**IDMEFv2**

**Version 0.3**

**DRAFT**

**Cyber / Physical / Availability Examples**

Table des matières

[1 Physical detection 3](#_Toc70666174)

[1.1 First physical intrusion detected by a detector+sensor "all in one" 3](#_Toc70666175)

[1.2 First physical intrusion detected by a couple detector + sensor 4](#_Toc70666176)

[1.3 Second physical intrusion detected by the same couple 5](#_Toc70666177)

[1.4 Multiple physical vectors detected at once by a single sensor 6](#_Toc70666178)

[1.5 Separate sensors detect separate vectors during the same timeframe 8](#_Toc70666179)

[1.6 Different detections for the same vectors depending on the sensor 12](#_Toc70666180)

[2 Physical PTI 16](#_Toc70666181)

[2.1 PTI alert created the Monday announcing a storm from Tuesday 16h to Wednesday 20h 16](#_Toc70666182)

[2.2 PTI alert update of the same storm on Tuesday morning 17](#_Toc70666183)

[3 Cyber detection 18](#_Toc70666184)

[3.1 Malicious content detected by a system acting as both an analyzer and sensor 18](#_Toc70666185)

[3.2 Cyber detection: Unknown IP Protocol detected 20](#_Toc70666186)

[3.3 Cyber detection: Enrichment AD 21](#_Toc70666187)

[3.4 Enrichment based on Cyber-Threat Intelligence data 23](#_Toc70666188)

[4 Cyber Correlation / aggregation: enrichment 25](#_Toc70666189)

[4.1 N Alert for Single authentication failed 25](#_Toc70666190)

[4.2 Aggregation (condition) of a password brute force attack 26](#_Toc70666191)

[4.3 Authentication failure for SSH service 27](#_Toc70666192)

[4.4 Authentication failure for HTTP service 29](#_Toc70666193)

[4.5 Authentication failure for SMTP service 31](#_Toc70666194)

[4.6 Multiple authentication failures (password spraying attack) 33](#_Toc70666195)

[4.7 Single authentication failed detected by detector 34](#_Toc70666196)

[4.8 Correlator analyze the alert and add CTI on IP source 35](#_Toc70666197)

[5 Physical correlation / aggregation 36](#_Toc70666198)

[5.1 Physical correlation / aggregation Alert 1 : Drone detection 36](#_Toc70666199)

[5.2 Physical correlation / aggregation Alert 2 : Drone detection 38](#_Toc70666200)

[5.3 Physical correlation / aggregation Alert 3 : Drone detection 39](#_Toc70666201)

[5.4 Aggregation (liste ?) : Drone moving in area 40](#_Toc70666202)

[5.5 update of the alert 42](#_Toc70666203)

[6 Availability 44](#_Toc70666204)

[6.1 Abnormal temperature detected in a server 44](#_Toc70666205)

[6.2 Device stopped responding to ICMP PING solicitations 45](#_Toc70666206)

[6.3 Alert on external temperature planned to be high AND temperature high in DataCenter 46](#_Toc70666207)

# Physical detection

## First physical intrusion detected by a detector+sensor "all in one"

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",

"Entity": "EXAMPLE",

"Category": [

"Intrusions.Burglary"

],

"Cause": "Malicious",

"Description": "Physical intrusion detected",

"Status": "Incident",

"Severity": "Medium",

"CreateTime": "2021-01-18T23:33:05.21Z",

"DetectTime": "2021-01-18T23:33:04.52Z",

"Confidence": 0.9,

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Front door camera",

"Hostname": "camera3.example.com",

"Type": "Physical",

"Model": "Netatmo 42B",

"Category": [

"HAR"

],

"Data": [

"Images"

],

"Method": [

"Movement"

],

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Front Door"

},

"Sensor": [

{

"CaptureZone": "{\"type\":\"conic-zone\",\"Azimuth\":34.00,\"El\u00e9vation\":-30.00,\"Range\":600.00,\"HFOV\":200.00,\"VFOV\":20.00}"

}

],

"Target": [

{

"Location": "Garden"

}

],

"Vector": [

{

"Category": "Human",

"Name": "Unknown",

"Size": "Medium",

"Observable": [

"PTZ Relative position"

]

}

],

"Observables": [

{

"Name": "PTZ Relative position",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":34.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

}

]

}

## First physical intrusion detected by a couple detector + sensor

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",

"Description": "Physical intrusion detected",

"Cause": "Malicious",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Medium",

"Confidence": 0.9,

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Analyzer": {

"IP": "1.1.1.1",

"Name": "Motion detector",

"Hostname": "analyzer.acme.eu",

"Model": "MD 9.9.3",

"Category": [

"MWIR",

"HAR"

],

"Data": [

"Images",

"Thermic"

],

"Method": [

"Movement",

"Heat"

]

},

"Sensor": [

{

"IP": "1.1.1.2",

"Name": "Infrared camera 42",

"Model": "IC 3.5.2",

"UnLocation": "GR ATH",

"Location": "Front Door"

}

],

"Vector": [

{

"Category": [

"human"

],

"Attachment": [

"attach1"

],

"Observable": [

"obs1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "img2021011823330521.jpg",

