place.

- Table discussions about collaboration until then?

- *Meeting with Mitre strategy folks Friday to setup an OASIS discussion, if you approve -

Suggestion2 : Meeting with EDR and NDR teams to pick their brains, if you approve

- Would like to schedule exploratory discussion with Chris Kruegel, Lastline NDR, VMware – They are facing this correlation challenge (integration) at both the behavior and identifier level (XDR x NDR over dynamic assets. Who else?
- Who else, especially who in OSS NDR/EDR?
  - Comodo – widely used
  - GRR - cloud scale
  - BlueSpawn – academic
  - OSS XDR Challenge: “curated behavior feeds” – Is ATT&CK an answer to this roadblock?
- NDR and XDR are seeing the projections same malware’s behavior, in any attacked environment, but they see the endpoints and behaviors very differently (so do NDR competitors)

Update

- Any group feedback on the second track?
- 2nd Track - What problem?
  - Plausible EDR/NDR/XDR/MDR normalization for all threats, across all technologies?
    - Agent telemetry is not normalize-able across products in the same enterprise
      - Different *DR products detect the same mal-behaviors in using very different behaviors/indicators
      - Different *DR products expose detection at very different architectural loci (some at the controller, some at an analytics feed (from cloud), some from the agent.
      - Different *DR products consume response commands at different architectural loci (some at the controller, some at the agent) using different asset identifiers.
    - But almost all *DR products map their detections into an ATT&CK identification, TTP vector. As Mitre demonstrated, this is highly comparable across products, but still highly variable for almost every attack.
    - Also, almost all *DR products have a mapping to some reconcilable Asset Identifier

2nd Track – Proposed first normalizations?

1. Interacting with *DR at the right place for a specific product (controller, cloud, asset instrumentation, …)
2. Resilient asset identifier (tolerates normal operational dynamics)
   - Probably endpoint GUID or GUID tuple (e,g, Container GUID, Service GUID, …) which can always be mapped to other proxies (e.g. IP current associated with an invariant GUID, generates a, IP trajectory over time)
   - The inverse mapping (e.g. IP-> GUID is not unique (multi-homing , load balancing (IPS), durable (temporally)), enough, not complete (progressive apps), provide no glue to dev/supply chain/context across innvocations).
   - On AWS , ARNs solve all of these issues handily, and can always get at other proxies (IP, MAC SSID, other GUIDs) via logs.
   - Normalize for other platforms (cloud , premise, edge, …)
   - Normalize across platforms (multi-cloud (see new NIST MCSWG) and ZT (see NCCoE use case 5))
3. Normalized detections (only unify-able at the attack level (different product TTPs -> same attack), so use ATT&CK ? Or enhanced ATT&CK? Or …
4. Normalized response (ATT&CK TTP action mitigations (product))? Or D3FEND?

2nd Track – proposed next steps

- Meeting with Mitre strategy folks Friday to setup an OASIS discussion, if you approve
- Meeting with EDR and NDR teams to pick their brains, if you approve

Or, … is this the right time for this group to grapple with this?

- EO EDR mandate
- EO modernization mandate (for infra, apps and cyber)
- …

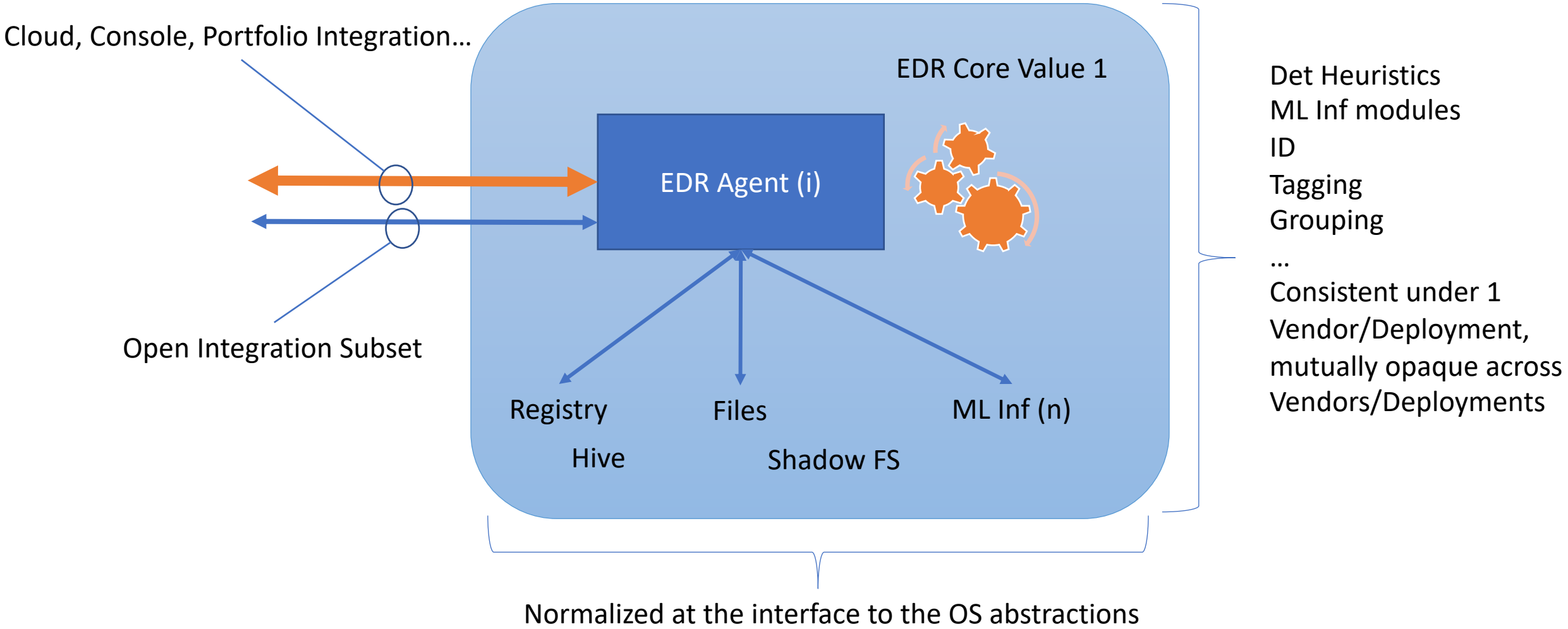
Restatement of Recommendation from last Update

- Two parallel tracks
  1. Continue to do what can be done with existing mapping approach
     - Has hard limits requiring additional parallel mechanisms
     - Enhanced by interacting with EDR systems, beyond just instrumented endpoints.
     - Can happen fast and needs a plan
  2. Investigate the potential of leveraging existing models to extend the normalization of EDR/XDR consumption
     - More general enablement of normalized EDR consumption for more use cases
     - Requires analysis, debate and design
     - I'd like to lead or co-lead this effort

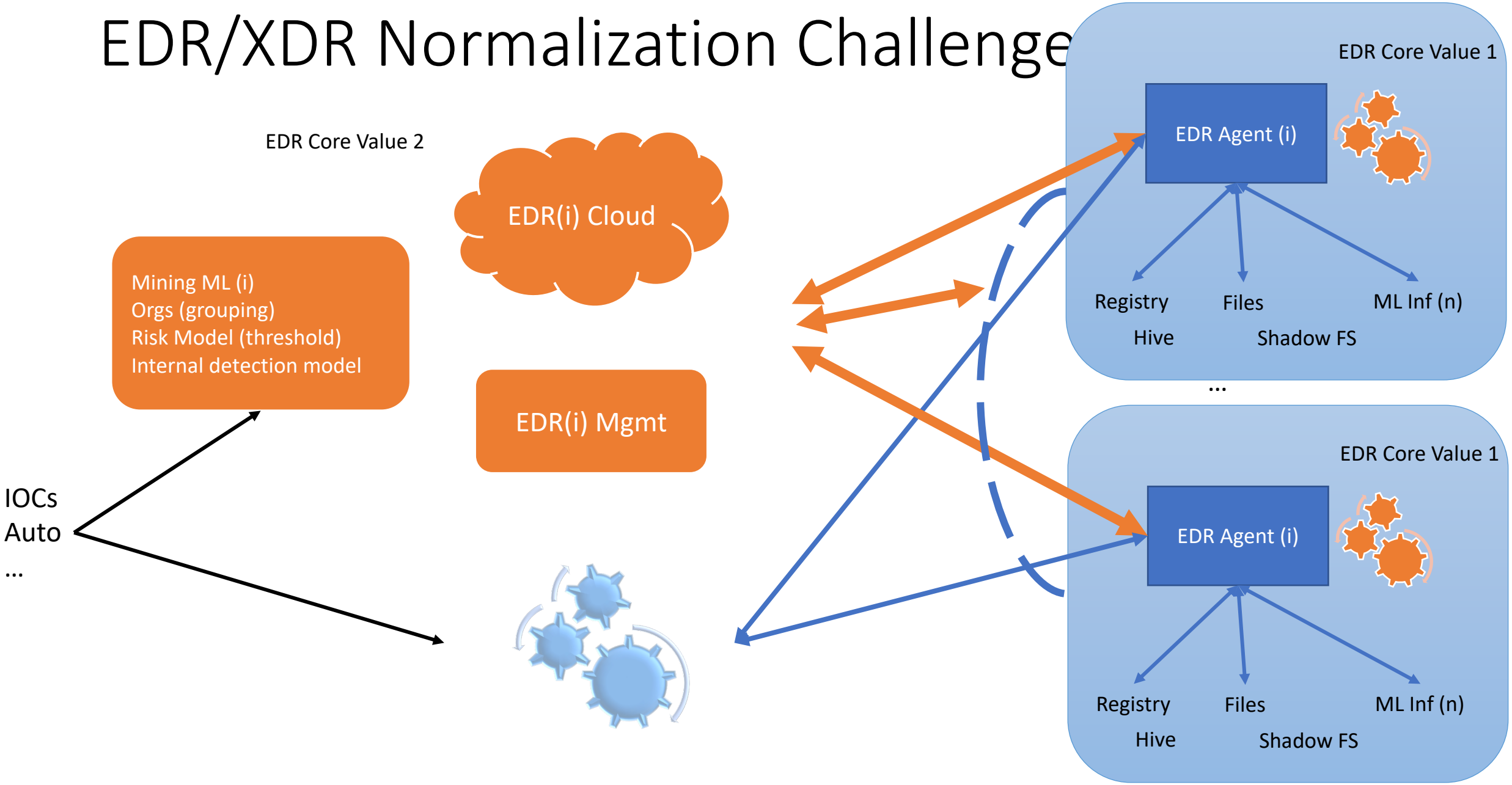
Update - Dennis

- Suggestion 1: Make sure we design to interact with EDR systems, not solely with instrumented EDR endpoints
  - Strong contextual, detection, analysis, explain-ability and action consistency within an EDR system.
  - Working on how we extend (information architecture) to incorporate the EDR system view.
- Suggestion 2: I believe that we need models to expand use cases significantly
  - Rationale follows…

