CYBEATS

Automation Village

Vulnerability Early Warning System

Dmitry Raidman

April 2024

CVE IOE (Indication Of Active Exploitation)

RWR (Threat Warning Receiver)

01

Shows data picked up by aircraft sensors to identify radar scan spikes emitted by enemy or weapons

Vulnerability Early Warning Lifecycle

Warnings are distributed using STIX format and consumed by SBOM Management Platforms

1

TAXII

Threat Intelligence Sensors (Honeypots) - TIP

STIX

CYWARE™

2

Threat Intelligence to Asset Correlation

CYBEATS { IOE SBOM VEX }

3

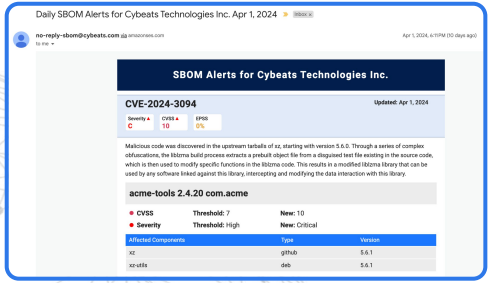
Responders Mitigation

cacao PLAYBOOKS

VEX DRIVEN RESPONSE

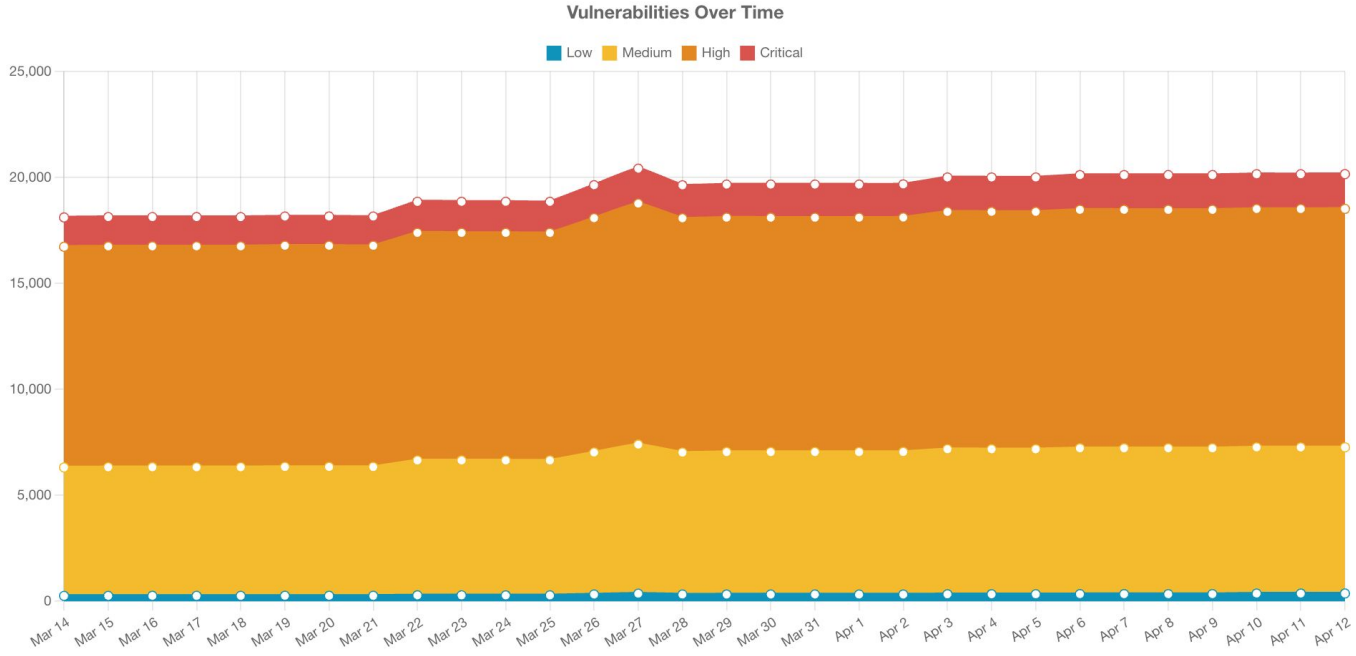

```
{
    "type": "vulnerability",
    "spec_version": "2.1",
    "id": "vulnerability--8323404c-1fdd-4272-822b-829f85556c53",
    "created": "2024-03-29T09:12:16.432Z",
    "modified": "2024-04-03T09:12:16.432Z",
    "name": "CVE-2024-3094",
    "description": "lzma vulnerability exploited by APTXX",
    "external_references": [
      {
        "source_name": "cve",
        "external_id": "CVE-2011-3544"
      }
    ]
}
```

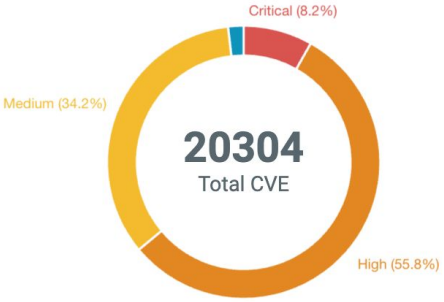

API



Who has this problem?