"ExternalURI": "https://data.acme.eu/img2021011823330521.jpg",

"ContentType": "image/jpeg"

}

],

"Observable": [

{

"Name": "obs1",

"Content": "{\"Xmin\": 34, \"Xmax\": 120, \"Ymin\": 101, \"Ymax\": 369}"

}

]

}

## Second physical intrusion detected by the same couple

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb2",

"Cause": "Malicious",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Medium",

"Confidence": 0.9,

"Description": "Physical intrusion detected",

"CreateTime": "2021-01-18T23:34:05.21Z",

"StartTime": "2021-01-18T23:34:04.52Z",

"Analyzer": {

"IP": "1.1.1.1",

"Name": "Motion detector"

},

"Sensor": [

{

"IP": "1.1.1.2",

"Name": "Infrared camera 42"

}

],

"Vector": [

{

"Category": [

"human"

],

"Attachment": [

"attach1"

],

"Observable": [

"obs1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "img2021011823340521.jpg",

"ExternalURI": "https://data.acme.eu/img2021011823340521.jpg",

"ContentType": "image/jpeg"

}

],

"Observable": [

{

"Name": "obs1",

"Content": "{\"Xmin\": 22, \"Xmax\": 100, \"Ymin\": 501, \"Ymax\": 692}"

}

]

}

## Multiple physical vectors detected at once by a single sensor

A security camera filmed 2 persons intruding into facility grounds. The camera's management server detects the intruders and sends an alert with a link to a still image where both intruders are visible.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef00",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Other.Undetermined"

],

"Confidence": 0.8,

"Severity": "Low",

"Description": "Several ground objects detected near the main building",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": {

"IP": "172.10.5.31",

"Name": "Front door camera",

"Hostname": "camera1.example.com",

"Model": "Netatmo 42B",

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Front Door"

},

"Target": [

{

"Location": "Northern Hallway"

}

],

"Vector": [

{

"Category": [

"man"

],

"Name": "Intruder #1",

"Size": "medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

},

{

"Category": [

"human"

],

"Name": "Intruder #2",

"Size": "medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "c1-2021.04.12-64216343.jpg",

"Hash": "sha-256: 01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b",

"Size": 2132078,

"ExternalURI": "https://sec-center.example.com/archive?sensor=c1&ref=2021.04.12-64216343",

"Note": "Still image from 'Front Door Camera' depicting Intruder #1 and Intruder #2",

"ContentType": "image/jpeg"

}

]

}

## Separate sensors detect separate vectors during the same timeframe

Three separate sensors (3 cameras) detect one vector each. These detections occurred during the same timeframe. Therefore, a correlation engine dedicated to physical sensors could try to infer an incident (e.g. protesters marching toward a building) from these individual alerts.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef90",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-19T23:33:05.21Z",

"StartTime": "2021-01-19T23:33:04.52Z",

"Category": [

"Other.Undetermined"

],

"Confidence": 0.9,

"Severity": "Low",

"Description": "Single object detected near the facilities",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": [

{

"IP": "172.10.5.31",

"Name": "Front door camera",

"Hostname": "camera1.example.com",

"Model": "Netatmo 42B",

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Front Door"

}

],

"Target": [

{

"Location": "Entryway"

}

],

"Vector": [

{

"Category": [

"man"

],

"Name": "Detected #1",

"Size": "Medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.09",

"GeoRadius": 42.5,

"Location": "Entryway",

"Attachment": [

"attach1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "c1-2021.01.19-64216341.jpg",

"Hash": "sha-256: 01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b",

"Size": 2132078,

"ExternalURI": "https://sec-center.example.com/archive?sensor=c1&ref=2021.01.19-64216341",

"Note": "Still image showing vector #1",

"ContentType": "image/jpeg"

}

]

}

------------------------------------------

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef91",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-19T23:33:06.21Z",

"StartTime": "2021-01-19T23:33:05.52Z",

"Category": [

"Other.Undetermined"

],

"Confidence": 0.9,

"Severity": "Low",

"Description": "Single object detected near the facilities",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": [

{

"IP": "172.10.5.32",

"Name": "Northern hallway camera",

"Hostname": "camera2.example.com",

"Model": "Netatmo 42B",

"GeoLocation": "+48.75726,+2.299529,+65.1",

"UnLocation": "GR ATH",

"Location": "Northern Hallway"

}

],

"Target": [

{

"Location": "Northern Hallway"

}

],

"Vector": [

{

"Category": [

"human"

],

"Name": "Detected #1",

"Size": "medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Entryway",

"Attachment": [

"attach1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "c1-2021.01.19-64216342.jpg",

"Hash": "sha-256: 01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b",

"Size": 2132078,

"ExternalURI": "https://sec-center.example.com/archive?sensor=c1&ref=2021.01.19-64216342",

"Note": "Still image showing vector #1",

"ContentType": "image/jpeg"

}

]

}

----------------------------

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef83",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-19T23:33:07.21Z",

"StartTime": "2021-01-19T23:33:06.52Z",

"Category": [

"Other.Undetermined"

],

"Confidence": 0.9,

"Severity": "Low",

"Description": "Single object detected near the facilities",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": [