EDR Normalization Challenge



EDR/XDR Normalization Challenge

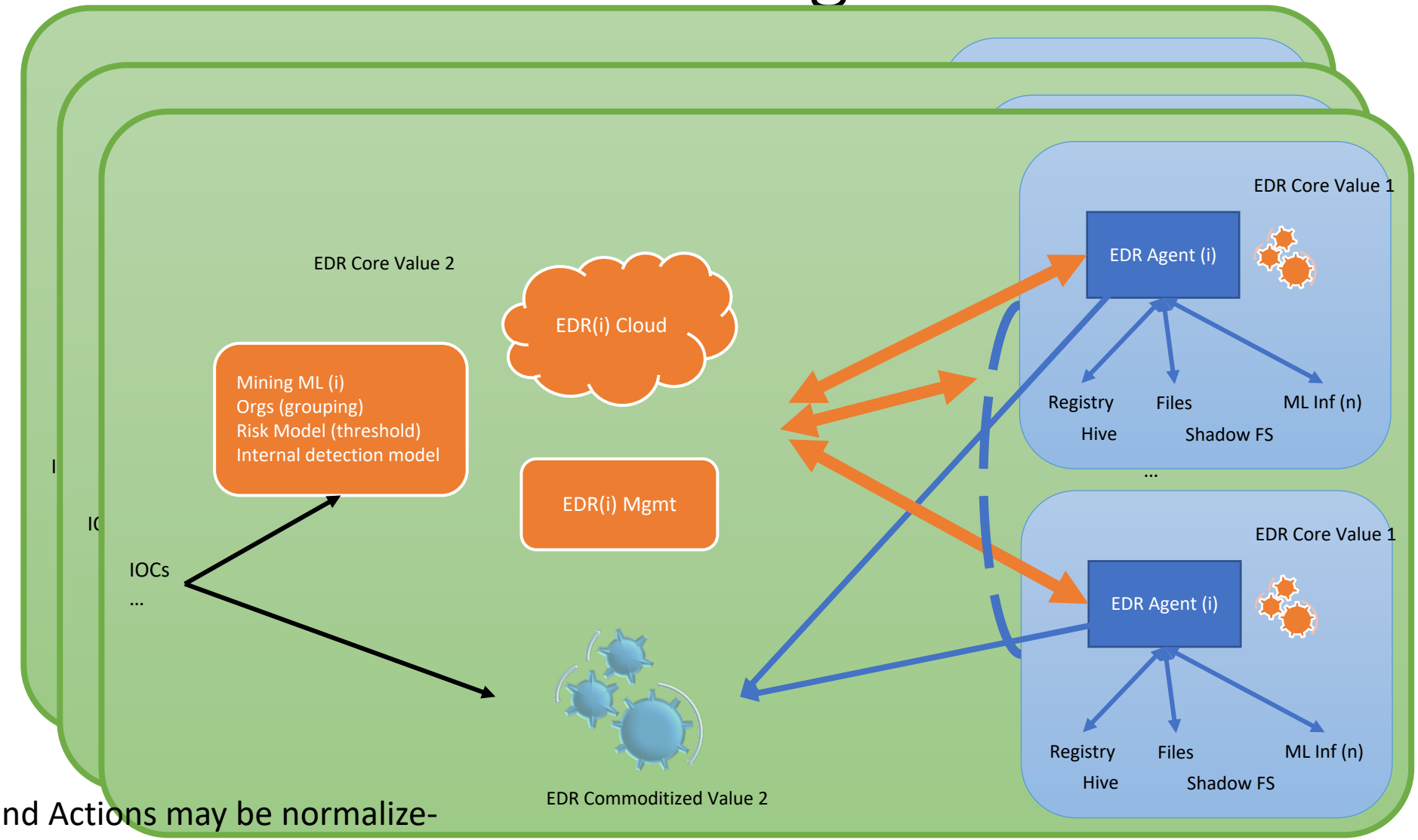


EDR/XDR Normalization Challenge

Context, heuristics, ML training, ML inference, grouping, management topology… are effectively silo'd

Comparability, explain-ablility, and interpretability are only possible across consistent underlying attributes/relationships.

Hunting, analysis, planning, actions at scale … all need context that is not unifyable across vendors.



*Communicating Indicators and Actions may be normalize-able, but may not be enough for effective EDR operation

Stix-Shifter:

Highlights the limits of model-less normalization xEDRs

Distributing IOCs , fielding simple alerts and taking simple action may work fine, if aimed at the EDR as a system ... and if Stix-Shifter mappings are expanded consistently.

Semantic inconsistencies that will interfere with xEDR sense making, decision support and action:

xEDR attrib relationships
xEDR attrib representations
Opaque unjoinable IDs

Normalizing the consumption of EDR capability, via the Stix-Shifter mapping approach won't work, due to limitations in what products expose (attributes, reps, analytics, inf, train, …mgmt).

We need a model… probably two models

CarbonBlack

STIX Object	STIX Property	Data Source Field
directory	path	process_path
directory	path	parent_path
file	name	process_name
file	hashes.MD5	process_md5
file	hashes.SHA-256	process_sha256
file	parent_directory_ref	process_path
file	name	parent_name
file	hashes.MD5	parent_md5
file	hashes.SHA-256	parent_sha256
file	parent_directory_ref	parent_path
process	creator_user_ref	process_username
process	created	process_start_time
process	name	process_name
process	binary_ref	process_name
process	pid	process_pid
process	x_unique_id	process_guid
process	command_line	process_cmdline
process	name	parent_name
process	binary_ref	parent_name
process	parent_ref	parent_name
process	pid	parent_pid
process	x_unique_id	parent_guid
process	command_line	parent_cmdline
user-account	user_id	process_username
x-cbcloud	device_name	device_name
x-cbcloud	device_internal_ip	device_internal_ip
x-cbcloud	device_external_ip	device_external_ip
x-cbcloud	device_os	device_os
x-cbcloud	device_id	device_id
x-cbcloud	device_timestamp	device_timestamp
x-cbcloud	org_id	org_id
x-cbcloud	device_group_id	device_group_id
x-cbcloud	process_terminated	process_terminated
x-cbcloud	regmod_count	regmod_count
x-cbcloud	netconn_count	netconn_count
x-cbcloud	filemod_count	filemod_count
x-cbcloud	modload_count	modload_count
x-cbcloud	childproc_count	childproc_count
x-cbcloud	crossproc_count	crossproc_count
x-cbcloud	scriptload_count	scriptload_count

Trend (XDR-ish)

