**7SHIELD UAF Examples**

Unified Alert Format

V 0.1

# Example 1: Cyber message example in UAF format

Login attempt from Internet to a Linux station through the SSH protocol. The targeted device is lnx8.tls.acme.eu and the attempt was done at 23h33 on 2021-01-18.

{

"Version": "0.1",

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

"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",

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

"Agent": {

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

"Name": "Cyber Detect Module",

"Category": "SIEM",

"Data": "Log",

"Method": "Signature",

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

"IP4": ["192.168.1.1"]

},

"Source": [

{

"IP4": ["218.49.183.17"],

"Proto": [ "ssh”, “tcp"],

}

],

"Target": [

{

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

"Service": "sshd",

"IP4": ["192.168.1.1"],

}

]

}

# Example 2: Physical message example in UAF format

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

{

"Version": "0.1",

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

"Cause": "Malicious",

"CategoryRef": "ENISA : RIST",

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

"Severity": "High",

"Confidence": "0.4",

"Description": "Unknown person is moving towards the GS area",

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

"Agent": {

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

"Name": "Camera42",

“Category”: [“HAR”],

"Model": "AXIS Q8742-E",

"Data": "Video",

"Method": "Statistical",

"GeoLocation": "+48.75726 , +2.299528, +65,1",

"Azimuth": 34,

"Elevation": "-30",

"Range": "600",

"HFOV": "200",

"VFOV": "200",

"UnLocation": "GR, ATH",

"Location": "GS Entrance",

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

"IP4": ["192.24.37.78"]

},

"Vector": [

{

"Category": "Face",

"Name": “John Doe”

"GeoLocation": "+22.75726 , +5.299528, +20,1",

"GeoRadius": "0",

"Location": "GS Area"

}

]

}