This document represents the position of FireEye on the topic of how best to represent information pertaining to cyber investigations (events, alerts, incidents, etc).

Key Terms

- An ***Event*** is an occurrence of some activity characterized by the observables indicating such action occurred. (e.g. a remote login occurred from a given account)
- An ***Alert*** is a grouping of one or more Events believed to be suspicious along with some explanation of why the activity is believed to be suspicious (e.g. a remote login occurred from a given account during atypical hours and from an atypical IP address)
- An ***Investigation*** is an exploration of the facts involved in a cyber-relevant set of suspicious activity
    - An ***Incident*** is a formally tracked investigation (has specific legal meaning in many jurisdictions)

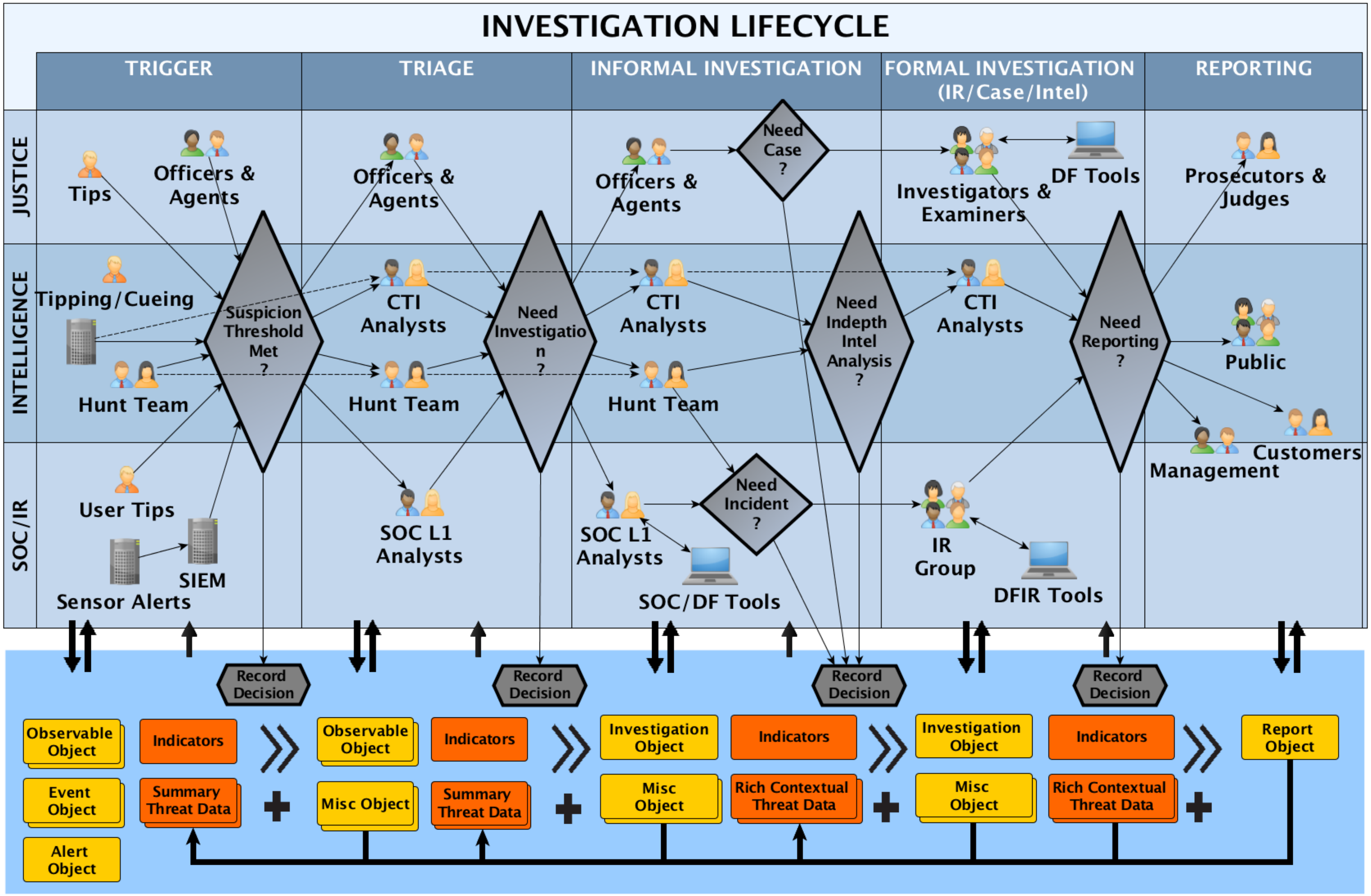
The Investigation Lifecycle

Cyber investigations may take many different forms from SOC operations and Incident Response to intelligence to justice/legal investigations. Regardless of the particular contextual form these investigations typically follow a common investigation lifecycle. This lifecycle consists of five basic phases: Trigger, Triage, Informal Investigation, Formal Investigation, Reporting. Most investigations do not make it all the way through the lifecycle, terminating at some interim phase, but the phases are typically consistent nonetheless.

Very briefly, the phases could be described in this way:

- **Trigger**: Some suspicious Event is observed or reported and a very quick decision is made whether it is suspicious enough to consider at that point (e.g. automated alert of a certain type or severity) or will be ignored or postponed. Often automated.
