**IDMEF Examples**

Intrusion Detection Message Exchange Format

V 0.2

# Example 1: Cyber message example in IDMEF v0.2 format

Login attempt from Internet to a Linux station through the SSH protocol. The targeted device’s hostname is “lnx8.tls.acme.eu” and the attempt occurred on January 18th 2021 at 23:33.

{

"Version": "0.1",

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

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

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

"Cause": "Malicious",

"CategoryRef": "ENISA : RIST",

"Category": ["Intrusion Attempts.Login attempts"],

"Severity": "low",

"Confidence": 0.9,

"Description": "Someone tried to login as root from 218.49.183.17 port 20486 using the ssh2 method",

"Agent": {

"ID": "azdabae-543e-21f9-f7f2-afjkn12324",

"Name": "Cyber Detect Module",

"Model": "SuperDetector v3.14",

"Category": ["SIEM"],

"Data": ["Log"],

"Method": ["Signature"],

"Hostname": "lnx8.tls.acme.eu",

"IP4": "192.168.1.1",

"IP6": "2001:db8::1"

},

"Source": [

{

"Proto": ["tcp", "ssh"],

"IP4": ["218.49.183.17"]

}

],

"Target": [

{

"Hostname": ["lnx8.tls.acme.eu"],

"Service": ["sshd"],

"IP4": ["192.168.1.1"]

}

]

}

Proto : Keep in mind that the protocols/services listed here must be ordered from the one closest to the medium to the one furthest from the medium.

# Example 2: Physical message example in UAF format

An unknown person is running towards the GS area and has been detected by the camera named “Camera42” positioned in the GS entryway. The hostname of the camera is “camera42.acme.eu”.

{

"Version": "0.1",

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

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

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

"Cause": "Malicious",

"CategoryRef": "ENISA : RIST",

"Category": ["Intrusions.Burglary"],

"Severity": "high",

"Confidence": 0.4,

"Description": "An unknown person is moving towards the GS area",

"Agent": {

"ID": "azdabae-543e-21f9-f7f2-afjkn12324",

"Name": "Camera42",

"Model": "AXIS Q8742-E",

“Category”: ["HAR"],

"Data": ["Video"],

"Method": ["Statistical"],

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

"UnLocation": "GR ATH",

"Location": "GS Entryway",

"Hostname": "camera42.acme.eu",

"IP4": "192.24.37.78",

"IP6": "2001:db8::1",

"Azimuth": 34,

"Elevation": -30,

"Range": 600,

"HFOV": 200,

"VFOV": 200

},

"Vector": [

{

"Category": "face",

"Name": “John Doe”

"GeoLocation": "+22.75726, +5.299528, +20.1",

"GeoRadius": 0,

"Location": "GS Area"

}

]

}