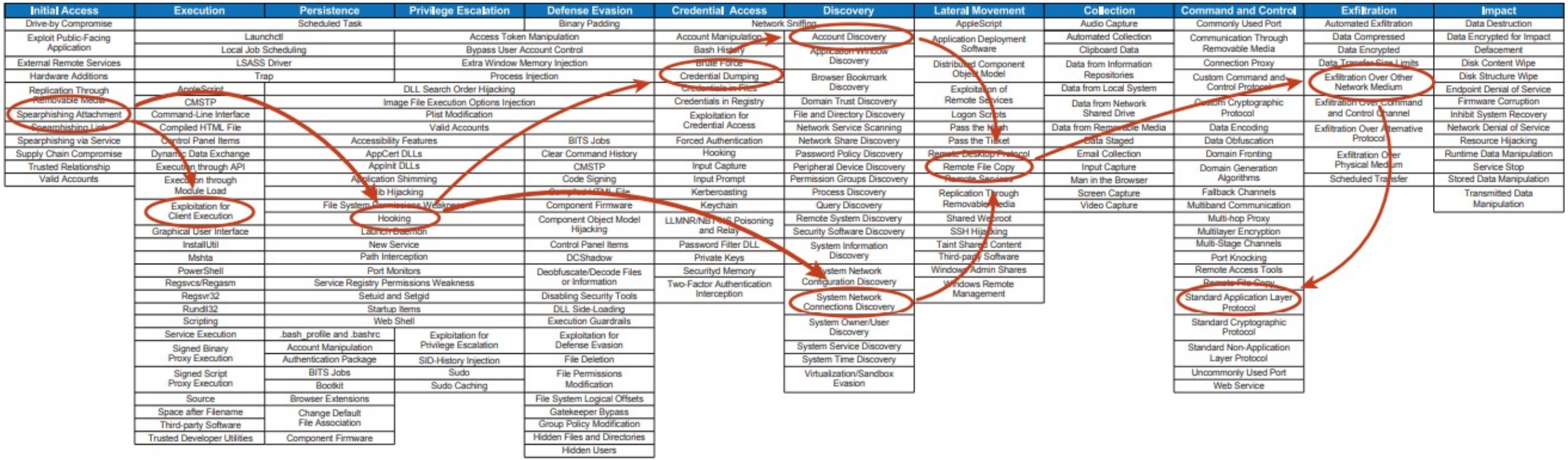
STIX Object	STIX Property	Data Source Field
directory	path	objectFilePath
directory	path	processFilePath
directory	path	parentFilePath
directory	path	srcFilePath
domain-name	value	hostName
domain-name	value	objectHostName
domain-name	value	source_domain
email-addr	value	mail_message_sender
email-addr	value	mail_message_recipient
email-message	sender_ref	mail_message_sender
email-message	is_multipart	mail_message_sender
email-message	to_refs	mail_message_recipient
email-message	is_multipart	mail_message_recipient
email-message	subject	mail_message_subject
email-message	is_multipart	mail_message_subject
email-message	date	mail_message_delivery_time
email-message	is_multipart	mail_message_delivery_time
email-message	additional_header_fields	mail_internet_headers
file	hashes.SHA-1	objectFileHashSha1
file	name	objectFilePath
file	parent_directory_ref	objectFilePath
file	hashes.SHA-1	processFileHashSha1
file	name	processFilePath
file	parent_directory_ref	processFilePath
file	hashes.SHA-1	parentFileHashSha1
file	name	parentFilePath
file	parent_directory_ref	parentFilePath
file	name	srcFilePath
file	parent_directory_ref	srcFilePath
file	hashes.SHA-1	srcFileHashSha1
file	name	file_name
file	hashes.SHA-1	file_sha1
ipv4-addr	value	src
ipv4-addr	value	dst
ipv4-addr	value	endpointIp
ipv4-addr	value	objectIp
ipv4-addr	value	objectIps
ipv4-addr	value	source_ip
ipv6-addr	value	src
ipv6-addr	value	dst
ipv6-addr	value	endpointIp
ipv6-addr	value	objectIps
ipv6-addr	value	source_ip
network-traffic	src_ref	src
network-traffic	protocols	src
network-traffic	src_port	spt
network-traffic	protocols	spt
network-traffic	dst_ref	dst
network-traffic	protocols	dst
network-traffic	dst_port	dpt
network-traffic	protocols	dpt
network-traffic	dst_ref	objectIp
network-traffic	protocols	objectIp
network-traffic	dst_port	objectPort
network-traffic	protocols	objectPort
network-traffic	src_ref	source_ip
network-traffic	protocols	source_ip
process	command_line	objectCmd
process	binary_ref	objectFileHashSha1
process	binary_ref	objectFilePath
process	command_line	processCmd
process	binary_ref	processFileHashSha1
process	binary_ref	processFilePath
process	command_line	parentCmd
process	binary_ref	parentFileHashSha1
process	binary_ref	parentFilePath
url	value	request
url	value	mail_urls
user-account	account_login	logonUser
user-account	user_id	objectUser
windows-registry-key	key	objectRegistryKeyHandle
windows-registry-key	values	objectRegistryValueType

CrowdStrike

STIX Object	STIX Property	Data Source Field
directory	path	filepath
domain-name	Value	domain_ioc
File	Name	filename
file	parent_directory_ref	filepath
file	hashes.SHA-256	sha256
file	hashes.MD5	md5
file	hashes.SHA-256	parent_sha256
file	hashes.SHA-256	sha256_ioc
file	hashes.SHA-256	quarantined_file_sha256
file	hashes.MD5	md5_ioc
file	hashes.MD5	parent_md5
ipv4-addr	value	external_ip
ipv4-addr	value	local_ip
mac-addr	value	mac_address
network-traffic	dst_ref	domain_ioc
process	binary_ref	filename
process	name	filename
process	binary_ref	filepath
process	command_line	cmdline
process	creator_user_ref	user_name
process	creator_user_ref	user_id
process	binary_ref	parent_sha256
process	parent_ref	parent_sha256
process	pid	parent_process_graph_id
process	parent_ref	parent_process_graph_id
process	pid	triggering_process_graph_id
process	binary_ref	parent_md5
process	parent_ref	parent_md5
process	command_line	parent_cmdline
process	parent_ref	parent_cmdline
user-account	account_login	user_name
user-account	user_id	user_id
windows-registry-key	key	registry_key
x-crowdstrike	machine_domain	machine_domain
x-crowdstrike	device_id	device_id
x-crowdstrike	detection_id	detection_id
x-crowdstrike	scenario	scenario
x-crowdstrike	technique	technique
x-crowdstrike	tactic	tactic
x-crowdstrike	tactic_id	tactic_id
x-crowdstrike	technique_id	technique_id
x-crowdstrike	agent_local_time	agent_local_time
x-crowdstrike	agent_version	agent_version
x-crowdstrike	first_seen	first_seen
x-crowdstrike	last_seen	last_seen
x-crowdstrike	platform_id	platform_id
x-crowdstrike	confidence	confidence
x-crowdstrike	ioc_type	ioc_type
x-crowdstrike	ioc_value	ioc_value
x-crowdstrike	ioc_value	bios_manufacturer
x-crowdstrike	ioc_value	bios_version
x-crowdstrike	ioc_value	config_id_base
x-crowdstrike	ioc_value	config_id_build
x-crowdstrike	ioc_value	config_id_platform
x-crowdstrike	ioc_value	product_type
x-crowdstrike	ioc_value	product_type_desc
x-crowdstrike	ioc_value	site_name
x-crowdstrike	ioc_value	system_product_name
x-crowdstrike	ioc_value	modified_timestamp
x-oca-asset	ip_refs	external_ip
x-oca-asset	hostname	hostname
x-oca-asset	ip_refs	local_ip
x-oca-asset	mac_refs	mac_address
x-oca-asset	os_version	os_version
x-oca-asset	os_platform	platform_name
x-oca-event	created	timestamp
x-oca-event	process_ref	filename
x-oca-event	action	display_name
x-oca-event	outcome	description
x-oca-event	registry_ref	registry_key
x-oca-event	network_ref	domain_ioc
x-oca-event	file_ref	sha256_ioc
x-oca-event	file_ref	quarantined_file_sha256
x-oca-event	file_ref	md5_ioc
x-oca-event	parent_process_ref	parent_md5
x-oca-event	host_ref	hostname
x-oca-event	provider	provider
x-oca-event	severity	severity

Ref. https://github.com/opencybersecurityalliance/stix-shifter/tree/develop/adapter-guide

Malware behavior: invariant across EDR/XDRs (good normalization candidate)



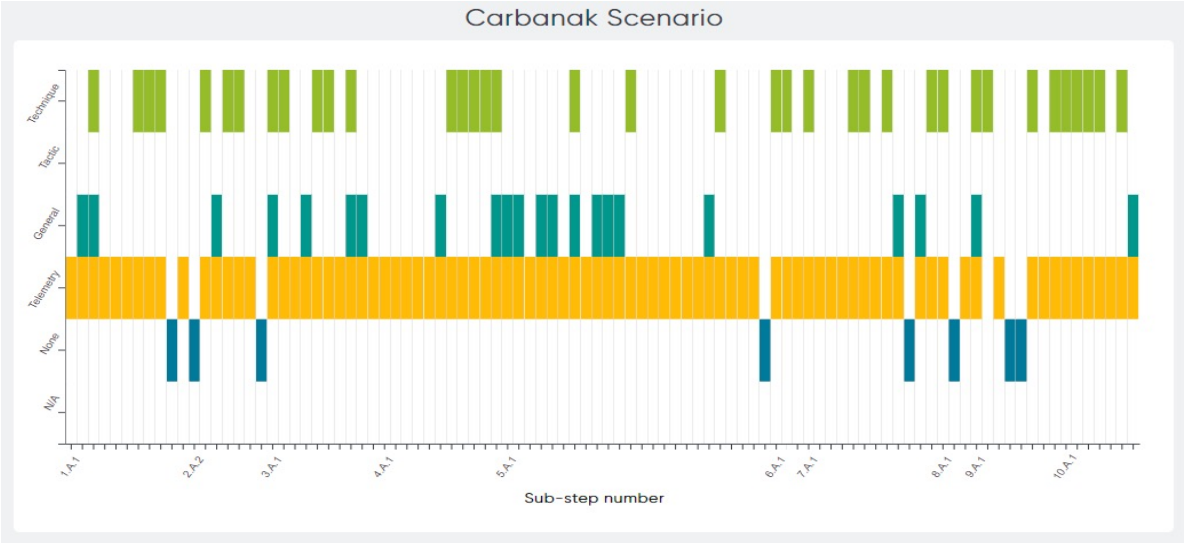
Representative malware behavior and detection is only visible at the EDR/XDR system level. Not in endpoint telemetry. Consider “action profile detection” vs “HMM detection” or “Kalman detection” … completely different (inconsistent) X EDRs