- **Triage**: Suspicious Event is evaluated according to basic criteria, cursorily discovered information and basic contextual knowledge to determine if further investigation is needed. Often human with automation support.
- **Informal Investigation**: Event is summarily investigated to better understand what occurred and the nature, scale and scope of risk it represents.
- **Formal Investigation**: Event is investigated in detail following a defined process to fully understand what occurred, to quantify and qualify impact, to remediate effects and to leverage knowledge learned for future operations and intelligence.
- **Reporting**: Relevant details and summarized analysis from the investigation are packaged and conveyed to decision makers.

The figure below attempts to convey in a single picture the basic flow of the investigation lifecycle, the commonality across differing forms of investigation, the decision gates between phases of the lifecycle, the typical roles involved in differing phases and differing forms of investigation and the typical knowledge involved across the lifecycle. While somewhat complex the figure is incomplete and not intended to convey the full details of everything involved. A typical investigation would evolve left-to-right through the lifecycle within a single horizontal swimlane.



INVESTIGATION LIFECYCLE

TRIGGER | TRIAGE | INFORMAL INVESTIGATION | FORMAL INVESTIGATION (IR/Case/Intel) | REPORTING

JUSTICE | INTELLIGENCE | SOC/IR

Trigger: Tips; Officers & Agents; Tipping/Cueing; Hunt Team; User Tips; SIEM; Sensor Alerts

Suspicion Threshold Met ?

Triage: Officers & Agents; CTI Analysts; Hunt Team; SOC L1 Analysts

Need Investigatio n ?

Informal Investigation: Officers & Agents; CTI Analysts; Hunt Team; SOC L1 Analysts; SOC/DF Tools

Need Case ?

Need Incident ?

Need Indepth Intel Analysis ?

Formal Investigation: Investigators & Examiners; DF Tools; CTI Analysts; IR Group; DFIR Tools

Need Reporting ?

