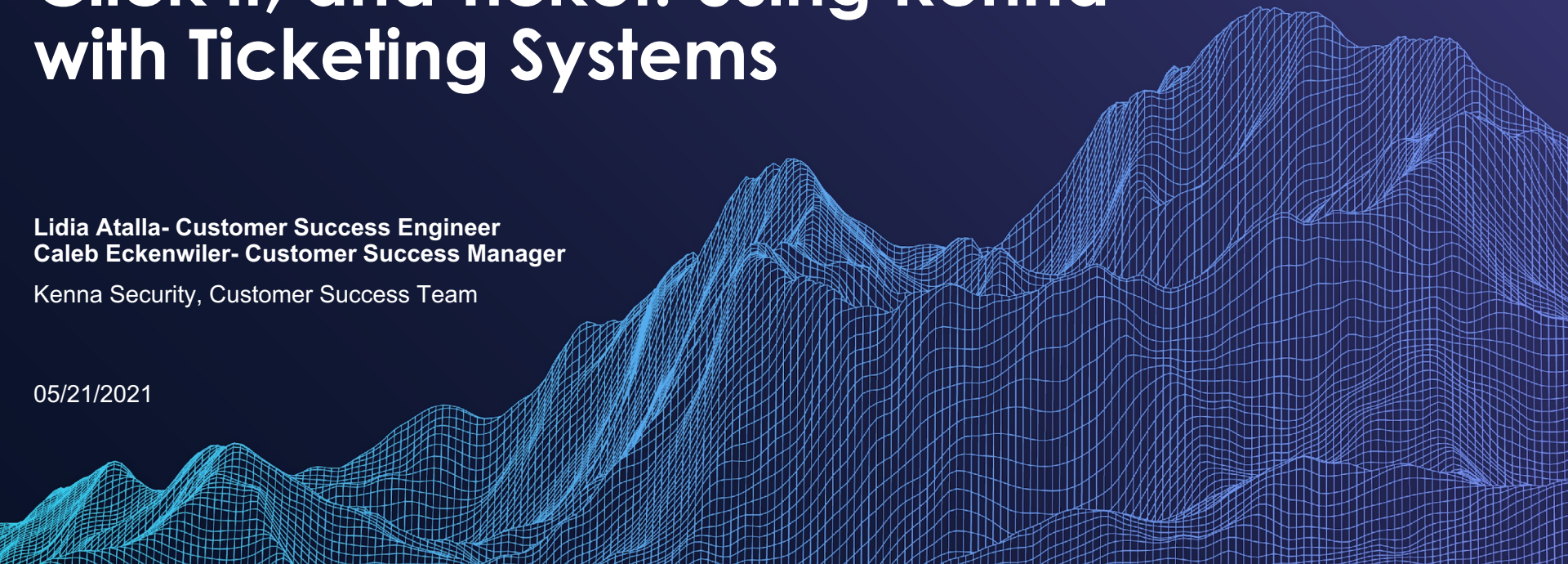KENNA
Security

Click it, and Ticket: Using Kenna with Ticketing Systems

Lidia Atalla- Customer Success Engineer
Caleb Eckenwiler- Customer Success Manager