{

"IP": "172.10.5.33",

"Name": "Back door camera",

"Hostname": "camera3.example.com",

"Model": "Netatmo 42B",

"GeoLocation": "+48.75727,+2.299528,+65.12",

"UnLocation": "GR ATH",

"Location": "Back Door"

}

],

"Target": [

{

"Location": "Back Door"

}

],

"Vector": [

{

"Category": [

"woman"

],

"Name": "Detected #1",

"Size": "Medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Entryway",

"Attachment": [

"attach1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "c1-2021.01.19-64216343.jpg",

"Hash": "sha-256: 01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b",

"Size": 2132078,

"ExternalURI": "https://sec-center.example.com/archive?sensor=c1&ref=2021.01.19-64216343",

"Note": "Still image showing vector #1",

"ContentType": "image/jpeg"

}

]

}

## Different detections for the same vectors depending on the sensor

Separate sensors (a heat detector, a sound detector and a camera) detect the same vectors (2 men & 1 woman). Due to the way it works, the heat detector cannot identify each vector individually (it only detects a massive heat source compared to the surrounding environment). The sound detector detects only 2 vectors (2 men speaking to each other while the woman stayed quiet). The camera detects all 3 of them successfully.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef81",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Other.Undetermined"

],

"Severity": "Low",

"Confidence": 0.9,

"Description": "Heat source detected in closed building",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": [

{

"IP": "172.10.5.32",

"Name": "Heat sensor #1",

"Hostname": "heat1.example.com",

"Model": "Heatty 123",

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Northern Hallway"

}

],

"Target": [

{

"Location": "Northern Hallway"

}

],

"Vector": [

{

"Category": [

"High temperature"

],

"Name": "Heat source",

"Size": "large",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 37,

"Location": "Northern Hallway"

}

]

}

-------------------------------

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef82",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Other.Undetermined"

],

"Confidence": 0.7,

"Severity": "Low",

"Description": "Human voices detected in closed building",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": [

{

"IP": "172.10.5.32",

"Name": "Sound detector #1",

"Hostname": "sound1.example.com",

"Model": "Soundly 123",

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Northern Hallway"

}

],

"Target": [

{

"Location": "Northern Hallway"

}

],

"Vector": [

{

"Category": [

"man"

],

"Name": "Man #1",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

},

{

"Category": [

"man"

],

"Name": "Man #2",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "s1-2021.04.12-987449.wav",

"Hash": "sha-256: 02aa4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805dbea8602",

"Size": 210986,

"ExternalURI": "https://sec-center.example.com/archive?sensor=s1&ref= 2021.04.12-987449",

"Note": "Audio recording where 2 human voices can be heard",

"ContentType": "audio/x-wav"

}

]

}

-----------------------------

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef83",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Other.Undetermined"

],

"Confidence": 0.9,

"Severity": "Medium",

"Description": "Several ground objects detected near the main building",

"Analyzer": {

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Type": "Physical",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

},

"Sensor": [

{

"IP": "172.10.5.31",

"Name": "Front door camera",

"Hostname": "camera1.example.com",

"Model": "Netatmo 42B",

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Front Door"

}

],

"Target": [

{

"Location": "Northern Hallway"

}

],

"Vector": [

{

"Category": [

"man"

],

"Name": "Intruder #1",

"Size": "Medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

},

{

"Category": [

"man"

],

"Name": "Intruder #2",

"Size": "Medium",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

},

{

"Category": [

"woman"

],

"Name": "Intruder #3",

"Size": "small",

"UnLocation": "GR ATH",

"GeoLocation": "+48.75726, +2.299528, +65.1",

"GeoRadius": 42.5,

"Location": "Northern Hallway",

"Attachment": [

"attach1"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "c1-2021.04.12-64216343.jpg",

"Hash": "sha-256: 01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b",

"Size": 2132078,

"ExternalURI": "https://sec-center.example.com/archive?sensor=c1&ref=2021.04.12-64216343",

"Note": "Still image from 'Front Door Camera' depicting Intruder #1, Intruder #2 and Intruder #3",

"ContentType": "image/jpeg"

}

]

}

# Physical PTI

## PTI alert created the Monday announcing a storm from Tuesday 16h to Wednesday 20h

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb3",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-19T16:00:00.00Z",

"CeaseTime": "2021-01-20T20:00:00.00Z",

"Cause": "Natural",

"Category": [

"Meteorological.Storm"

],

"Severity": "Medium",

"Confidence": 0.8,

"Description": "Storm announced",

"Analyzer": {

"IP": "1.1.1.3",

"Name": "PTI"

},

"Vector": {

"GeoLocation": "+48.75726 , +2.299528",

"GeoRadius": 22000

}

}

## PTI alert update of the same storm on Tuesday morning

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb3",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-19T16:00:00.00Z",

"CeaseTime": "2021-01-20T20:00:00.00Z",

"Cause": "Natural",

"Category": [

"Meteorological.Storm"

],

"Severity": "Medium",

"Confidence": 0.8,

"Description": "Storm announced",

"Analyzer": {

"IP": "1.1.1.3",

"Name": "PTI"