Ref: https://attack.mitre.org/docs/attack_roadmap_2020_october.pdf

Different EDR/XDR tools observe, detect and respond very differently

Ref. https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/

Carbon Black

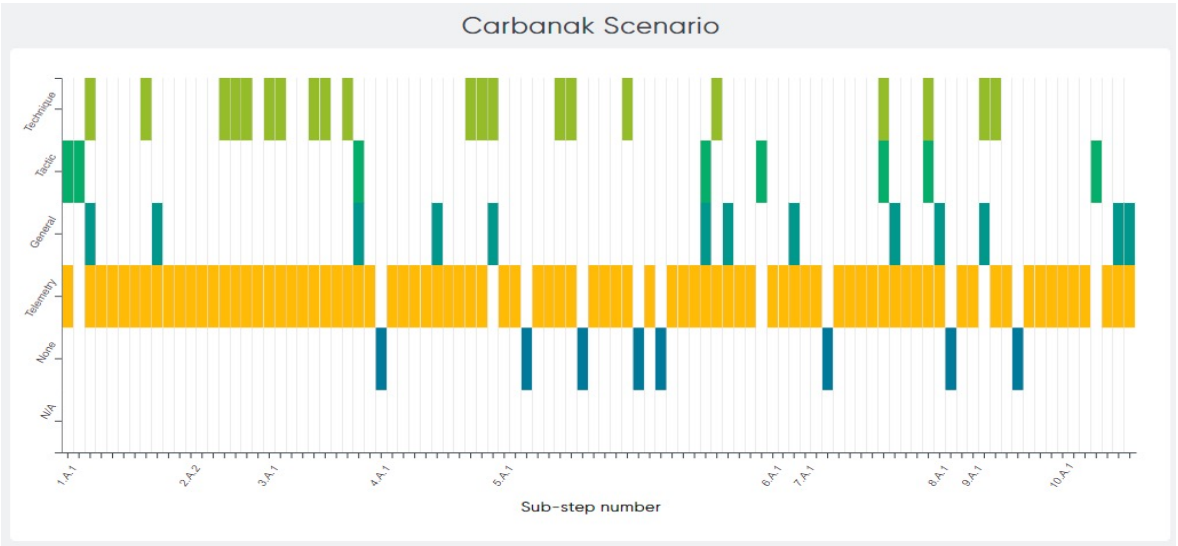


No clear basis for interpretability, explain-ability or actionability across different EDR/XDR tools at the telemetry or detection (largely cloud based) level.

Normalizing at the TTP level (via mapping) makes these semantic and action discontinuities clear.

IOCs and “actions” mask these fundamental differences, for all but the simplest actions and indications. Supply Chain and Ransomware exploits are much more complex, and often with little or know prior knowledge when it matters most (during hunting, anomaly and behavioral recognition).

FireEye

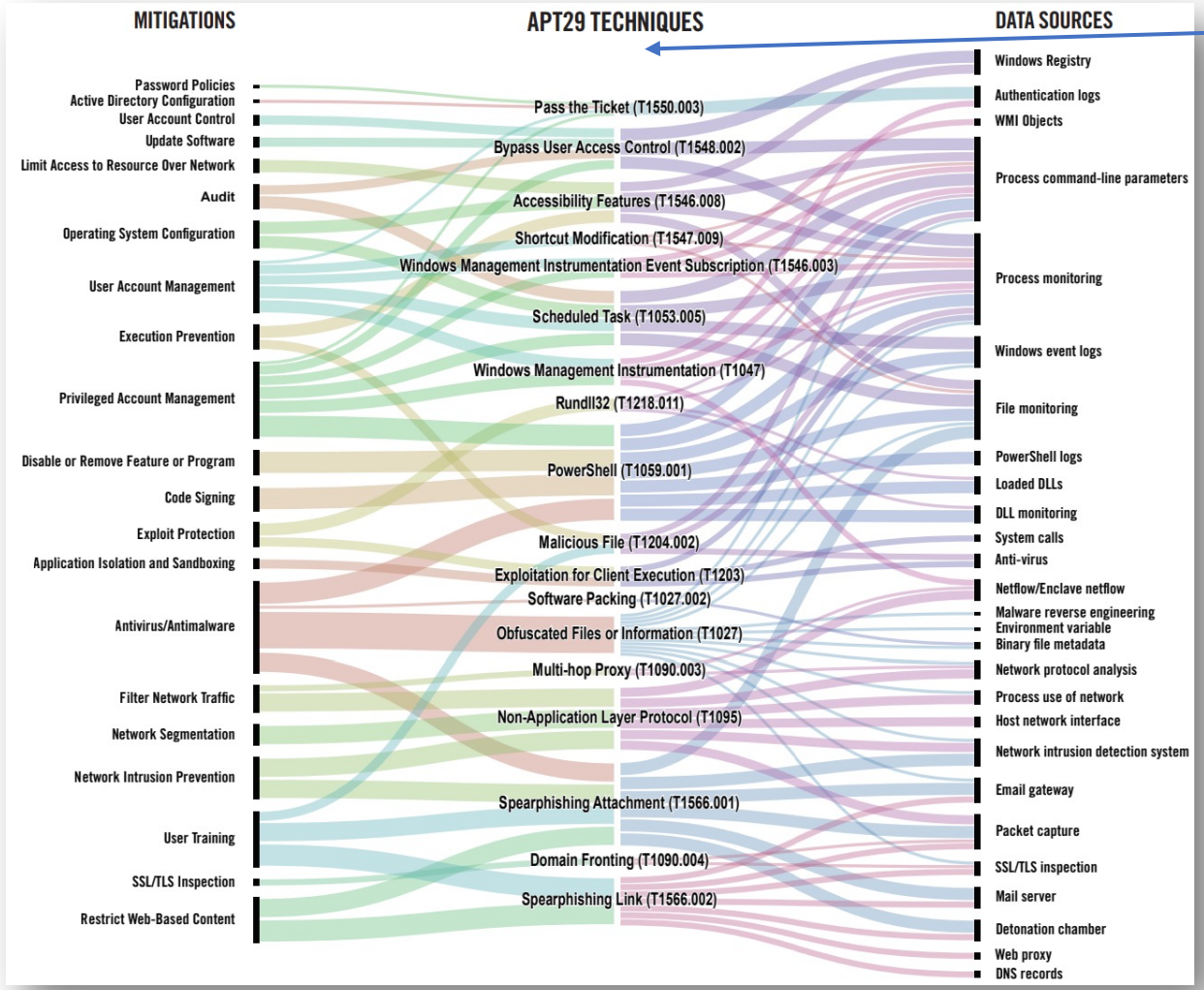


Needed to support EDR/XDR use cases (hunting, analysis mitigation planning, …)

Different EDR/XDR tools detect very differently

Different EDR/XDR tools mitigate (act) differently

Different EDR/XDR tools use different basis set



Ref: https://attack.mitre.org/docs/attack_roadmap_2020_october.pdf

* This is far less of a problem for detection and response over exactly 1 EDR/XDR solution per enterprise.

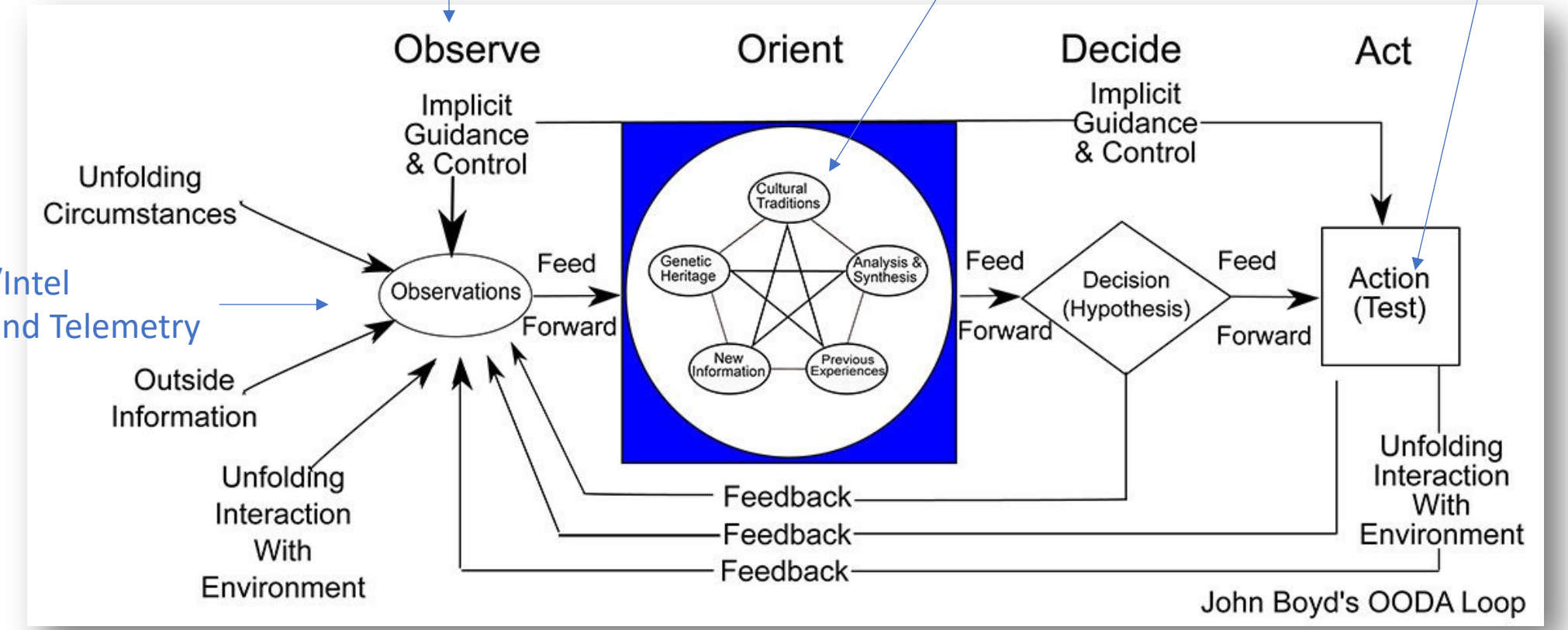
Inconsistencies across EDR/XDR break OODA; for a single EDR/XDR this is far less of a problem

Intention/Provisioning/Architecture

Model-Informed Orientation (different in every EDR)

Correct action and feedback efficacy both depend on a working model

Telemetry/Intel
EDR IOCs and Telemetry



Ref. https://commons.wikimedia.org/wiki/File:OODA.Boyd.svg

Recommendation

- Two parallel tracks
  1. Continue to do what can be done with existing mapping approach
     - Has hard limits requiring additional parallel mechanisms
     - Enhanced by interacting with EDR systems, beyond just instrumented endpoints.
     - Can happen fast
  2. Investigate the potential of leveraging existing models to extend the normalization of EDR/XDR consumption
     - More general enablement of normalized EDR consumption for more use cases
     - Requires analysis, debate and design
  3. 1. and 2. above are highly complementary, probably mutually necessary to cultivate sustainable communities of interest, and to influence the market.