Kenna Security, Customer Success Team
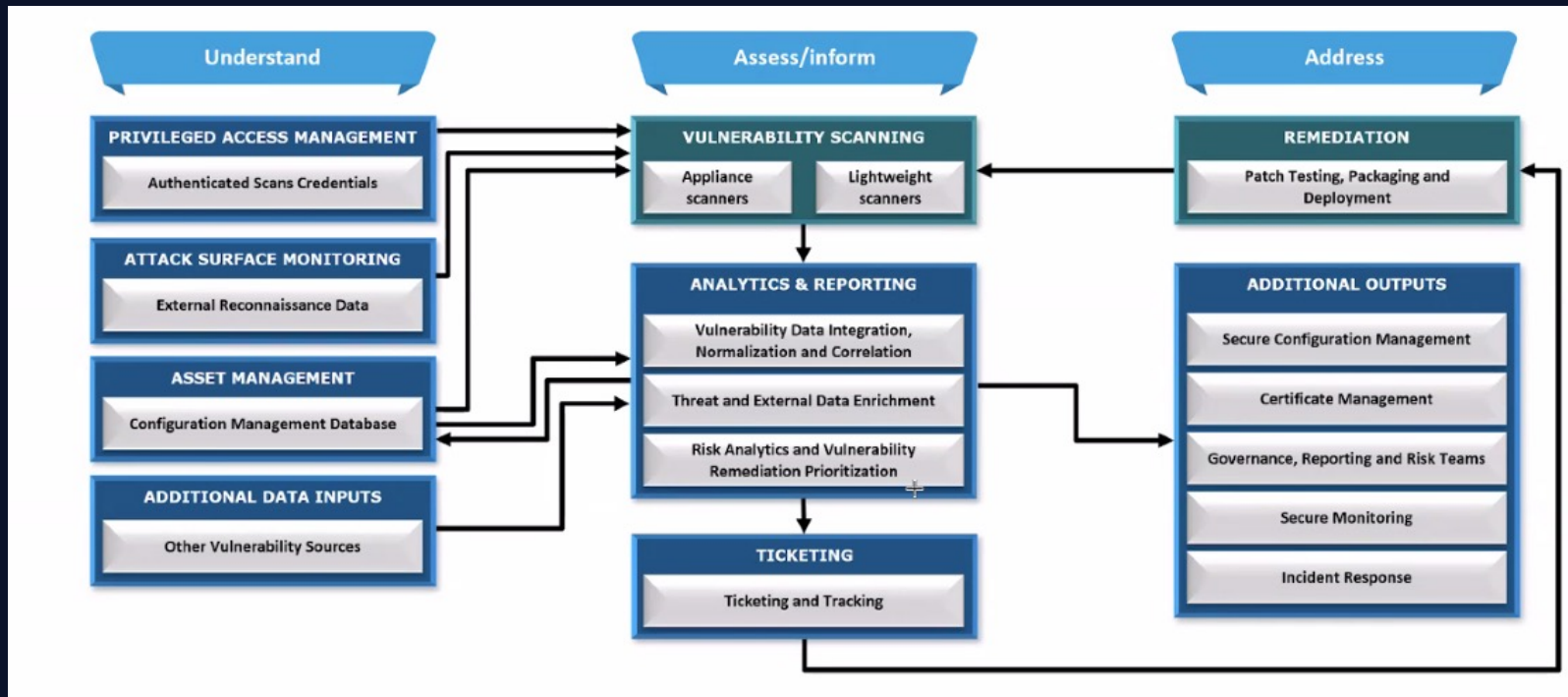
05/21/2021

Using Kenna with Ticketing Systems

Agenda

- Current Ticketing Integrations
  - ServiceNow
  - JIRA
  - Chewell
  - Remedy

- Ticketing Workflow

- Automation Examples and Discussion

KENNA
Security

Interactive Poll

What ticketing system(s) do you currently use? And/or are of interest to you today?

KENNA
Security

Standard Vulnerability Management Flow

Understand

PRIVILEGED ACCESS MANAGEMENT
- Authenticated Scans Credentials

ATTACK SURFACE MONITORING
- External Reconnaissance Data

ASSET MANAGEMENT
- Configuration Management Database

ADDITIONAL DATA INPUTS
- Other Vulnerability Sources

Assess/inform

VULNERABILITY SCANNING
- Appliance scanners
- Lightweight scanners

ANALYTICS & REPORTING
- Vulnerability Data Integration, Normalization and Correlation
- Threat and External Data Enrichment
- Risk Analytics and Vulnerability Remediation Prioritization

TICKETING
- Ticketing and Tracking

Address

REMEDIATION
- Patch Testing, Packaging and Deployment

ADDITIONAL OUTPUTS
- Secure Configuration Management
- Certificate Management
- Governance, Reporting and Risk Teams
- Secure Monitoring
- Incident Response

KENNA
Security

Intros to Ticketing

- Within Vulnerability Management, in order to patch an item, teams need to know what the asset affected is and what patch to apply (OS dependencies, version dependencies, etc.). An easy way to track general information as well as progress on open items is to leverage ticketing integrations.

- Create workflows for teams accountable for mitigating vulns, and establish a central repository for remediation information.

- Define Ticketing workflows in SOPs in order to inform teams where they need to go to remediate vulnerabilities.

- Document the workflow policies for client audits and regulators with respect to vulnerability management.

- In most if not all cases, the organization can define their own workflows. As long as the workflows are rigorous and clearly defined, there should be no issues with the remediation piece of the overall VM program.

ACCOUNTABILITY

Straight Ahead

KENNA
Security

# Value of Ticketing: Who, What, When, Where?

- Tracking for historical reference: Did we patch that vulnerability? Was it ever ticketed? Etc.

- Central repository for remediation workflow: Where do I go to look for my next remediation task?

- Who is assigned? We can track this via the assignment group & Assignee information.