},

"Vector": {

"GeoLocation": "+48.75726 , +2.299528",

"GeoRadius": 23000

}

}

# Cyber detection

## Malicious content detected by a system acting as both an analyzer and sensor

In this example, a malware execution was detected by an EDR. The EDR serves both as the sensor and the analyzer. Hence, the "sensor" class is left undefined.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fe876",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Cause": "Malicious",

"Category": [

"Intrusion.UserCompromise",

"Intrusion.SysCompromise",

"Malicious.System"

],

"AltCategory": [

"MITRE ATT&CK: T1566.001"

],

"Confidence": 1.0,

"Severity": "High",

"Description": "Execution of a malicious attachment could not be prevented",

"Ref": [

"https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp\_ixeshe.pdf"

],

"Analyzer": {

"IP": "172.100.0.2",

"Name": "EDR",

"Hostname": "jdoe.users.example.com",

"Type": "Cyber",

"Model": "Super EDR v1.2.3",

"Category": [

"SPAM",

"AV",

"EDR",

"HIDS"

],

"Data": [

"Data",

"File"

],

"Method": [

"signature"

]

},

"Source": [

{

"TI": [

"IP:Dshield",

"Email:Abuse.ch"

],

"IP": "1.2.3.4",

"Hostname": "hacker.example.com",

"Proto": [

"tcp",

"smtp"

],

"Email": "refunds@yourbank.com",

"Attachment": [

"attach1"

],

"Observable": [

"obs1"

]

}

],

"Target": [

{

"IP": "172.100.0.2",

"Hostname": "jdoe.users.example.com",

"User": "jdoe",

"Email": "john.doe@example.com"

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "Consumer Welfare Table.pdf",

"Hash": "md5:c61c231d93d3bd690dd04b6de7350abb",

"Size": 127728,

"Ref": [

"https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp\_ixeshe.pdf",

"http://contagiodump.blogspot.com/2009/12/dec-29-cve-2009-4324-adobe-0-day.html"

],

"Note": "This attachment refers to a malicious file and should only be handled by cybersecurity professionals.",

"ContentType": "application/pdf",

"ContentEncoding": "base64",

"Content": "ABCDEF\u20267890=="

}

],

"Observable": [

{

"Name": "obs1",

"Reference": "STIX",

"Content": "{\"type\":\"process\",\"pid\":314,\"name\":\"AcroRd32.exe\",\"extensions\":{\"windows-process-ext\":{\"aslr\_enabled\":true,\"dep\_enabled\":true,\"priority\":\"HIGH\_PRIORITY\_CLASS\",\"owner\_sid\":\"S-1-5-21-186985262-1144665072-74031268-1309\"}}}"

}

]

}

## Cyber detection: Unknown IP Protocol detected

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:05.21Z",

"DetectTime": "2021-01-18T23:33:04.52Z",

"Cause": "Malicious",

"Category": [

"Recon.Scanning"

],

"Severity": "Medium",

"Confidence": 0.9,

"Description": "An IDS event of type \"Unknown IP Protocol\" was observed",

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Core router",

"Hostname": "core-router.example.com",

"Type": "Cyber",

"Model": "Cisco 4532",

"Category": [

"NIDS"

],

"Data": [

"Datagram"

],

"Method": [

"signature"

],

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "SBDX1"

},

"Sensor": [

{

"CaptureZone": "[{\"type\":\"ipv4-addr\",\"spec\_version\":\"2.1\",\"id\": \"ipv4-addr--ff26c055-6336-5bc5-b98d-13d6226742dd\",\"value\": \"172.17.0.0\"},{\"type\":\"ipv4-net-mask\",\"spec\_version\":\"2.1\",\"id\":\"ipv4-net-mask--ff26c055-6336-5bc5-b98d-13d6226742dd\",\"value\":\"255.255.0.0\"}]"

}

],

"Source": [

{

"IP": "77.222.222.115",

"Proto": [

"Unknown"

]

}

],

"Target": [

{

"IP": "172.20.7.25",

"Proto": [

"IP",

"Unknown"

],

"Location": "Datacenter SBX1"

}

]

}

## Cyber detection: Enrichment AD

Based on “3.1 Cyber Virus detected by a detector+sensor "all in one" alert. Adding associated observable.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fe876",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:05.21Z",

"EventTime": "2021-01-18T23:33:04.52Z",

"Cause": "Malicious",

"Category": [

"Intrusion.UserCompromise",

"Intrusion.SysCompromise",

"Malicious.System"

],

"AltCategory": [

"MITRE ATT&CK: T1566.001"

],

"Severity": "High",

"Description": "Execution of a malicious attachment could not be prevented",

"Ref": [

"https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp\_ixeshe.pdf"

],

"Analyzer": {

"IP": "172.100.0.2",

"Name": "EDR",

"Hostname": "jdoe.users.example.com",

"Type": "Cyber",

"Model": "Super EDR v1.2.3",

"Category": [

"SPAM",

"AV",

"EDR",

"HIDS"

],

"Data": [

"Data",

"File"

],

"Method": [

"signature"

]

},

"Source": [

{

"IP": "1.2.3.4",

"Hostname": "hacker.example.com",

"Proto": [

"tcp",

"smtp"