  So, I'd like to still proceed on the expanded analysis proposed in the last meeting

Previous work follows …

EDR Now

- Mitre key EDR components
  - https://heimdalsecurity.com/blog/what-is-edr-endpoint-detection-and-response/
  - Endpoint data Collection
  - Data Analysis and Forensics
  - Threat Hunting – Chasing and resolving inconsistencies, indicators, outliers
  - Automated response to block malicious activity
- Gartner primary EDR capabilities
  - https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions
  - Detect Security Incidents
  - Contain Incident at the endpoint
  - Investigate security incidents
  - Provide remediation guidance
  - File-based and file-less threats

*Forrester EDR -> XDR :

From Adapt or Die: EDR is Dead, Forrester – Crowdstrike, PAN, Trend … April 28, 2021

- In XDR the endpoint becomes the correlation anchor, across sensing modalities, business context, and security tooling – consolidating related alerts across its data lake into a single incident.
- In XDR, all offerings support automated RCA (in EDR: Trend, Kaspersky). *Extends detection to entire attack lifecycle.*
- In XDR, responses are analytics triggered workflows, adaptively triggering (risk or criteria) captive playbooks. *Risk-based triggers, policy structure/logic and orchestration are offering specific and externally opaque.*
- In XDR, beyond endpoint telemetry, includes network, platform, user, device, … in one place. (for analysis, ML training, pivoting, …) . Hunting, causal analysis, mitigation planning, … are all more accessible without cobbling across tools.

*Current XDR design drivers

- In modern attacks, coherent telemetry across all endpoints is necessary (workstations, servers, mobile devices, cloud assets, …)
- Cloud hosted data lake, analytics, training require cloud hosting for elasticity and pervasive availability, despite enterprise compromise.
- Many enterprise will augment with, or rely on MDR to gain security analyst, hunting, mitigation planning expertise.

EDR Tools Now - Open Source

- *Wazuh – OSSEC ++
- *OSSEC – LIDS (xEndpoint), MW & RK detection, Automatable Actions, FIM, Inventory
- *TheHive Cortex - IP, URL, domain, hashes, files, containment integration
- OSQuery – very generic host monitoring (configuration, performance , infrastructure health), + FIM, YARA (file artifacts) scanning, anomaly detection, process auditing, log settings, …
- *GRR – YARA, APIs, search and collect : files, reg, procs, mem cap, CPU, network, context … all OSs, massive scale, full API, full cloud enablement/leveraging
- MIG – logs, files, memory, network, auditing, vulnerability mgmt, … eroding forensics
- Volatility – digital forensics & incident response, EDR ++ (forensic dimension)
- Complementary Open Source (NDRish)
  - NESSUS –
  - SNORT –
  - Ethercap –
  - Infection Monkey – (Guardicore)

* Multi-endpoint enabled comparison, analytics, behavior, detection. Querying individual endpoints severely limits EDR utility for these OS EDR tools.

EDR Tools Now - Commercial

Gartner EPP MQ Leaders

- Microsoft - Defender for Endpoint
- Crowdstrike - Falcon
- Trend Micro Apex One – XDR for Cloud (Cloud One)
- SentinelOne - Singularity
- McAfee – MVISION EDR
- Sophos – Intercept-X
- 13 non-Leaders

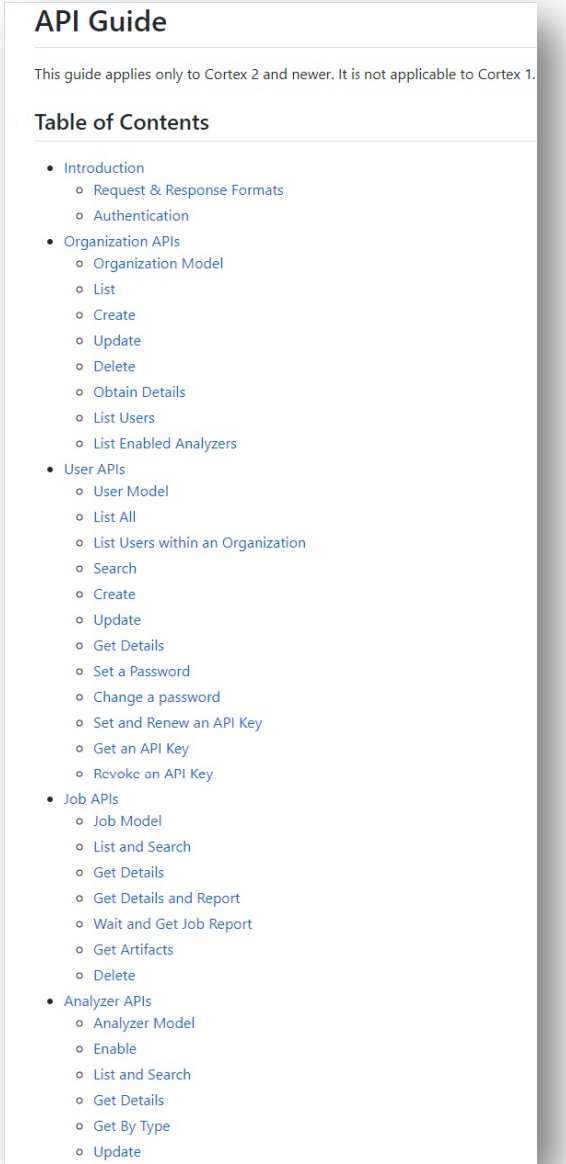
Very different models, semantics, actions, integrations, positioning

But EDR queries, results and semantics are highly balkanized

- Different EDR interaction models: Structured API model , Query, Analyzers (which the refer artifacts), inter-endpoint…
- Different property/attribute/value naming and representations – not too bad at the OS, but diverges as synthetic artifacts get referenced
- Semantics can be wildly different:
  - Different detection approaches have different SNR, meaning and mitigation contexts (nw detection of any anomaly only informs network mitigation; ep detection may not know about any nw mitigations (.g. virtual patching))
  - Virtual patching at an upstream firewall, is not comparable to actual patching of a discovered vulnerability.
- Example: See STIX Shifter

Example: Cortext 2

Cortex 2 API: https://github.com/TheHive-Project/CortexDocs/blob/master/api/api-guide.md#analyzer-model



API Guide

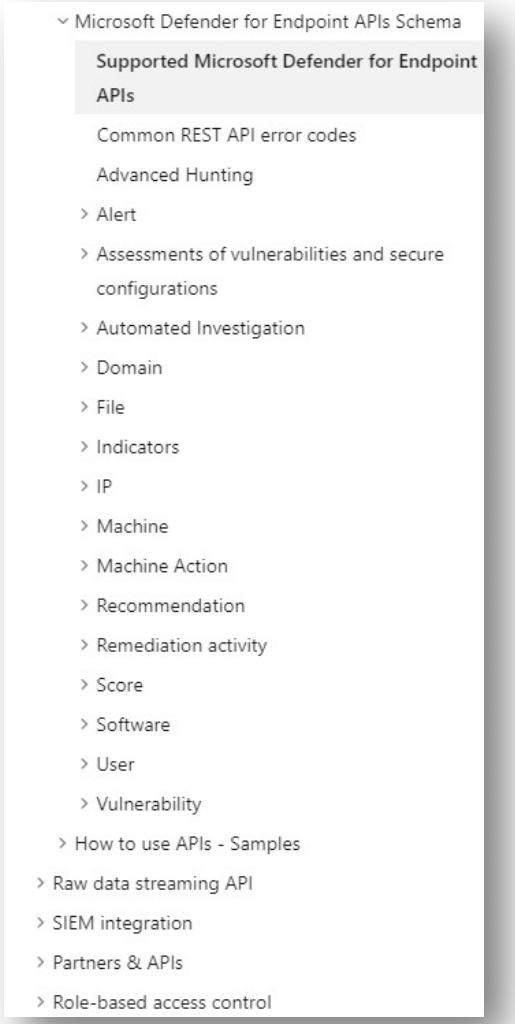
This guide applies only to Cortex 2 and newer. It is not applicable to Cortex 1.

Table of Contents

- Not artifact centric. Stimulate analyzers that the touch whatever observables they need to.
- Heavily focused on the process of orchestrating EDR across roles and controlling access to the observables.
- Enables analysis, detection and response across endpoints.
- Many internally defined abstractions (orgs, users, jobs, analyzers, …). Conventional EDR is embedded.
- There is a file analyzer.