Reporting: Prosecutors & Judges; Public; Customers; Management

Record Decision

Record Decision

Record Decision

Record Decision

Observable Object; Event Object; Alert Object; Indicators; Summary Threat Data

Observable Object; Misc Object; Indicators; Summary Threat Data

Investigation Object; Misc Object; Indicators; Rich Contextual Threat Data

Investigation Object; Misc Object; Indicators; Rich Contextual Threat Data

Report Object

Unified Knowledge Repository / Integrated Knowledge Repositories

Figure Notes

Columns represent phases in the investigation lifecycle moving left to right

- **Trigger**:
  - Knowledge:
    - Created - Observable Objects characterizing what was seen that was deemed suspicious, Event Object(s) referencing relevant Observables, Alert Object referencing relevant Event(s) of suspicion along with characterization of why they were deemed suspicious (e.g. Indicator sighting, signature fired, anomalous behavior, etc.), Sightings of Indicators.
    - Considered – Indicators, summary threat data
  - Decision Gate - Suspicion Threshold Met?: Suspicion threshold is typically based on nature of Event, currently defined priorities and what context is known at the time. Typically based on information and knowledge in hand at the time without further evaluation or investigation. Often automated.
  -
- **Triage**:
  - Knowledge:
    - Created – Observable Objects characterizing further detail of the suspicious activity, Sightings of Indicators, and miscellaneous contextual Objects (Locations, Identities, etc.).
    - Considered - Indicators, summary threat data, available COAs.
  - Decision Gate - Need Investigation?: Typically based on nature of Event, potential risk of Event, available COAs for mitigation/remediation and available resources and priorities. Often human with automation support.
- **Informal Investigation**:
  - Knowledge:
    - Created – Investigation Object, full range of miscellaneous Objects representing what is discovered, Forensic Actions, Provenance Records, Annotations, Sightings of Indicators.
    - Considered - Indicators, rich contextual threat data (TTPs, Campaigns, Threat Actors, Victim Targeting, etc.).
  - Decision Gate - Need Case, Indepth Intel Analysis or Incident?: Typically based on potential risk and the nature of the discovered activity/impact.
- **Formal Investigation**:
  - Knowledge:
    - Created – Updates to Investigation Object, full range of miscellaneous Objects representing what is discovered, Forensic Actions, Provenance Records, Annotations, Sightings of Indicators..
    - Considered - Indicators, rich contextual threat data (TTPs, Campaigns, Threat Actors, Victim Targeting, etc.).
  - Decision Gate - Need Reporting? Typically based on nature/scope of impact, level of residual risk and any binding policy/legal requirements.
- **Reporting**:

        - Knowledge:
            - Created – Created - Report Object

Rows represent key specific contexts of cyber investigations

- Justice:
    - Investigations into potential criminal activity
- Intelligence:
    - Investigations of suspicious activity with a primary focus on developing intelligence to inform strategic and operational decisions and activities.
- SOC/IR:
    - Investigations of suspicious activity with a primary focus on sense making and secure operations.

- Diamonds represent key decision points in the lifecycle
- Thin arrows in the table represent information flows
- Large blue knowledge box represents a unified knowledge repository (ideally) or multiple integrated knowledge repositories
- Yellow knowledge boxes represent information created as part of the investigation
- Orange knowledge boxes represent intelligence information considered and/or leveraged as part of the investigation
- Chevrons/plus-signs indicate knowledge builds and aggregates throughout the investigation and at any stage all information from previous stages is available

Proposed Approach

Following our policy of not reinventing wheels, FireEye proposes that the CTI TC leverage the CASE/UCO standardized representation being developed by the cyber investigation community rather than trying to invent a separate conflicting version.

Specifically, FireEye proposes the four key objects (Event, Alert, Investigation, Grouping) outlined below as well as the two referenced relevant related objects (ForensicAction, ProvenanceRecord) and facet/extensions as appropriate.

One potential concern for CTI TC adoption of CASE/UCO to support cyber investigation related information is the fact that CASE/UCO specify JSON-LD as their default serialization. We would like to point out that this should not be a barrier as non-JSON-LD serialized STIX can support JSON-LD use cases through the inclusion of a simple context. This means that "id" and "type" can be used rather than "@id" and "@type".

It may also be useful to point out that the concept of "propertyBundle" in CASE/UCO is very similar to the STIX concept of "extensions". They both allow sets of properties to be specified to further characterize an object. The difference is that propertyBundle is defined as an array of JSON nodes where STIX extension is defined as a property that is a dictionary of JSON nodes.

FireEye proposes that for now the CTI TC community focus on a core minimal set of expressivity for now and leave more detailed areas (Impact, COAs, etc.) for future discussion and inclusion as facets/extensions.

FireEye proposes using CASE/UCO objects directly rather than attempting to duplicate their structure in STIX which is likely to lead to significant maintenance and alignment issues going forward.
A discussion will need to occur to determine the appropriate seam/interface between the two.

The following characterizations are provided as CASE/UCO objects.

Key Objects

In current STIX parlance, these are all SDOs.

Event:

In process of being added to CASE/UCO. Direct derivation of uco-core:ContextualCompilation class.
An occurrence of some activity characterized by the observables indicating such action occurred.

Properties

Property Name	Type	Description
`type` (required)	`string`	The value of this field **MUST** be `event`
`name` (required)	`string`	A name used to identify the Event.
`description` (optional)	`string`	A description that provides more details and context about the Event, potentially including its purpose and its key characteristics.
`object`	`list` of type `identifier`	A list of Observable and potentially other objects that are linked to this event

Example JSON

```
{
  "id": "event-51f4a684-c7c4-4d8d-9d5f-9f72b07565a5",
  "type": "Event",
  "name": "Remote Login",
  "object": ["account-login-59e9cf76-08c3-4f0b-a319-2a3b55b54f03",
"ipv4address-bcc67257-331c-4151-8818-1196eb91e7e0", "relationship-51f4a684-
c7c4-4d8d-9d5f-9f72b07565a5", "location-5ec73396-fb52-4bd5-9a66-
e6dddfc96d76"]
}
```

Alert:

In process of being added to CASE/UCO. Derivation of uco-core:Grouping class with "context" property renamed to "alertContext".