],

"Email": "refunds@yourbank.com",

"Attachment": [

"attach1"

],

"Observable": [

"obs1"

]

}

],

"Target": [

{

"IP": "172.100.0.2",

"Hostname": "jdoe.users.example.com",

"User": "jdoe",

"Email": "john.doe@example.com",

"Observable": [

"jdoe\_details"

]

}

],

"Attachment": [

{

"Name": "attach1",

"FileName": "Consumer Welfare Table.pdf",

"Hash": "md5:c61c231d93d3bd690dd04b6de7350abb",

"Size": 127728,

"Ref": [

"https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp\_ixeshe.pdf",

"http://contagiodump.blogspot.com/2009/12/dec-29-cve-2009-4324-adobe-0-day.html"

],

"Note": "This attachment refers to a malicious file and should only be handled by cybersecurity professionals.",

"ContentType": "application/pdf",

"ContentEncoding": "base64",

"Content": "ABCDEF\u20267890=="

}

],

"Observable": [

{

"Name": "obs1",

"Reference": "STIX",

"Content": "{\"type\":\"process\",\"pid\":314,\"name\":\"AcroRd32.exe\",\"extensions\":{\"windows-process-ext\":{\"aslr\_enabled\":true,\"dep\_enabled\":true,\"priority\":\"HIGH\_PRIORITY\_CLASS\",\"owner\_sid\":\"S-1-5-21-186985262-1144665072-74031268-1309\"}}}"

},

{

"Name": "jdoe\_details",

"Reference": "STIX",

"Content": "{\"type\":\"user-account\",\"spec\_version\":\"2.1\",\"id\":\"user-account--0d5b424b-93b8-5cd8-ac36-306e1789d63c\",\"user\_id\":\"1001\",\"account\_login\":\"jdoe\",\"account\_type\":\"unix\",\"display\_name\":\"John Doe\",\"is\_service\_account\":false,\"is\_privileged\":false,\"can\_escalate\_privs\":true,\"account\_created\":\"2016-01-20T12:31:12Z\",\"credential\_last\_changed\":\"2016-01-20T14:27:43Z\",\"account\_first\_login\":\"2016-01-20T14:26:07Z\",\"account\_last\_login\":\"2016-07-22T16:08:28Z\"}"

}

]

}

## Enrichment based on Cyber-Threat Intelligence data

An attempt to connect to the SpyEye trojan's C&C server was detected by a dedicated CTI analyzer. The detection is based on various pieces of information found in the corporate proxy server's logs (domain name, HTTP method, requested URL, etc.).

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef01",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Malicious.Distribution",

"Malicious.System",

"Intrusion.SysCompromise"

],

"Confidence": 0.9,

"Severity": "Medium",

"Description": "A system infected with the SpyEye trojan was detected",

"Ref": [

"http://www.malwaredomainlist.com/hostslist/spyeye.xml"

],

"Analyzer": {

"IP": "172.10.1.2",

"Name": "CTI Analyzer",

"Hostname": "cti.example.com",

"Type": "Cyber",

"Model": "CTI Analyzer v5.2",

"Category": [

"LOG"

],

"Data": [

"Connection",

"Protocol"

],

"Method": [

"recon"

]

},

"Sensor": [

{

"IP": "172.10.1.4",

"Name": "Proxy server",

"Hostname": "proxy.example.com",

"Model": "Squid v4.4"

}

],

"Source": [

{

"TI": [

"Hostname:malwaredomainlist"

],

"IP": "93.184.216.34",

"Hostname": "c2.example.com",

"Proto": [

"tcp",

"http"

],

"Port": [

80

]

}

],

"Target": [

{

"IP": "172.100.0.2",

"Hostname": "jdoe.users.example.com",

"User": "jdoe",

"Service": "firefox.exe",

"Observable": [

"obs1"

]

}

],

"Observable": [

{

"Name": "obs1",

"Reference": "STIX",

"Content": "\"type\":\"network-traffic\",\"spec\_version\":\"2.1\",\"id\":\"network-traffic--f8ae967a-3dc3-5cdf-8f94-8505abff00c2\",\"dst\_ref\":\"ipv4-addr--6da8dad3-4de3-5f8e-ab23-45d0b8f12f16\",\"protocols\":[\"tcp\",\"http\"],\"extensions\":{\"http-request-ext\":{\"request\_method\":\"post\",\"request\_value\":\"/e/bt\_version\_checker.php\",\"request\_version\":\"http/1.1\",\"request\_header\":{\"Accept-Encoding\":\"gzip,deflate\",\"User-Agent\":\"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\",\"Host\":\"c2.example.com\"}}}"

}

]

}

# Cyber Correlation / aggregation: enrichment

## N Alert for Single authentication failed

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb4",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T16:00:00.00Z",

"CeaseTime": "2021-01-18T20:00:00.00Z",

"AggrCondition": [

"Source.IP",

"Target.IP",

"Caategory"

],

"Cause": "Unknown",

"Category": [

"Attempt.Login"

],

"Severity": "Low",

"Confidence": 1,

"Analyzer": {

"IP": "1.1.1.4",

"Name": "Aggregator"

