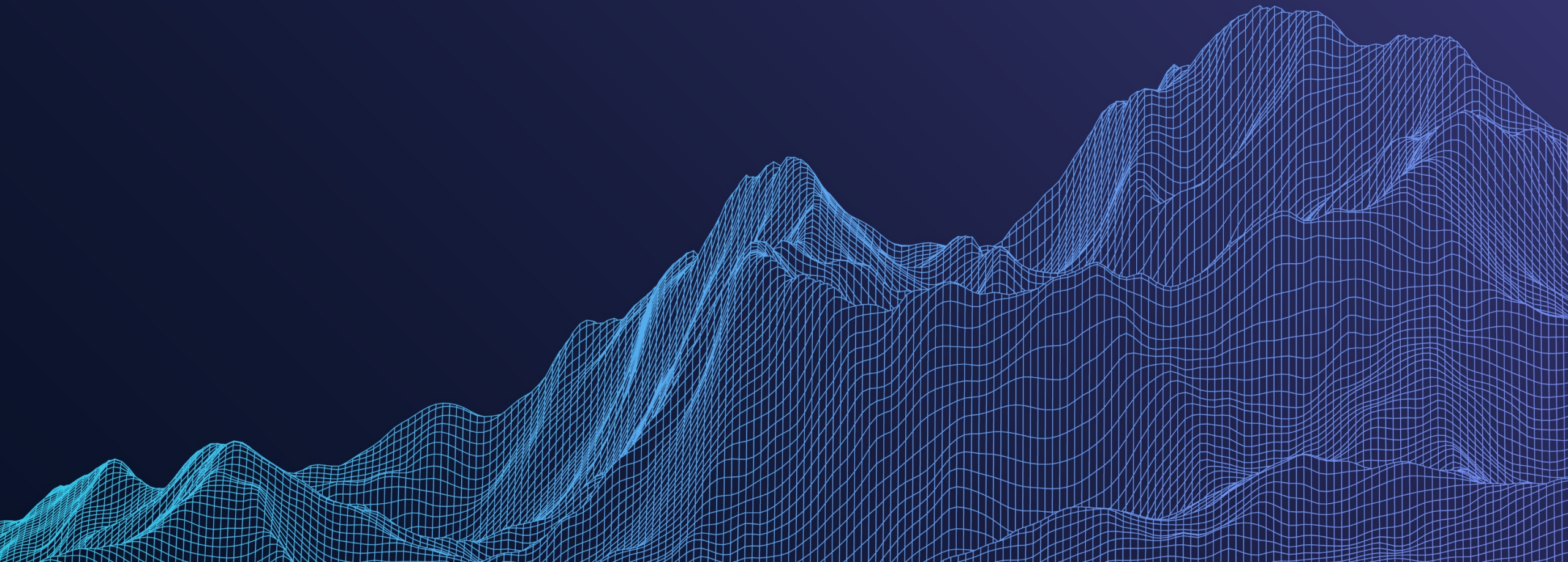
KENNA Security

Kenna Security -

(ISC)² Partnership and Education Credit Program



What's New with Kenna in 2021?

(ISC)² | CPE SUBMITTER

Kenna is now an official partner of (ISC)² !

- Customers that participate in live Kenna's webinar programs, can receive CPE (continuing education credits) toward (ISC)² certification.
- Kenna is initiating this program with a focus on webinar programs and may expand into other digital programs in 1H 2021

What do you need to do?

- ✓ ***Provide*** your ISC2 member ID when registering for a Kenna webinar
- ✓ ***Attend*** the live webinar
- ✓ Kenna will submit attendance info to (ISC)²
- ✓ (ISC)² will reflect credit for attendance in your personal (ISC)² account
- ✓ (ISC)² may take up to10 business days before the credit is reflected in your account
- ✓ One CPE Credit is earned for each hour of attendance

KENNA Security

KENNA Security

Getting the Most Out of Data Exports

Katie Kolon and Jared Kalmus

Kenna Security, Customer Success Engineer

2/5/2021

Getting the Most Out of Data Exports

Agenda

- Use cases for data exports
  - Custom reporting
  - Historical reporting
  - Audit/Compliance requirements
- Types of Exports
  - Assets
  - Vulnerabilities
  - Fixes
- Generating Exports
  - Crafting API Requests
  - Output file formats
  - Incremental Exports

KENNA Security

Group Chat Question

Is anyone already using data exports in your organization? If so what use cases are you accomplishing?