A report of one or more Events believed to be suspicious along with some explanation of why the activity is believed to be suspicious.

Properties

Property Name	Type	Description
`type` (required)	`string`	The value of this field **MUST** be `alert`
`name` (required)	`string`	A name used to identify the Alert.
`description` (optional)	`string`	A description that provides more details and context about the Alert, potentially including its purpose and its key characteristics.
`alertContext` (required)	`open-vocab`	This is an open vocabulary and values **SHOULD** come from the `alert-context-ov` vocabulary.
`object`	`list` of type `identifier`	A list of Event and potentially other objects that are linked to this alert

Example JSON

```
{
  "id": "alert-a41737ad-558c-44a4-8031-40c623b3f07b",
  "type": "Alert",
  "alertContext": "Anomalous Login",
  "object": ["event-51f4a684-c7c4-4d8d-9d5f-9f72b07565a5"]
}
```

Investigation:

Currently defined in CASE/UCO

An exploration of the facts involved in a cyber-relevant set of suspicious activity.

If an investigation starts as informal and transitions to formal (e.g. Incident) the same object is used (conveying all historical context) and the "investigationForm" property value is simply changed as appropriate.

Properties

Property Name	Type	Description
`type` (required)	`string`	The value of this field **MUST** be `investigation`
`name` (required)	`string`	A name used to identify the Investigation.
`description` (optional)	`string`	A description that provides more details and context about the Investigation, potentially including its purpose and its key characteristics.
`investigationStatus` (required)	`open-vocab`	This is an open vocabulary and values **SHOULD** come from the `investigation-status-ov` vocabulary.

`investigationForm` (required)	`open-vocab`	This is an open vocabulary and values **SHOULD** come from the `investigation-form-ov` vocabulary.
`focus`	`string`	Specifies the topical focus of an investigation.
`startTime`	`timestamp`	The initiation time of the investigation.
`endTime`	`timestamp`	The termination time of the investigation.
`object`	`list` of type `identifier`	A list of Objects that are linked to this investigation

Example JSON

As an informal investigation:

```
{
    "id": "investigation-4586742a-710a-454f-bcb8-b60e230ec1b2",
    "type": "Investigation",
    "name": "Case-4233456",
    "focus": "Remote Penetration",
    "investigationForm": "suspicious-activity",
    "investigationStatus": "active",
    "object": ["alert-a41737ad-558c-44a4-8031-40c623b3f07b", "event-51f4a684-
c7c4-4d8d-9d5f-9f72b07565a5", "account-login-59e9cf76-08c3-4f0b-a319-
2a3b55b54f03", "ipv4address-bcc67257-331c-4151-8818-1196eb91e7e0",
"relationship-51f4a684-c7c4-4d8d-9d5f-9f72b07565a5", "location-5ec73396-fb52-
4bd5-9a66-e6dddfc96d76", "device-4fe57390-0b6e-4ac8-b813-bbfe3a8ab14d",
"netflow-fbfeff04-806d-407f-adf9-7b0258773d57"]
}
```