Example: Microsoft Defender for Endpoint

Defender for Endpoint API: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/ti-indicator?view=o365-worldwide



Properties

Property	Type	Description
id	String	Identity of the Indicator entity.
indicatorValue	String	The value of the Indicator.
indicatorType	Enum	Type of the indicator. Possible values are: "FileSha1", "FileSha256", "FileMd5", "CertificateThumbprint", "IpAddress", "DomainName" and "Url".
application	String	The application associated with the indicator.
action	Enum	The action that will be taken if the indicator will be discovered in the organization. Possible values are: "Warn", "Block", "Audit", "Alert", "AlertAndBlock", "BlockAndRemediate" and "Allowed".
externalID	String	Id the customer can submit in the request for custom correlation.
sourceType	Enum	"User" in case the Indicator created by a user (for example, from the portal), "AadApp" in case it submitted using automated application via the API.
createdBySource	string	The name of the user/application that submitted the indicator.
createdBy	String	Unique identity of the user/application that submitted the indicator.
lastUpdatedBy	String	Identity of the user/application that last updated the indicator.
creationTimeDateTimeUtc	DateTimeOffset	The date and time when the indicator was created.
expirationTime	DateTimeOffset	The expiration time of the indicator.
lastUpdateTime	DateTimeOffset	The last time the indicator was updated.
severity	Enum	The severity of the indicator. possible values are: "Informational", "Low", "Medium" and "High".
title	String	Indicator title.
description	String	Description of the indicator.
recommendedActions	String	Recommended actions for the indicator.
rbacGroupNames	List of strings	RBAC device group names where the indicator is exposed and active. Empty list in case it exposed to all devices.
rbacGroupIds	List of strings	RBAC device group ID's where the indicator is exposed and active. Empty list in case it exposed to all devices.
generateAlert	Enum	**True** if alert generation is required. **False** if this indicator should not generate an alert.

Method	Return Type	Description
List MachineActions	Machine Action	List Machine Action entities.
Get MachineAction	Machine Action	Get a single Machine Action entity.
Collect investigation package	Machine Action	Collect investigation package from a machine.
Get investigation package SAS URI	Machine Action	Get URI for downloading the investigation package.
Isolate machine	Machine Action	Isolate machine from network.
Release machine from isolation	Machine Action	Release machine from Isolation.
Restrict app execution	Machine Action	Restrict application execution.
Remove app restriction	Machine Action	Remove application execution restriction.
Run antivirus scan	Machine Action	Run an AV scan using Windows Defender (when applicable).
Offboard machine	Machine Action	Offboard machine from Microsoft Defender for Endpoint.
Stop and quarantine file	Machine Action	Stop execution of a file on a machine and delete it.
Run live response	Machine Action	Runs a sequence of live response commands on a device
Get live response result	URL entity	Retrieves specific live response command result download link by its index.
Cancel machine action	Machine Action	Cancel an active machine action.

- Very artifact centric..
- Unique abstractions (e.g. “investigation package”)
- Deep integration of opaque analytics, correlation, policy driven actions.

EDR, NDR, XDR, and MDR are converging.

- *Gartner labels the market for technology in this convergence EPP subsuming EDR.
  - Endpoint and network convergence is accelerating. All attacks exhibit both. Detect++
  - By 2032 YE, cloud delivered EPP will exceed 95% of deployments
  - By 2025 50% of EDR users will be using managed detection and response
  - By 2025 60% of EDR solutions will include data from multiple security control sources, such as Identity, CASB and DLP
- Question: Do we address this rapidly consolidating EPP space, which includes EDR, NDR, XDR, MDR? Or focus on the evaporating conventional EDR space?
- Concern: Directly interacting with endpoints, about files processes, hashes, simple indicators … does not seem to be the center of EDR-EPP detection or action.

*Gartner EPP MQ May 2021

OASIS OpenC2-ap-edr

openc2-ap-edr - Defining Actions, Targets, Specifiers and Options that are consistent with the version 1.0 of the OpenC2 Language Specification in the context of command and control of various endpoint detection and response technologies.

https://github.com/oasis-tcs/openc2-ap-edr

Q: How much of this scope, do we envision covering?

Q: If not all, how do we describe the subset we will cover?

Assumption: Schema extension must be a semantic and context cover of the scope we embrace.

Utility of Mitre ATT&CK is growing

- Comparing EDR, NDR, XDR, MDR detection coverage
- Bridging endpoint and network observed behaviors and state
- Normalizing results (via mappings) across EDR, NDR, XDR, MDR offerings
- Augmentation with Detection and Mitigation alternatives for same Procedure
- TTPs across layers of abstraction:
  - Enterprise - OS, Cloud, Network, Container,
  - Mobile ,
  - ICS
- …and across endpoints

Big Question

Question: Should we be integrating the schema at EDR system abstractions, rather than endpoint EDR instrumentation tool?

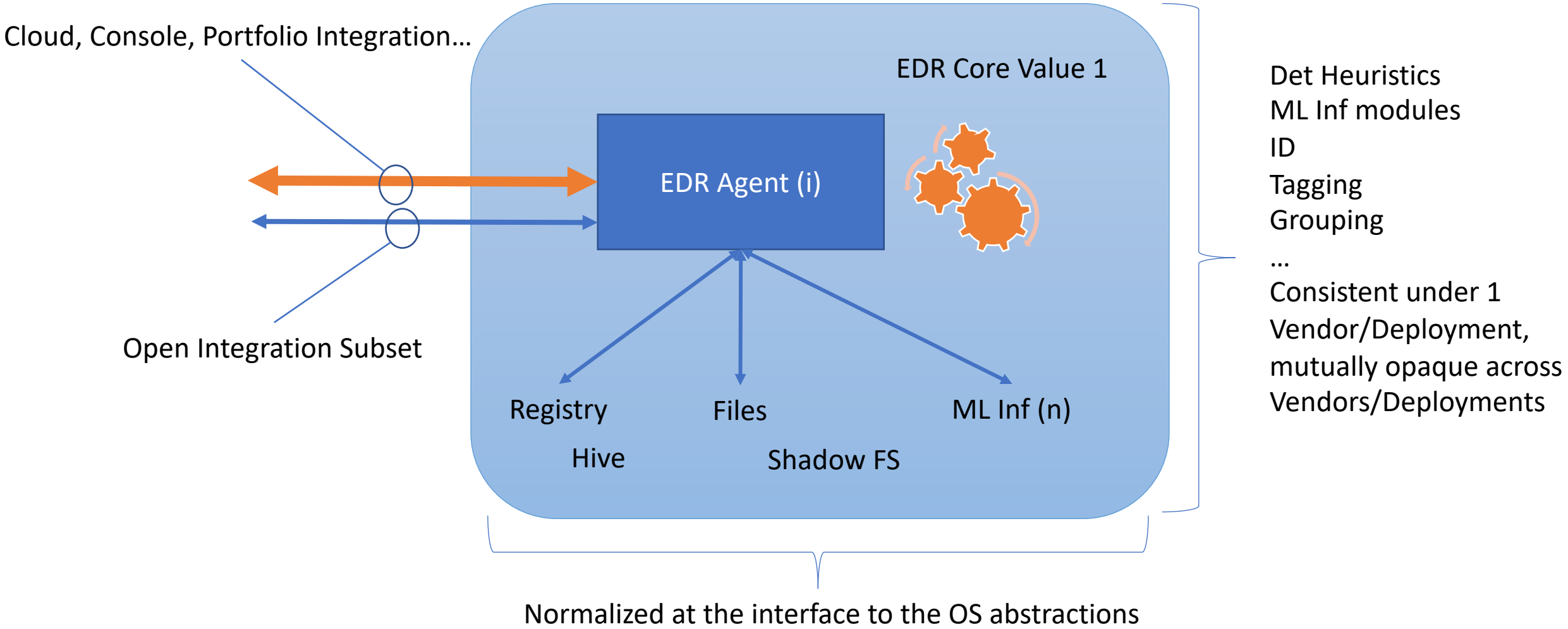
- Would leverage higher level functionality.
- Would leverage pre-existing policy orchestration and automation.
- Would leverage real-time in-line controls.