},

"Source": [

{

"IP": "2.2.2.2"

}

],

"Target": [

{

"IP": "1.1.1.1"

}

]

}

## Aggregation (condition) of a password brute force attack

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf1232b4",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T16:00:00.00Z",

"CeaseTime": "2021-01-18T20:00:00.00Z",

"AggrCondition": [

"Source.IP",

"Target.IP",

"Category"

],

"PredID": [

"e5f9bbae-163e-42f9-a2f2-0daaf78fefb4"

],

"Cause": "Malicious",

"Category": [

"Attempt.Login"

],

"Severity": "High",

"Confidence": 0.9,

"Description": "Brute-force attack",

"Analyzer": {

"IP": "1.1.1.4",

"Name": "Aggregator"

},

"Source": [

{

"IP": "2.2.2.2"

}

],

"Target": [

{

"IP": "1.1.1.1"

}

]

}

## Authentication failure for SSH service

A failed attempt at authenticating to a remote connection service (SSH service) with the "root" login was detected.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef01",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Recon.Scanning",

"Attempt.Login"

],

"Confidence": 1.0,

"Severity": "Low",

"Description": "error: Host key c7:18:8f:7f:92:a2:77:84:13:8f:08:67:54:7e:fb:95 blacklisted (see ssh-vulnkey(1))",

"Analyzer": {

"IP": "172.10.1.2",

"Name": "Local SIEM",

"Hostname": "siem.example.com",

"Type": "Cyber",

"Model": "Super SIEM v5.2",

"Category": [

"LOG"

],

"Data": [

"Log"

],

"Method": [

"signature"

]

},

"Sensor": [

{

"IP": "172.10.1.1",

"Name": "Remote connection service",

"Hostname": "mail.example.com",

"Model": "OpenSSH v7.4p1"

}

],

"Source": [

{

"IP": "1.2.3.4",

"Hostname": "hacker.example.com",

"Proto": [

"tcp",

"ssh"

],

"Port": [

1234

]

}

],

"Target": [

{

"IP": "172.10.5.30",

"Hostname": "mail.example.com",

"GeoLocation": "+48.5840961,+7.7509093,+14",

"UnLocation": "FR SXB",

"Location": "SBG1 DC",

"User": "root",

"Service": "sshd",

"Port": [

22

]

}

]

}

## Authentication failure for HTTP service

A failed attempt at authenticating to a web application with the "admin" login was detected.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef02",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Recon.Scanning",

"Attempt.Login"

],

"Confidence": 1.0,

"Severity": "Low",

"Description": "401 Unauthorized",

"Analyzer": {

"IP": "172.10.1.2",

"Name": "Local SIEM",

"Hostname": "siem.example.com",

"Type": "Cyber",

"Model": "Super SIEM v5.2",

"Category": [

"LOG"

],

"Data": [

"Log"

],

"Method": [

"signature"

]

},

"Sensor": [

{

"IP": "172.10.1.1",

"Name": "Internet-facing webserver",

"Hostname": "www.example.com",

"Model": "Apache HTTP Server v2.4.8"

}

],

"Source": [

{

"IP": "1.2.3.4",

"Hostname": "hacker.example.com",

"Proto": [

"tcp",

"http"

],

"Port": [

2345

]

}

],

"Target": [

{

"IP": "172.10.5.30",

"Hostname": "www.example.com",

"GeoLocation": "+48.5840961,+7.7509093,+14",

"UnLocation": "FR SXB",

"Location": "SBG1 DC",

"User": "admin",

"Service": "httpd",

"Port": [

80,

8080

]

}

]

}

## Authentication failure for SMTP service

A failed attempt at authenticating to the corportate mail server with the "jdoe" login was detected.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef03",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Recon.Scanning",

"Attempt.Login"

],

"Confidence": 1.0,

"Severity": "Low",

"Description": "535 Authentication failed",

"Analyzer": {

"IP": "172.10.1.2",

"Name": "Local SIEM",

"Hostname": "siem.example.com",

"Type": "Cyber",

"Model": "Super SIEM v5.2",

"Category": [

"LOG"

],

"Data": [

"Log"

],

"Method": [

"signature"

]

},

"Sensor": [

{

"IP": "172.10.5.30",

"Name": "Mail gateway",

"Hostname": "mail.example.com",

"Model": "sendmail v8.14.7"

}

],

"Source": [

{

"IP": "1.2.3.4",

"Hostname": "hacker.example.com",

"Proto": [

"tcp",

"smtp"

],

"Port": [

3456

]

}

],

"Target": [

{

"IP": "172.10.5.30",

"Hostname": "mail.example.com",

"GeoLocation": "+48.5840961,+7.7509093,+14",

"UnLocation": "FR SXB",

"Location": "SBG1 DC",

"User": "jdoe",

"Service": [

"smtp",

"sendmail"

],

"Port": [

25

]

}

]

}

## Multiple authentication failures (password spraying attack)

Based on the previous alerts related to authentication failures, a password spraying attack is detected, i.e. an attempt to use a given password against multiple user accounts/services in order to get initial access to the corporate network.