How we can find what software based products affected by 🚨CVE-2024-3094🚨?





Demo Time
02

SBOM based rapid identification of assets impacted by 🚨 CVE-2024-3094 🚨 aka “xz” supply-chain attack

Rapid impact analysis getting actionable answers <5 sec

Single API call to display all affected products and business units (BUs/OUs), incorporating VEX data.

Cybeats' Universal Governor Public API: {{api-url}}/governors/analytics/details -> (Supports batch CVEs query)

Request Body:

```
{
    "vulnIds": ["CVE-2024-3094"]
}
```

Response, Part 1: The whole request completes **in about 1 sec**: Status: 200 OK Time: 934 ms Size: 4.05 KB


```
"id": "CVE-2024-3094",
                "cvssV3": 10,
                "cvssV3Version": "3.1",
                "vectorStringV3": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
                "epss": 0.0012,
                "published": 1711732500,
                "modified": 1712906100,
                "summary": "Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0.",
                "cwes": [
                    {
                        "id": "CWE-506"
                    }
                ],
```

Rapid search means we have under 5 sec to get results

We want **one** API call that shows all affected business units (BUs) or (OUs), and simple to use

Response, Part 2: This part of the API call response returns all the high-level (products): device, service, software


```
"impactedOrgs": [
  {
    "orgName": "Cybersecurity Automation Village Organization",
    "products": [
      {
        "type": "device",
        "name": "Pet Feeder",
        "version": "1.0",
        "vexes": [
          {
            "vulnId": "CVE-2024-3094",
            "analysisStatus": "not_affected",
            "analysisJustification": "code_not_reachable",
            "analysisResponse": [
              "will_not_fix"
            ],
            "analysisDetails": "The vulnerable code is not reachable due to the architecture of the device.",
            "analysisInternalDetails": "Validated with exploit EDB-ID: XXXXX"
          }
        ]
      }
    ],
```


Based on VEX data provided by manufacturer we are out of the danger zone. The lower level components are affected see next slides, the product we use is not affected.

We still can validate vendor's findings and keep as internal note in the platform see **`analysisInternalDetails`**.

Rapid search means we have under 5 sec to get results

We want **one** API call that shows all affected business units (BUs) or (OUs), and simple to use

Response, Part 3: This part of the API call response returns all the mid-level components like apps, containers, firmware, etc...


```
    "applications": [
      {
        "pkgType": "generic",
        "name": "pet-scheduler",
        "version": "1.83",
        "purl": "pkg:generic/pet-scheduler@1.83",
        "vexes": [
          {
            "vulnId": "CVE-2024-3094",
            "analysisStatus": "affected",
            "analysisResponse": [
              "will_not_fix"
            ],
            "analysisDetails": "Mitigated by disabling network access to the host on port 7878, use CACAO Mitigation Playbook
for CISCO FW",
            "analysisInternalDetails": "This it not real VEX record for demo purposes"
          }
        ]
      }
    ],
```

Rapid search means we have under 5 sec to get results

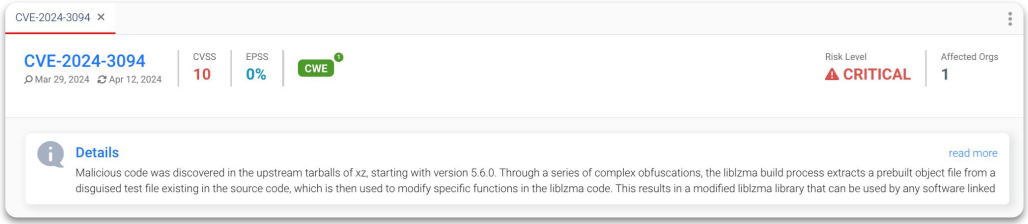
We want **one** API call that shows all affected business units (BUs) or (OUs), and simple to use