Appendix

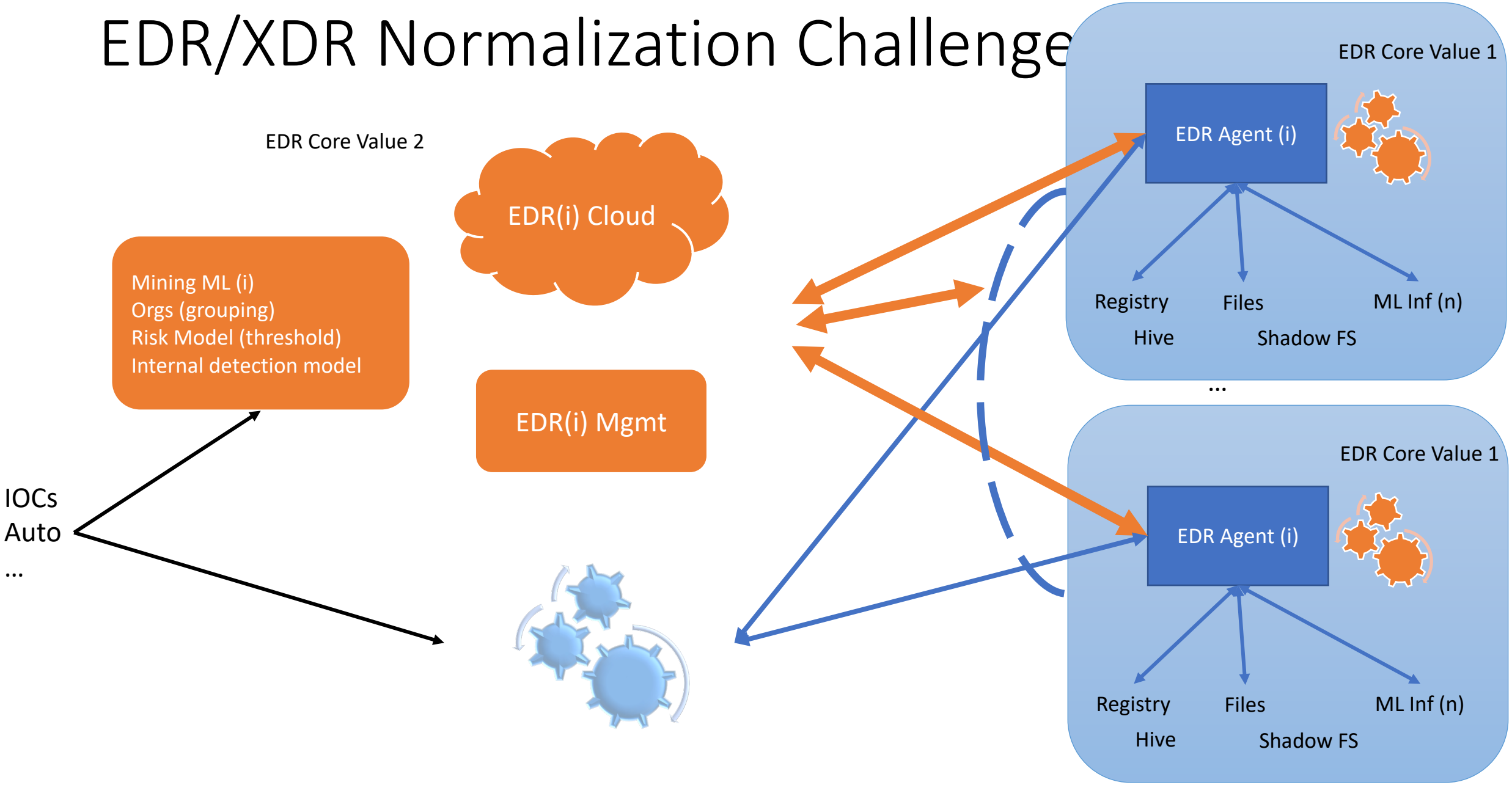
Suggestions

- Make sure we design to interact with EDR systems, not solely with instrumented EDR endpoints
  - Strong contextual, detection, analysis, explain-ability and action consistency within an EDR system.
  - Working on how we extend (information architecture) to incorporate the EDR system view.

EDR Normalization Challenge



EDR/XDR Normalization Challenge

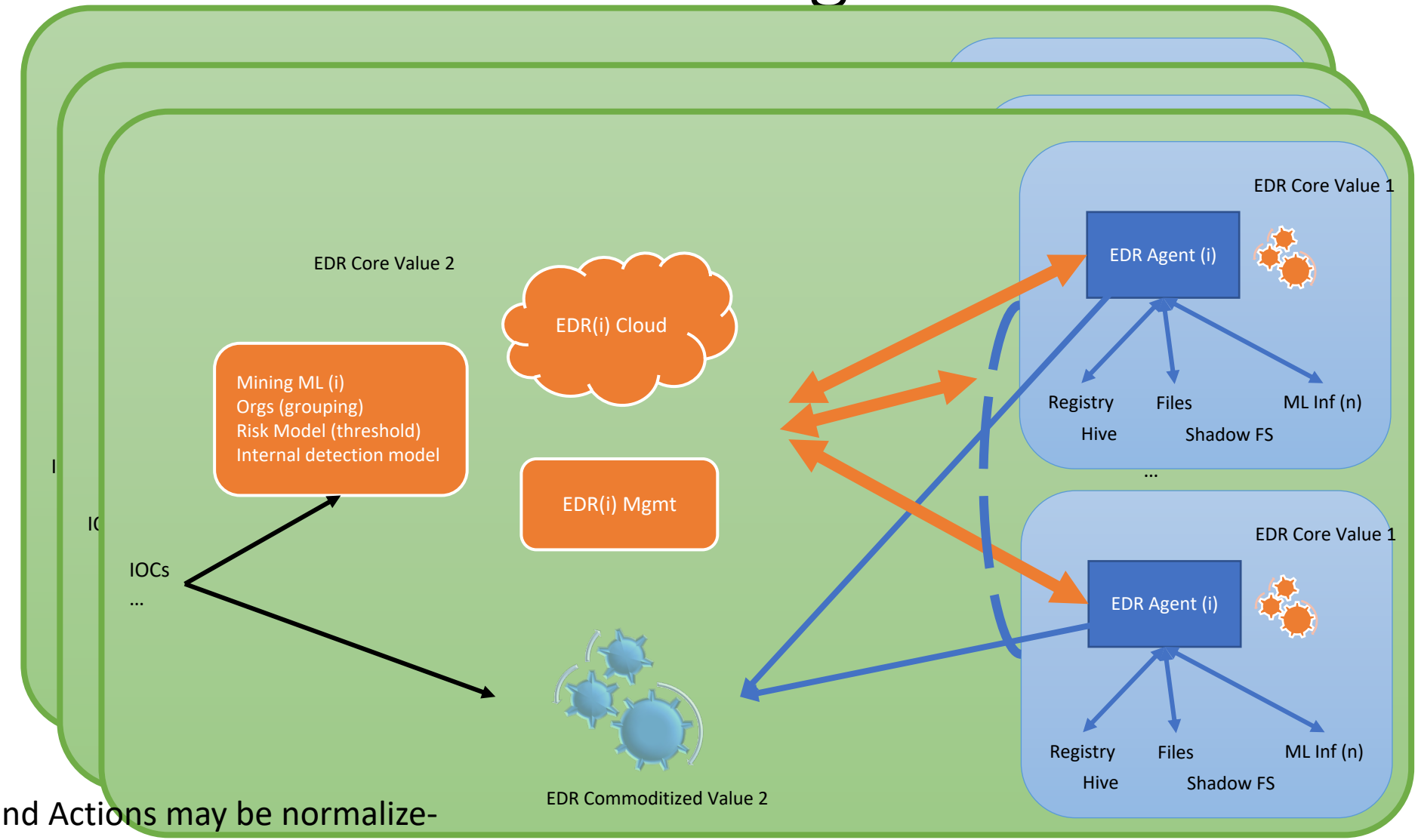


EDR/XDR Normalization Challenge

Context, heuristics, ML training, ML inference, grouping, management topology… are effectively silo'd

Comparability, explain-ablility, and interpretability are only possible across consistent underlying attributes/relationships.

Hunting, analysis, planning, actions at scale … all need context that is not unifyable across vendors.



*Communicating Indicators and Actions may be normalize-able, but may not be enough for effective EDR operation

Stix-Shifter:

Highlights the limits of model-less normalization xEDRs

Distributing IOCs , fielding simple alerts and taking simple action may work fine, if aimed at the EDR as a system ... and if Stix-Shifter mappings are expanded consistently.

Semantic inconsistencies that will interfere with xEDR sense making, decision support and action:

xEDR attrib relationships
xEDR attrib representations
Opaque unjoinable IDs

Normalizing the consumption of EDR capability, via the Stix-Shifter mapping approach won't work, due to limitations in what products expose (attributes, reps, analytics, inf, train, …mgmt).

We need a model… probably two models

CarbonBlack

STIX Object	STIX Property	Data Source Field
directory	path	process_path
directory	path	parent_path
file	name	process_name
file	hashes.MD5	process_md5
file	hashes.SHA-256	process_sha256
file	parent_directory_ref	process_path
file	name	parent_name
file	hashes.MD5	parent_md5
file	hashes.SHA-256	parent_sha256
file	parent_directory_ref	parent_path
process	creator_user_ref	process_username
process	created	process_start_time
process	name	process_name
process	binary_ref	process_name
process	pid	process_pid
process	x_unique_id	process_guid
process	command_line	process_cmdline
process	name	parent_name
process	binary_ref	parent_name
process	parent_ref	parent_name
process	pid	parent_pid
process	x_unique_id	parent_guid
process	command_line	parent_cmdline
user-account	user_id	process_username
x-cbcloud	device_name	device_name
x-cbcloud	device_internal_ip	device_internal_ip
x-cbcloud	device_external_ip	device_external_ip
x-cbcloud	device_os	device_os
x-cbcloud	device_id	device_id
x-cbcloud	device_timestamp	device_timestamp
x-cbcloud	org_id	org_id
x-cbcloud	device_group_id	device_group_id
x-cbcloud	process_terminated	process_terminated
x-cbcloud	regmod_count	regmod_count
x-cbcloud	netconn_count	netconn_count
x-cbcloud	filemod_count	filemod_count
x-cbcloud	modload_count	modload_count
x-cbcloud	childproc_count	childproc_count
x-cbcloud	crossproc_count	crossproc_count
x-cbcloud	scriptload_count	scriptload_count

Trend (XDR-ish)