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fef19",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"CorrelID": [

"e5f9bbae-163e-42f9-a2f2-0daaf78fef01",

"e5f9bbae-163e-42f9-a2f2-0daaf78fef02",

"e5f9bbae-163e-42f9-a2f2-0daaf78fef03"

],

"Category": [

"Recon.Scanning",

"Attempt.Login"

],

"Confidence": 0.8,

"Severity": "Medium",

"Description": "Password spraying attack detected",

"Analyzer": {

"IP": "172.10.1.2",

"Name": "Alert correlator",

"Hostname": "siem.example.com",

"Type": "Cyber",

"Model": "Super Correlator v5.2",

"Category": [

"LOG"

],

"Data": [

"Correlation"

],

"Method": [

"recon"

]

}

}

## Single authentication failed detected by detector

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb5",

"CreateTime": "2021-01-18T23:33:09.21Z",

"Cause": "Unknown",

"Category": [

"Attempt.Login"

],

"Description": "Login attempt through SSH",

"Severity": "Low",

"Confidence": 1,

"Analyzer": {

"IP": "1.1.1.6",

"Name": "Detector"

},

"Sensor": [

{

"Name": "SSH"

}

],

"Source": [

{

"IP": "2.2.2.2"

}

],

"Target": [

{

"IP": "1.1.1.4",

"User": "admin",

"Service": "sshd",

"Port": [

22

]

}

]

}

## Correlator analyze the alert and add CTI on IP source

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0da12453efb5",

"CreateTime": "2021-01-18T23:33:09.21Z",

"Cause": "Malicious",

"PredID": [

"e5f9bbae-163e-42f9-a2f2-0daaf78fefb5"

],

"Category": [

"Attempt.Login"

],

"Description": "Login attempt through SSH",

"Severity": "High",

"Confidence": 1,

"Analyzer": {

"IP": "1.1.1.6",

"Name": "Detector"

},

"Sensor": [

{

"Name": "SSH"

}

],

"Source": [

{

"IP": "2.2.2.2",

"TI": [

"IP:Dshield"

]

}

],

"Target": [

{

"IP": "1.1.1.4",

"User": "admin",

"Service": "sshd",

"Port": [

22

]

}

]

}

# Physical correlation / aggregation

## Physical correlation / aggregation Alert 1 : Drone detection

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:05.21Z",

"DetectTime": "2021-01-18T23:33:04.52Z",

"Cause": "Unknown",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Low",

"Confidence": 0.9,

"Description": "Unknown drone intrusion detected",

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Camera42",

"Hostname": "camera42.example.com",

"Type": "Physical",

"Model": "MMAS.MOVEMENT",

"Category": [

"ADS"

],

"Data": [

"Video"

],

"Method": [

"Monitor"

],

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "GS Entrance"

},

"Sensor": [

{

"CaptureZone": "{\"type\":\"conic-zone\",\"Azimuth\":34.00,\"El\u00e9vation\":-30.00,\"Range\":600.00,\"HFOV\":200.00,\"VFOV\":20.00}"

}

],

"Target": [

{

"Location": "GS Entrance"

}

],

"Vector": [

{

"Category": "Drone",

"Name": "Unknown",

"Size": "Small",

"Observable": [

"PTZ Relative position"

]

}

],

"Observables": [

{

"Name": "PTZ Relative position",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":34.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

}

]

}

## Physical correlation / aggregation Alert 2 : Drone detection

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0ddaf78fefb1",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:15.21Z",

"DetectTime": "2021-01-18T23:33:14.52Z",

"Cause": "Unknown",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Low",

"Confidence": 0.9,

"Description": "Unknown drone intrusion detected",

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Camera42",

"Type": "Physical"

},

"Target": [

{

"Location": "GS Entrance"

}

],

"Vector": [

{

"Category": "Drone",

"Name": "Unknown",

"Size": "Small",

"Observable": [

"PTZ Relative position"

]

}

],

"Observables": [

{

"Name": "PTZ Relative position",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":37.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

}

]

}

## Physical correlation / aggregation Alert 3 : Drone detection

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78aefb1",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:25.21Z",

"DetectTime": "2021-01-18T23:33:24.52Z",

"Cause": "Unknown",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Low",

"Confidence": 0.9,

"Description": "Unknown drone intrusion detected",

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Camera42",

"Type": "Physical"

},

"Target": [

{

"Location": "GS Entrance"

}

],

"Vector": [

{

"Category": "Drone",

"Name": "Unknown",

"Size": "Small",

"Observable": [

"PTZ Relative position"

]

}

],

"Observables": [

{

"Name": "PTZ Relative position",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":42.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

}

]

}

## Aggregation (liste ?) : Drone moving in area

{

"Version": "0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf79fefb1",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:26.21Z",

"StartTime": "2021-01-18T23:33:04.52Z ",

"CeaseTime": "2021-01-18T23:33:24.52Z ",

"AggCondition": [

"Category",

"Target.Location",

"Vector.Category"

],

"Cause": "Unknown",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Medium",

"Confidence": 0.9,

"Description": "Unknown drone moving in GS Area",

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Geo Correlator",

"Hostname": "geocorrelator.example.com",

"Type": "Physical",

"Model": "MMAS.MOVEMENT",

"Category": [

"ADS"