KENNA Security

Use Cases for Data Exports

- Customized Reporting
  - While Kenna offers many great reporting features, no vendor product will ever perfectly match your organizations' unique reporting needs
  - Exporting data from Kenna opens up even more integration opportunities with data lakes, SIEMs, etc.
- Historical Reporting
  - Kenna is not a historical reporting tool
  - Exporting the data for offline storage allows more in-depth inquiries into trends and "look back" analysis
- Audit/Compliance Requirements
  - Many frameworks and regulations require data to be stored offline and/or for a certain number of years

KENNA Security

Types of Data Exports

- Kenna provides three different types of exports
  - Assets
  - Vulnerabilities
  - Fixes
- Each export type provides a different data set
- The export type can be defined in the API request
- Combining these three export types allow you to fully replicate your full Kenna data set outside of the user interface

KENNA Security

Asset Exports

- Each asset is listed by its ID with all known metadata included such as
  - Asset priority
  - Operating system
  - Tags
  - Asset owner
  - IP address
  - Hostname
  - MAC address
  - Etc…


```
{
    "id": 11012,
    "created_at": "2020-11-06T21:18:21Z",
    "priority": 10,
    "operating_system": "Microsoft Windows Server 2008 R2 Standard Service Pack 1",
    "notes": null,
    "last_booted_at": null,
    "primary_locator": "mac_address",
    "locator": "00:50:56:81:01:df",
    "vulnerabilities_count": 29,
    "status": "active",
    "last_seen_time": "2013-07-01T11:47:23Z",
    "network_ports": [
        {
            "id": 55204,
            "port_number": 80,
            "extra_info": "",
            "hostname": null,
            "name": "www",
            "ostype": "",
            "product": null,
            "protocol": "tcp",
            "state": "open",
            "version": null
        },
        {
        {
        {
        {
        {
        {
        {
        {
        {
        {
    ],
    "tags": [],
    "owner": null,
    "inactive_at": null,
    "status_set_manually": false,
    "urls": {
        "vulnerabilities": "api.kennasecurity.com/assets/11012/vulnerabilities"
    },
    "ip_address": "10.31.112.26",
    "database": null,
    "hostname": "qa3app06",
    "fqdn": null,
    "netbios": "QA3APP06",
    "application": null,
    "file": null,
    "mac_address": "00:50:56:81:01:df",
    "ec2": null,
    "url": null,
    "external_id": null,
    "ipv6": null,
    "risk_meter_score": 320,
    "asset_groups": [
        {
            "id": 251316,
            "name": "All Assets"
        },
        {
            "id": 252525,
            "name": "Nessus"
        },
        {
```

Vulnerability Exports

- Each finding of a vulnerability is included separately
- As an example, if CVE-2021-1234 is found on 25 assets, we'll have 25 entries in the export
- Data points include
  - Asset ID
  - Creation date
  - Associated fix
  - Connector
  - Scanner detection
  - Risk score
  - Custom fields
  - Etc…


```
{
    "id": 629607,
    "status": "open",
    "closed_at": null,
    "created_at": "2020-11-06T21:18:21Z",
    "due_date": null,
    "notes": null,
    "port": [
        3389
    ],
    "priority": 10,
    "identifiers": [
        "18405"
    ],
    "last_seen_time": "2013-07-01T11:47:23.000Z",
    "scanner_score": 2.0,
    "fix_id": 1770971,
    "scanner_vulnerabilities": [
        {
            "port": 3389,
            "external_unique_id": "18405",
            "open": true
        }
    ],
    "asset_id": 11012,
    "connectors": [
        {
            "id": 156474,
            "name": "Nessus XML",
            "connector_definition_name": "Nessus XML",
            "vendor": "Tenable"
        }
    ],
    "service_ticket": null,
    "urls": {
        "asset": "api.kennasecurity.com/assets/11012"
    },
    "solution": "- Force the use of SSL as a transport layer for
    this service if supported, or/and\n- Select the 'Allow
    connections only from computers running Remote Desktop with
    Network Level Authentication' setting if it is available.",
    "patch": true,
    "patch_published_at": null,
    "cve_id": "CVE-2005-1794",
    "cve_description": "Microsoft Terminal Server using Remote
    Desktop Protocol (RDP) 5.2 stores an RSA private key in
    mstlsapi.dll and uses it to sign a certificate, which allows
```

