CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

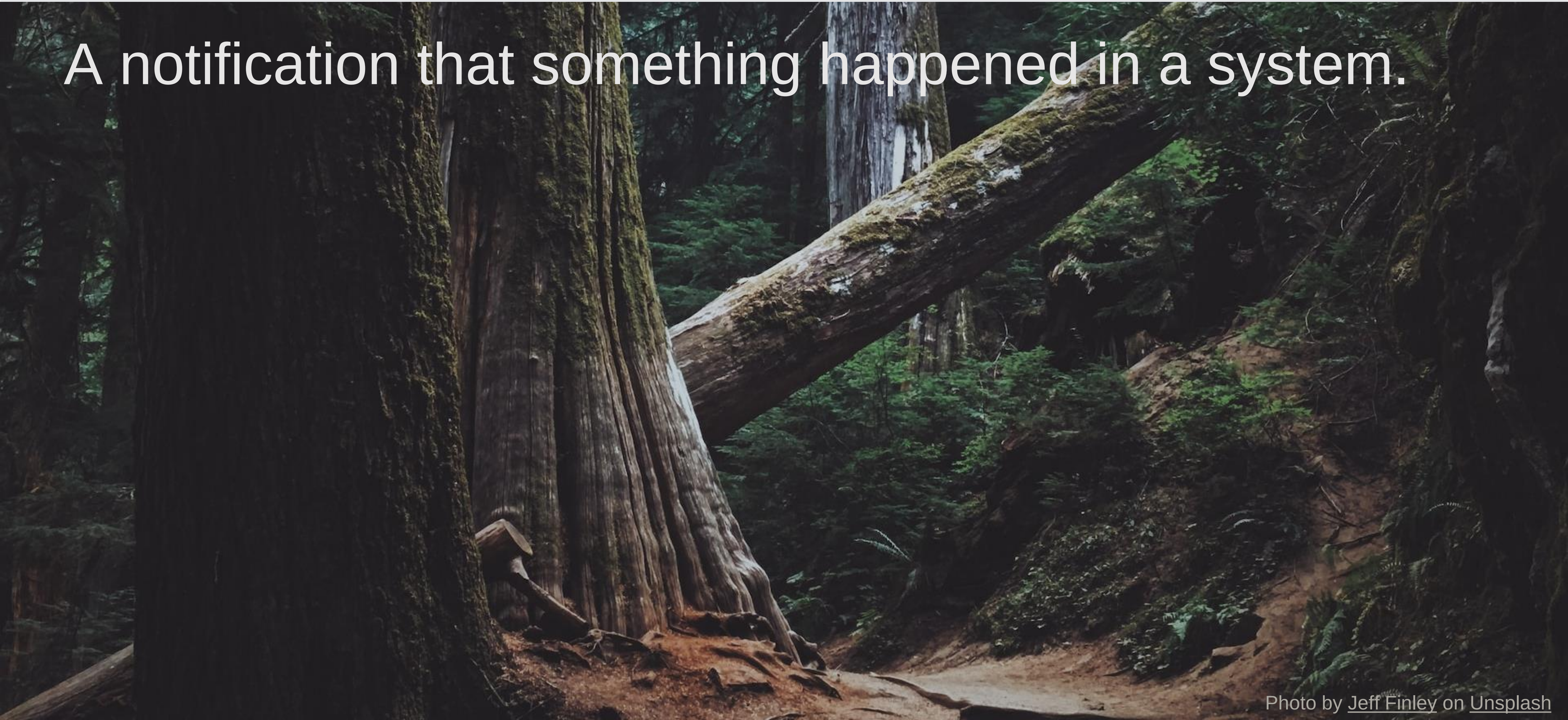
CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

Cloud(Security)Events

A Lightweight Framework For Security Reactions

Evan Anderson

What Is An Event?



A notification that something happened in a system.

Photo by Jeff Finley on Unsplash

What Is CloudEvents?

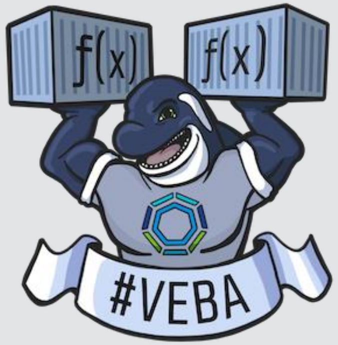
CNCF project to standardize event format and metadata

Key fields (extensible):

```
type
source
id
timestamp
```

Documented formats:

- JSON
- AVRO
- Protobuf
- XML



Security Events

Before an Incident

- Software builds
- Deployments
- Vulnerability Scans
- CVEs
- Test results
- SDL process stages

Incident Response

- Unexpected System Calls
- Configuration Changes
- Network Connections
- Logins and Authentications
- Tokens or certs issued

Examples?

Falco has a series of blog posts using the following projects to achieve the same result:

- Delete any pod which spawns an interactive terminal shell

https://falco.org/blog/falcosidekick-response-engine-part-1-kubeless/

Example Events

```
ce-specversion: 1.0
ce-type: falco.rule.output.v1
ce-source: falco.org
ce-id: f7628198-3822-4c98-ac3f-71770e272a16
ce-time: 2023-01-11T21:45:31Z
ce-rule: Terminal shell in container

{
  "output": "21:45:31 ...",
  "rule": "Terminal shell in container",
  "output_fields": {
    "container.id": "f29b261f8831",
    "container.image.repository": "mysql",
    "k8s.ns.name": "default",
    "k8s.pod.name": "alpine",
    "proc.cmdline": "bash -il",
    "proc.name": "bash",
    "proc.pname": "runc",
    "proc.tty": 34816,
    "user.loginuid": -1,
    "user.name": "root“
  }
}
```

```
ce-specversion: 1.0
ce-type: dev.cdevents.service.upgraded.0.1-draft
ce-source: https://my-argo-instance.dev/
ce-subject: /namespaces/myns/deployments/foo
ce-time: 2023-01-18T22:14:17Z
ce-id: e699633e-de83-4427-a6dd-9e702ae008d9-8

{
  "context": {
    ...
  },
  "subject": {
    "id": "deployments/foo“,
    "environment": {
      "id": “namespaces/myns",
      "source": "...",
      "name": "staging",
      "url": "..."
    },
    "artifactId": "oci:/..."
  }
}
```

If You Are A Vendor:

Generate CloudEvents!

Document how to consume them – webhook, kafka topic, etc

Document your event types and schemas

If You Are An End-User:

Remediation data (react immediately):

- Use event routing and serverless to automatically remediate!

SIEM data (keep for medium time to support post-hoc analysis):

- Index and store in queryable format. (BigQuery / Snowflake)

Critical data (keep for a long time as part of audit records):

- Archive and store as log-type records. (S3 / cold storage)

Thank You!

Please scan the QR Code above
to leave feedback on this session