],

"Data": [

"Alerts"

],

"Method": [

"Correlation"

],

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "GS Datacenter"

},

"Target": [

{

"Location": "GS Entrance"

}

],

"Vector": [

{

"Category": "Drone",

"Name": "Unknown",

"Size": "Small",

"Observable": [

"PTZ1",

"PTZ2",

"PTZ3"

]

}

],

"Observable": [

{

"Name": "PTZ1",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":34.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

},

{

"Name": "PTZ2",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":37.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

},

{

"Name": "PTZ3",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":42.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

}

]

}

## update of the alert

{

"Version": "0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0da123459fefb1",

"Status": "Incident",

"Entity": "EXAMPLE",

"CreateTime": "2021-01-18T23:33:30.21Z",

"StartTime": "2021-01-18T23:33:04.52Z ",

"CeaseTime": "2021-01-18T23:33:28.52Z ",

"AggCondition": [

"Category",

"Target.Location",

"Vector.Category"

],

"PredID": [

"e5f9bbae-163e-42f9-a2f2-0daaf79fefb1"

],

"Cause": "Unknown",

"Category": [

"Intrusions.Burglary"

],

"Severity": "Medium",

"Confidence": 0.9,

"Description": "Unknown drone moving in GS Area",

"Analyzer": {

"IP": "172.10.5.31",

"Name": "Geo Correlator",

"Hostname": "geocorrelator.example.com",

"Type": "Physical",

"Model": "MMAS.MOVEMENT",

"Category": [

"ADS"

],

"Data": [

"Alerts"

],

"Method": [

"Correlation"

],

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "GS Datacenter"

},

"Target": [

{

"Location": "GS Entrance"

}

],

"Vector": [

{

"Category": "Drone",

"Name": "Unknown",

"Size": "Small",

"Observable": [

"PTZ1",

"PTZ2",

"PTZ3",

"PTZ4"

]

}

],

"Observable": [

{

"Name": "PTZ1",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":34.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

},

{

"Name": "PTZ2",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":37.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

},

{

"Name": "PTZ3",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":42.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

},

{

"Handle": "PTZ4",

"Reference": "IDMEFv2",

"Content": "{\"type\":\"PTZ\",\"Pan\":45.00,\"Tilt\":-30.00,\"Zoom\":18.00}"

}

]

}

# Availability

## Abnormal temperature detected in a server

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Confidence": 1.0,

"Severity": "Critical",

"Description": "The internal temperature is outside permitted thresholds (81\u00b0C > 80\u00b0C)",

"Analyzer": {

"IP": "172.10.1.1",

"Name": "Local NMS",

"Hostname": "nms.example.com",

"Type": "Physical",

"Model": "Super NMS v5.2",

"Category": [

"NMS"

],

"Data": [

"Temperature"

],

"Method": [

"heat"

]

},

"Sensor": [

{

"IP": "172.10.1.2",

"Name": "Local monitoring server",

"Hostname": "nagios1.example.com",

"Model": "Nagios v4.5.2"

}

],

"Target": [

{

"IP": "172.10.5.30",

"Hostname": "mail.example.com",

"GeoLocation": "+48.5840961,+7.7509093,+14",

"UnLocation": "FR SXB",

"Location": "SBG1 DC"

}

]

}

## Device stopped responding to ICMP PING solicitations

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",

"Status": "Incident",

"Entity": "ACME",

"CreateTime": "2021-01-18T23:33:05.21Z",

"StartTime": "2021-01-18T23:33:04.52Z",

"Category": [

"Availability.Outage"

],

"Confidence": 1.0,

"Severity": "Critical",

"Description": "CRITICAL - 172.10.5.31: rta nan, lost 100%",

"Analyzer": {

"IP": "172.10.1.1",

"Name": "Local NMS",

"Hostname": "nms.example.com",

"Type": "Availability",

"Model": "Super NMS v5.2",

"Category": [

"NMS"

],

"Data": [

"Protocol"

],

"Method": [

"Threshold"

]

},

"Sensor": [

{

"IP": "172.10.5.1",

"Name": "Security Center",

"Hostname": "sec-center.example.com",

"Model": "Security Center v5.7",

"UnLocation": "GR ATH",

"Location": "Security Office"

}

],

"Target": [

{

"IP": "172.10.5.31",

"Hostname": "camera1.example.com",

"GeoLocation": "+48.75726,+2.299528,+65.1",

"UnLocation": "GR ATH",

"Location": "Front Door"

}

]

}

## Alert on external temperature planned to be high AND temperature high in DataCenter

{

"Version": "2.0.3",

"ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb6",

"CreateTime": "2021-01-18T23:33:09.21Z",

"Cause": "Unknown",

"Category": [

"Meteorological.Temperature"

],

"Severity": "high",

"Confidence": 1,

"Description": "High temperature in DataCenter and outside",

"CorrelID": [

"e5f9bbae-163e-42f9-a2f2-0daaf78fefa1",

"e5f9bbae-163e-42f9-a2f2-0daaf78fefa2"

],

"Analyzer": {

"IP": "1.1.1.5",

"Name": "Correlator"

}

}