- Where does the patch need to be applied? All information is held within the ticket.
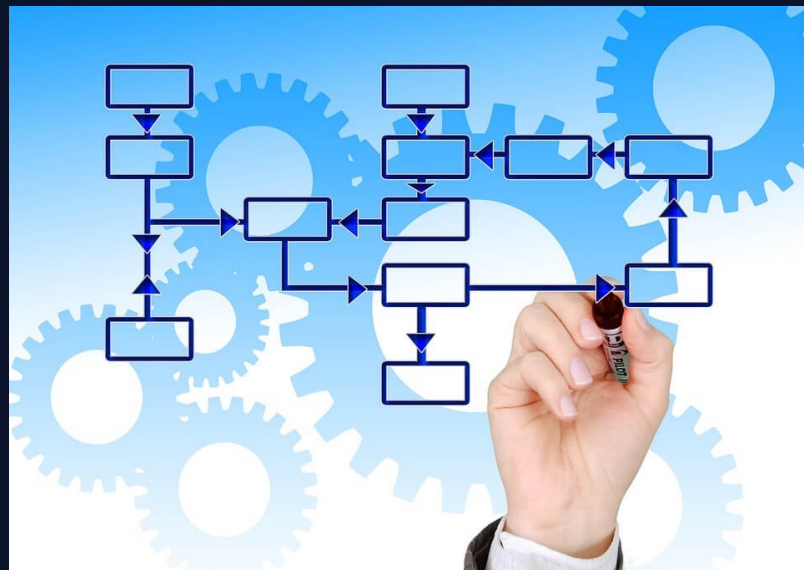
KENNA
Security

Ticketing Connections:

- Kenna Supports several Ticketing connectors out of the box:
  - ServiceNow
  - JIRA
  - Cherwell
  - BMC Remedy (specific versions)\

- Some organizations have used the Kenna API to extract data and create tickets if their system is not supported OOTB.

Connectors

Ticketing

Jira Software   bmc Remedy Ticketing   cherwell   servicenow Ticketing

KENNA
Security
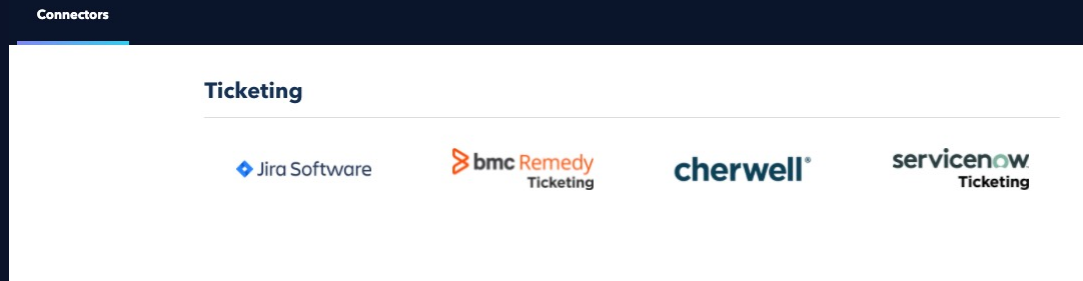
Ticketing Systems: ServiceNow

- For ServiceNow there are some requirements to set up the connector. The service account/user must have ITIL permissions and access to the table you wish to leverage.
  - Custom tables can be used

- By default we point towards the Incident table but this can be changed to any of the following pre-existing tables:
  - Problem
  - Request
  - Incident

- In order to leverage a custom table, we will need you to provide the custom table name information to us.

- Kenna also has a set of fields that we offer to push to ServiceNow tickets. If you would like to use pre-set fields, you can do so, and items will be "greyed-out" within Kenna and unavailable for edit during ticket creation.

- ServiceNow is a bi-directional Connector.

- Kenna Help Page Title: ServiceNow Ticketing Integration.

ServiceNow Connector

Incident Number	INC0366599
Assigned To	Kenneth Dennis
State	In Progress

View Incident

servicenow

KENNA
Security

Ticketing Systems: JIRA

External ID: ████████-108338
Status: Waiting for IT

- For JIRA there are some requirements to set up the connector. The service account/user must have access to the projects you wish to ticket.

- JIRA is a bi-directional Connector. We will bring back:
  - The ticket owner
  - The ticket status
  - The ticket number (REM-001 for example)
  - Direct link to the ticket

- Kenna Help Page Title: Jira Ticketing Integration.

Jira Software

KENNA
Security

Demo Time

KENNA
Security

Ticketing Systems: Cherwell

- To set up the Cherwell connector, you will need to follow the information on the Kenna Help Page (title provided below).

- You will also need information about your Business Object Schema from Cherwell.

- Cherwell is a bi-directional Connector.

- Kenna Help Page Title: Cherwell Ticketing Connector.

External ID:
94656efcd3af96c042114f473da9d

Status: New

Cherwell

KENNA
Security

Ticketing Systems: BMC Remedy (specific versions)

External ID:
INC000004097739
Status: Closed

- To set up the Remedy connector, please reach out to Kenna Support to determine if the version of Remedy you are leveraging is supported.

- BMC is a bi-directional Connector.

bmc Remedy

K≡NNA
Security

Tracking Tickets

- Each Ticket created via a ticketing integration in Kenna is tracked via bi-directional communication.

- We have the ability to view 2 date based ticket statuses:

  - On time

  - Overdue

  - For items "In-Progress" we will simply look at the due date and depending on that information, it will drop into the relevant on-time or overdue bucket.

- This graph is on the Home page, and will only appear if you have a ticketing integration set up within Kenna.

KENNA
Security