and then as a formal Incident:

```
{
    "id": "investigation-4586742a-710a-454f-bcb8-b60e230ec1b2",
    "type": "Investigation",
    "name": "Case-4233456",
    "focus": "Remote Penetration",
    "investigationForm": "incident",
    "investigationStatus": "active",
    "object": ["alert-a41737ad-558c-44a4-8031-40c623b3f07b", "event-51f4a684-
c7c4-4d8d-9d5f-9f72b07565a5", "account-login-59e9cf76-08c3-4f0b-a319-
2a3b55b54f03", "ipv4address-bcc67257-331c-4151-8818-1196eb91e7e0",
"relationship-51f4a684-c7c4-4d8d-9d5f-9f72b07565a5", "location-5ec73396-fb52-
4bd5-9a66-e6dddfc96d76", "device-4fe57390-0b6e-4ac8-b813-bbfe3a8ab14d",
"netflow-fbfeff04-806d-407f-adf9-7b0258773d57", "url-5ac08375-040f-4f49-a798-
7c7aeb7bbe72", "file-4b823cc5-fa95-481f-a266-bdb02ef7d041", "ipv4address-
b3d18c4c-6395-4488-8cd6-5ccd2d1f9ab6", "PhoneCall-64a02003-af72-470e-9401-
d7fbb86a63a1", "PhoneAccount-14db2f1e-5f6c-48d6-8215-2eafd9acdef8", "tool-
d8be53cd-5c02-47cf-bfe7-dba834662ca3", "tool-f9d860d2-bdfb-4739-a8a8-
0b5b58cefabd", "forensic-action-17635748-0dff-4488-ba0a-6c12b7387e52",
"provenance-recordß-96c5c340-5c83-472c-8251-1bc5374a8078", "identity-
6dfbf395-f7b7-43a2-8724-dd87db659e76", "identity-80ec0271-42bc-42b0-9b9a-
f326cb919368", "role-31a9db11-bb0f-4eae-bc01-6ad68ada926c"],
    "propertyBundle": [
      {
```

```
      "type": "IncidentTimestamps",
      "detectedTime": "2017-03-28T13:44:23.40Z",
      "openedTime": "2017-03-29T07:421:44.20Z"
      },
    ]
}
```

Extensions

The following is a non-exhaustive list of potential facet extensions to the Investigation object provided simply as exemplars for discussion.

- IncidentTimestamps
- QuantitativeImpact
- QualitativeImpact
- AdversaryMotivation

Relevant Related Objects

uco-investigation:ForensicAction
A forensic examination action taken as part of a cyber investigation.
This object is currently in process of changing its name to InvestigativeAction.

uco-investigation:ProvenanceRecord
A provenantial connection between a forensic action and a set of observations (items and/or actions) or interpretations that result from it.

Vocabularies

`investigation-status-ov`
The vocab values below are for exemplar and discussion purposes only. They are not intended to be a final specification. Further discussion is required.

Vocabulary Value	**Description**
`open`	The investigation is currently in an open status.
`active`	The investigation is currently active.
`paused`	The investigation has been paused.
`closed-resolved`	The investigation has been closed and resolved.
`closed-false-positive`	The investigation was closed and marked as a false positive.
`dismissed`	???

`investigation-form-ov`

The vocab values below are for exemplar and discussion purposes only. They are not intended to be a final specification. Further discussion is required.

Vocabulary Value	Description
`suspcicious-activity`	An informal investigation into suspicious activity.
`incident`	A formal investigation for incident response.
`case`	A formal investigation into potential criminal activity.
`Indepth-intel-analysis`	An formal investigation focused on indepth intelligence analysis.

Grouping:

Currently defined in CASE/UCO

This object supports a generalized contextual compilation of content (no restrictions on types of objects). It supports the general case that the MISP community has been asking for.

Properties

Property Name	Type	Description
type (required)	`string`	The value of this field **MUST** be `grouping`
name (required)	`string`	A name used to identify the Grouping.
description (optional)	`string`	A description that provides more details and context about the Grouping, potentially including its purpose and its key characteristics.
context(required)	`string`	A description of particular contextual affinity.
object	`list` of type `identifier`	A list of Objects that are linked to this Grouping

Example JSON

```
{
  "id": "grouping-51f4a684-c7c4-4d8d-9d5f-9f72b07565a5",
  "type": "Grouping",
  "name": "PiratePicnic info",
  "context": "investigation enrichment",
  "object": ["account-login-59e9cf76-08c3-4f0b-a319-2a3b55b54f03",
"ipv4address-bcc67257-331c-4151-8818-1196eb91e7e0", "relationship-51f4a684-
c7c4-4d8d-9d5f-9f72b07565a5", "location-5ec73396-fb52-4bd5-9a66-
e6dddfc96d76", "identity-6dfbf395-f7b7-43a2-8724-dd87db659e76", "PhoneCall-
64a02003-af72-470e-9401-d7fbb86a63a1", "PhoneAccount-14db2f1e-5f6c-48d6-8215-
2eafd9acdef8", "investigation-a41737ad-558c-44a4-8031-40c623b3f07b",
"annotation-5ec73396-fb52-4bd5-9a66-e6dddfc96d76", "relationship-30ef8107-
5678-4015-9fc3-c860b73c3dc2"]
},
```