STIX Object	STIX Property	Data Source Field
directory	path	objectFilePath
directory	path	processFilePath
directory	path	parentFilePath
directory	path	srcFilePath
domain-name	value	hostName
domain-name	value	objectHostName
domain-name	value	source_domain
email-addr	value	mail_message_sender
email-addr	value	mail_message_recipient
email-message	sender_ref	mail_message_sender
email-message	is_multipart	mail_message_sender
email-message	to_refs	mail_message_recipient
email-message	is_multipart	mail_message_recipient
email-message	subject	mail_message_subject
email-message	is_multipart	mail_message_subject
email-message	date	mail_message_delivery_time
email-message	is_multipart	mail_message_delivery_time
email-message	additional_header_fields	mail_internet_headers
file	hashes.SHA-1	objectFileHashSha1
file	name	objectFilePath
file	parent_directory_ref	objectFilePath
file	hashes.SHA-1	processFileHashSha1
file	name	processFilePath
file	parent_directory_ref	processFilePath
file	hashes.SHA-1	parentFileHashSha1
file	name	parentFilePath
file	parent_directory_ref	parentFilePath
file	name	srcFilePath
file	parent_directory_ref	srcFilePath
file	hashes.SHA-1	srcFileHashSha1
file	name	file_name
file	hashes.SHA-1	file_sha1
ipv4-addr	value	src
ipv4-addr	value	dst
ipv4-addr	value	endpointIp
ipv4-addr	value	objectIp
ipv4-addr	value	objectIps
ipv4-addr	value	source_ip
ipv6-addr	value	src
ipv6-addr	value	dst
ipv6-addr	value	endpointIp
ipv6-addr	value	objectIps
ipv6-addr	value	source_ip
network-traffic	src_ref	src
network-traffic	protocols	src
network-traffic	src_port	spt
network-traffic	protocols	spt
network-traffic	dst_ref	dst
network-traffic	protocols	dst
network-traffic	dst_port	dpt
network-traffic	protocols	dpt
network-traffic	dst_ref	objectIp
network-traffic	protocols	objectIp
network-traffic	dst_port	objectPort
network-traffic	protocols	objectPort
network-traffic	src_ref	source_ip
network-traffic	protocols	source_ip
process	command_line	objectCmd
process	binary_ref	objectFileHashSha1
process	binary_ref	objectFilePath
process	command_line	processCmd
process	binary_ref	processFileHashSha1
process	binary_ref	processFilePath
process	command_line	parentCmd
process	binary_ref	parentFileHashSha1
process	binary_ref	parentFilePath
url	value	request
url	value	mail_urls
user-account	account_login	logonUser
user-account	user_id	objectUser
windows-registry-key	key	objectRegistryKeyHandle
windows-registry-key	values	objectRegistryValueType

CrowdStrike

STIX Object	STIX Property	Data Source Field
directory	path	filepath
domain-name	Value	domain_ioc
File	Name	filename
file	parent_directory_ref	filepath
file	hashes.SHA-256	sha256
file	hashes.MD5	md5
file	hashes.SHA-256	parent_sha256
file	hashes.SHA-256	sha256_ioc
file	hashes.SHA-256	quarantined_file_sha256
file	hashes.MD5	md5_ioc
file	hashes.MD5	parent_md5
ipv4-addr	value	external_ip
ipv4-addr	value	local_ip
mac-addr	value	mac_address
network-traffic	dst_ref	domain_ioc
process	binary_ref	filename
process	name	filename
process	binary_ref	filepath
process	command_line	cmdline
process	creator_user_ref	user_name
process	creator_user_ref	user_id
process	binary_ref	parent_sha256
process	parent_ref	parent_sha256
process	pid	parent_process_graph_id
process	parent_ref	parent_process_graph_id
process	pid	triggering_process_graph_id
process	binary_ref	parent_md5
process	parent_ref	parent_md5
process	command_line	parent_cmdline
process	parent_ref	parent_cmdline
user-account	account_login	user_name
user-account	user_id	user_id
windows-registry-key	key	registry_key
x-crowdstrike	machine_domain	machine_domain
x-crowdstrike	device_id	device_id
x-crowdstrike	detection_id	detection_id
x-crowdstrike	scenario	scenario
x-crowdstrike	technique	technique
x-crowdstrike	tactic	tactic
x-crowdstrike	tactic_id	tactic_id
x-crowdstrike	technique_id	technique_id
x-crowdstrike	agent_local_time	agent_local_time
x-crowdstrike	agent_version	agent_version
x-crowdstrike	first_seen	first_seen
x-crowdstrike	last_seen	last_seen
x-crowdstrike	platform_id	platform_id
x-crowdstrike	confidence	confidence
x-crowdstrike	ioc_type	ioc_type
x-crowdstrike	ioc_value	ioc_value
x-crowdstrike	ioc_value	bios_manufacturer
x-crowdstrike	ioc_value	bios_version
x-crowdstrike	ioc_value	config_id_base
x-crowdstrike	ioc_value	config_id_build
x-crowdstrike	ioc_value	config_id_platform
x-crowdstrike	ioc_value	product_type
x-crowdstrike	ioc_value	product_type_desc
x-crowdstrike	ioc_value	site_name
x-crowdstrike	ioc_value	system_product_name
x-crowdstrike	ioc_value	modified_timestamp
x-oca-asset	ip_refs	external_ip
x-oca-asset	hostname	hostname
x-oca-asset	ip_refs	local_ip
x-oca-asset	mac_refs	mac_address
x-oca-asset	os_version	os_version
x-oca-asset	os_platform	platform_name
x-oca-event	created	timestamp
x-oca-event	process_ref	filename
x-oca-event	action	display_name
x-oca-event	outcome	description
x-oca-event	registry_ref	registry_key
x-oca-event	network_ref	domain_ioc
x-oca-event	file_ref	sha256_ioc
x-oca-event	file_ref	quarantined_file_sha256
x-oca-event	file_ref	md5_ioc
x-oca-event	parent_process_ref	parent_md5
x-oca-event	host_ref	hostname
x-oca-event	provider	provider
x-oca-event	severity	severity

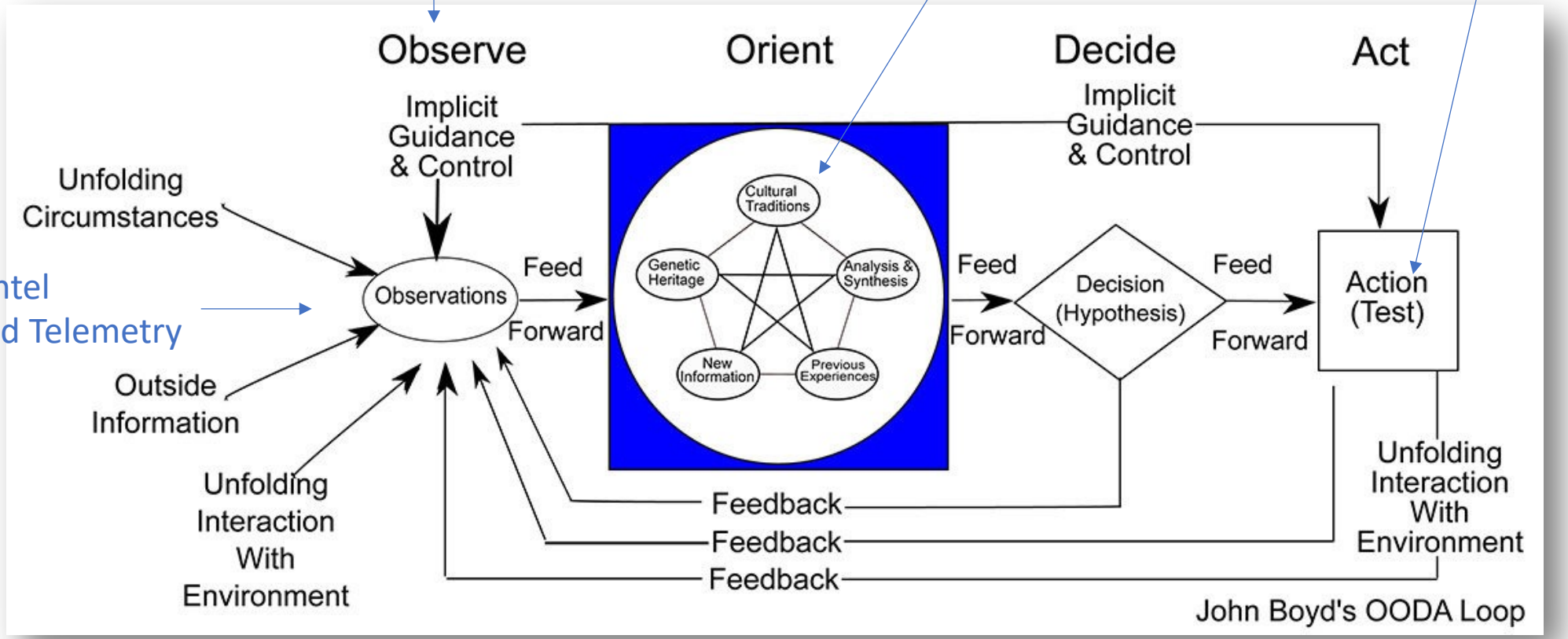
Inconsistencies across EDR/XDR break OODA

Intention/Provisioning/Architecture

Model-Informed Orientation
(different in every EDR)

Correct action and feedback efficacy
both depend on a working model

Telemetry/Intel
EDR IOCs and Telemetry



Recommendation

- Two parallel tracks
  1. Continue to do what can be done with existing mapping approach
     - Has hard limits requiring additional parallel mechanisms
     - Enhanced by interacting with EDR systems, beyond just instrumented endpoints.
     - Can happen fast
  2. Investigate the potential of leveraging existing models to extend the normalization of EDR/XDR consumption
     - More general enablement of normalized EDR consumption for more use cases
     - Requires analysis, debate and design
  3. 1. and 2. above are highly complementary, probably mutually necessary to cultivate sustainable communities of interest, and to influence the market.

  So, I'd like to still proceed on the expanded analysis proposed in the last meeting

EDR Normalization Objectives Expressed in PACE Meeting

- Normalizing Response to EDR Detections (detection and action) across uniform deployments of any EDR
  - Possible with OpenC2, but actionable context will need to communicated using another or additional functionality.
  - May require talking to EDR systems (managers)
- Normalizing Response to EDR Detections (detection and action) across heterogeneous deployments of arbitrary EDRs
  - Far harder, due to balkanized/fragmented and inconsistent model, analytics, ML, tagging, grouping, system topology, data domains (training) …
  - Certainly requires talking to managers.
- Liberating the market from the walled gardens of proprietary EDR
  - Requires models of Telemetry, Mal behavior and Mitigation options