Fixes Exports

- Each fix that applies to an asset in the environment can be exported
- Fixes are reported uniquely, with the associated assets and vulnerabilities linked
- Data points include
  - Assets
  - Vulnerabilities
  - Diagnosis
  - Solution
  - Reference links
  - Scanner IDs
  - Patch publication date
  - Etc…


```
"fixes": [
    {
        "id": 1770969,
        "diagnosis": "<p>One of several ports that were previously
        open are now closed or unresponsive. <br><br>There are several
        possible reasons for this :<br><br>  - The scan may have
        caused a service to freeze or stop     running.<br><br>  - An
        administrator may have stopped a particular service     during
        the scanning process.<br><br>This might be an availability
        problem related to the following :<br><br>  - A network outage
        has been experienced during the scan,     and the remote
        network cannot be reached anymore by the     scanner.<br><br>
        - This scanner may has been blacklisted by the system
        administrator or by an automatic intrusion detection /
        prevention system that detected the scan.<br><br>  - The
        remote host is now down, either because a user     turned it
        off during the scan or because a select denial     of service
        was effective.<br><br>In any case, the audit of the remote
        host might be incomplete and may need to be done again</p>",
        "consequence": null,
        "solution": "- Increase checks_read_timeout and/or reduce
        max_checks\n\n- Disable any IPS during the Nessus scan",
        "url": null,
        "title": "Open Port Re-check",
        "vendor": null,
        "reference_links": null,
        "exact_match": null,
        "alternates_visible": false,
        "assets": [
            "api.kennasecurity.com/assets/11011",
            "api.kennasecurity.com/assets/11012",
            "api.kennasecurity.com/assets/11013",
            "api.kennasecurity.com/assets/11014",
            "api.kennasecurity.com/assets/11015",
            "api.kennasecurity.com/assets/11016",
            "api.kennasecurity.com/assets/11017"
        ],
        "scanner_ids": [
            "10919"
        ],
        "cves": [],
        "updated_at": "2020-11-06T21:18:02.000Z",
        "patch_publication_date": null,
        "category": null,
        "vuln_count": 7,
        "vulnerabilties": [
            "api.kennasecurity.com/vulnerabilties/629570",
```

Interactive Poll

What type of export would provide a list of the tags found on each asset?

KENNA Security

Demo Time

- Crafting API requests to target data exports
- Using Gzip to unzip output
- How and why to use incremental exports

KENNA Security

Using the API to create data exports

- Data exports are asynchronous so you must run one request to generate an export, and then another to download that export
- Add query parameters to the body of the request to fine-tune your export so that you only grab the data that you need
- Declare your data export type (Asset/Vulnerability/Fix) and file format (XML/Json) in the body of the request

KENNA Security

Using Gzip

- Data exports are condensed into a zipped file format called Gzip
- Gzip utilities are built into Linux/Mac OS, but you may need to install additional software such as 7zip to extract on Windows

KENNA Security

Incremental Exports

- Export file sizes can be huge! Use incremental exports to only download data that has changed or been added since your last export
- Both relative time ranges and literal date/time stamps can be used e.g. (“records_updated_since” : “now-1w”) or (“records_updated_since” : “2021-01-01”)

KENNA Security

Interactive Poll

- Which of these is not a benefit of incremental exports?

KENNA Security

KENNA
Security

Thank you

Katie Kolon, Customer Success Operations Specialist

Jared Kalmus, Customer Success Engineer