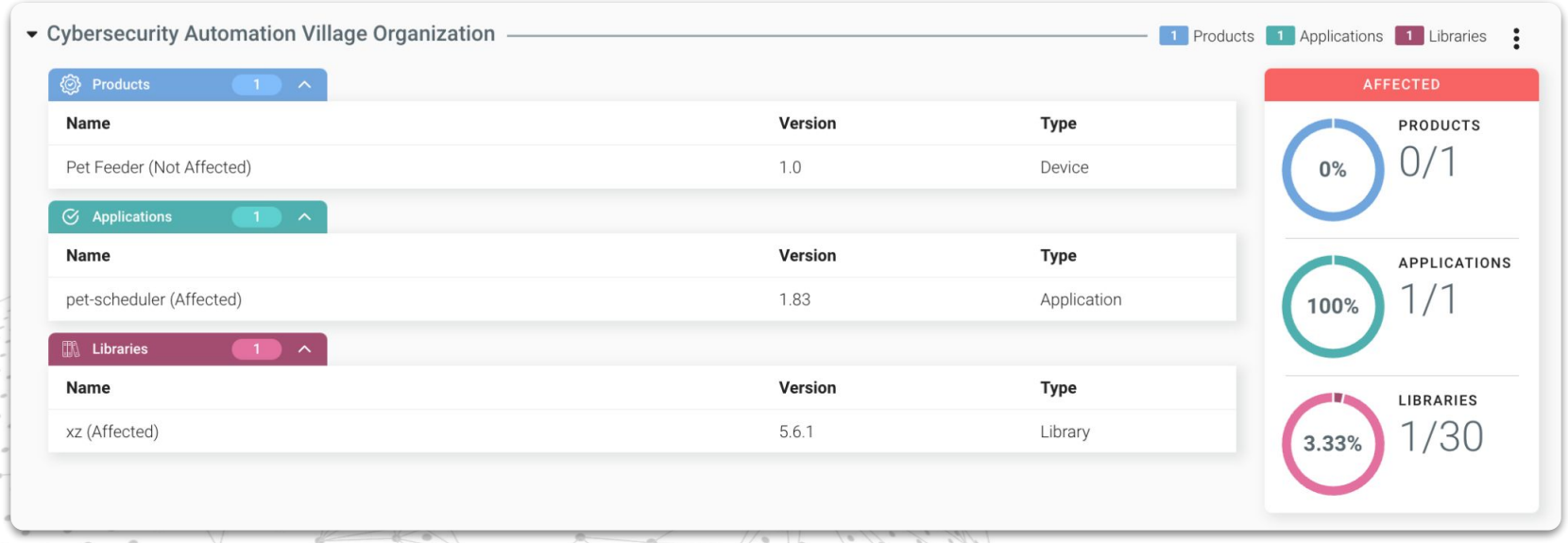
Response, Part 4: This part of the API call response returns all the low level components like packages and libs


```
    "libraries": [
      {
        "pkgType": "generic",
        "name": "xz",
        "version": "5.6.1",
        "purl": "pkg:generic/xz@5.6.1",
        "vexes": [
          {
            "vulnId": "CVE-2024-3094",
            "analysisStatus": "affected",
            "analysisResponse": [
              "will_not_fix"
            ],
            "analysisDetails": "Mitigated by disabling network access to the host on port 7878, use CACAO Mitigation
Playbook for CISCO FW",
            "analysisInternalDetails": "This it not real VEX record for demo purposes"
          }
        ]
      }
    ]
  }
]
```

Not a big fan of APIs?

How **Cybeats SBOM Studio** will show it?





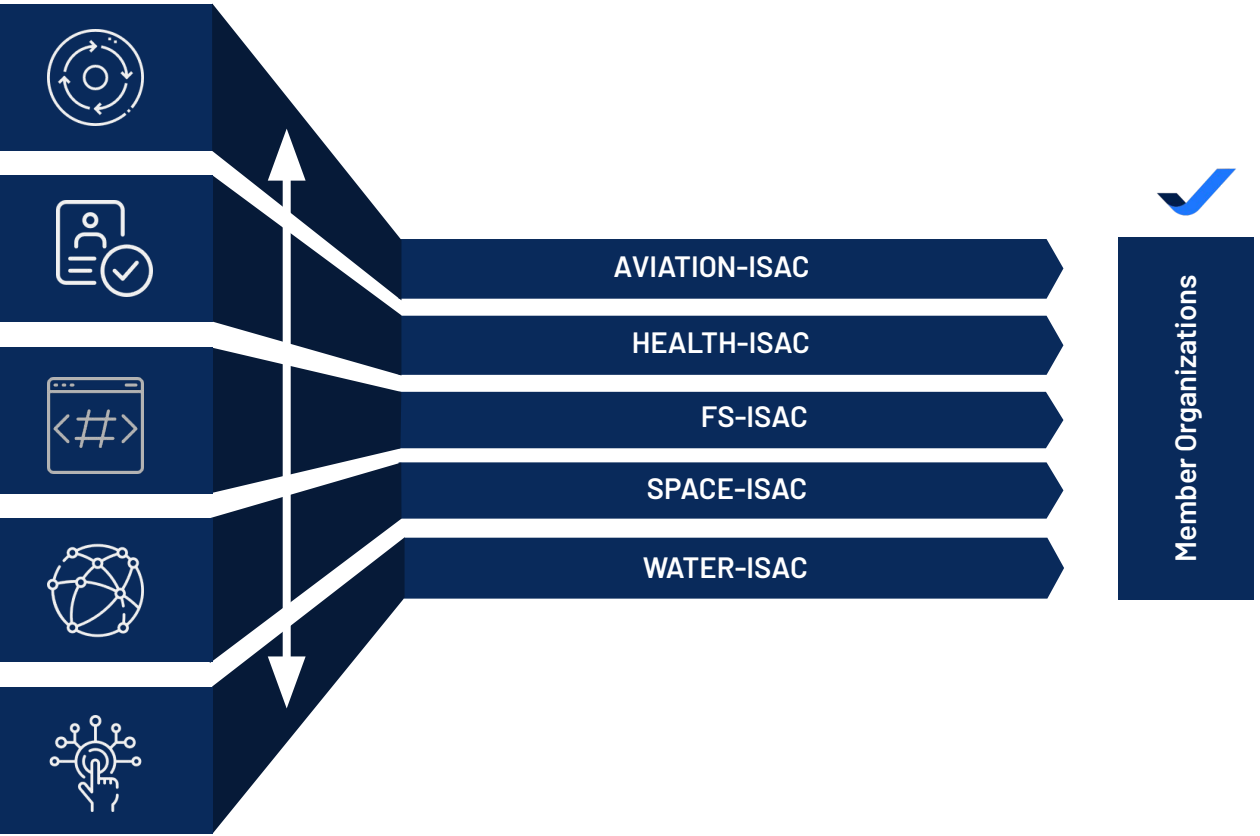
ISAC/AWACS

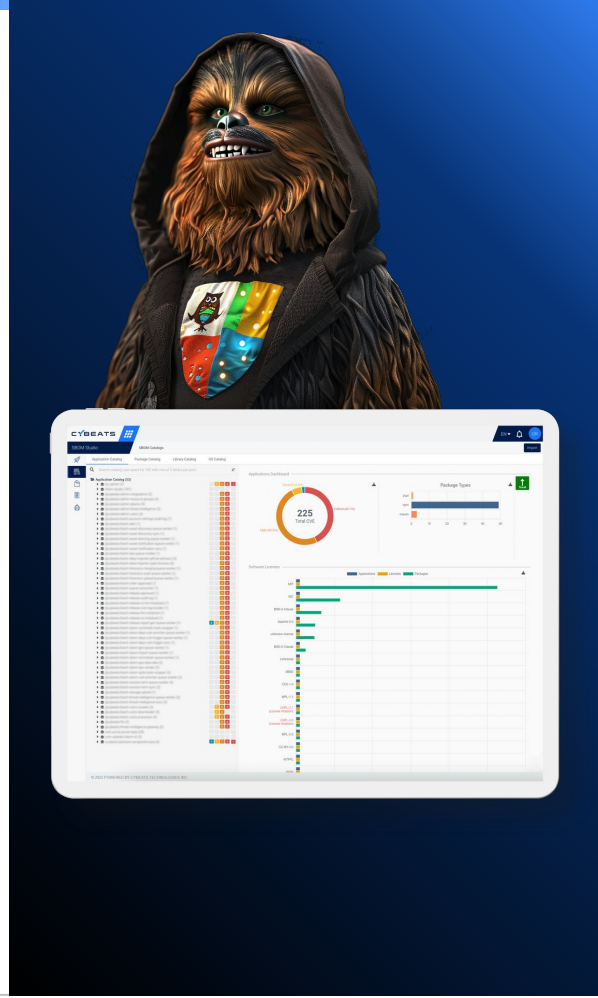
03

Getting cross domain threat intelligence data, enriching and distributing to community members

Horizontal and Vertical Sharing of IOEs

Indication of Exploitation Information is shared between ISACs and to Members





Thank You

04

“For demo contact us you shall”
“May the SBOM be with you”

✓ **https://cybeats.com**