Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

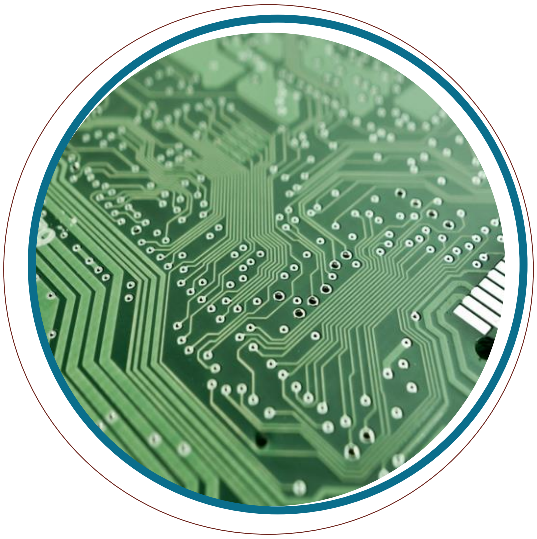
November 2024

Module 6

Advanced Hunting

Module 5 Contents:

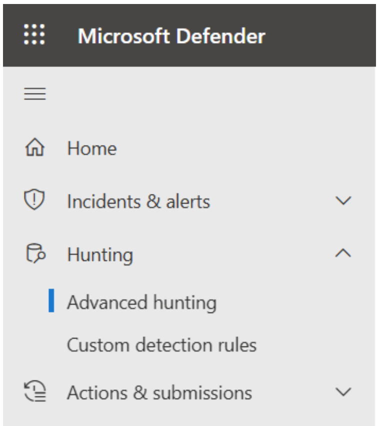
- **Advanced Hunting**
- **Kusto Query Language**
  - General
  - Data flow pipeline
  - Statements
  - Useful Links



Advanced Hunting

Advanced Hunting

' … is a query-based threat hunting tool … '

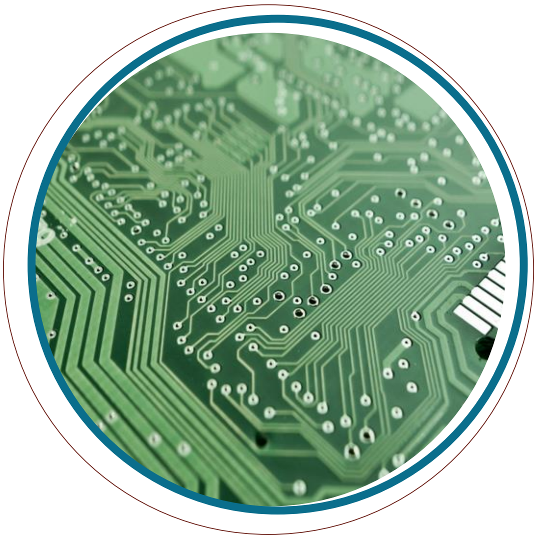


- Modes
  - guided
  - advanced
- Data freshness
  - Event and activity date (alerts, security events, …)
    - immediately
  - Entity data
    - up to 24 hours

Advanced Hunting

- Schema - Tables
  - from multiple Defender Sources
  - Description in documentation
- Queries
  - could be saved query or function
  - added to schema for all administrators
- Result used
  - for investigation
  - Take actions
  - Detection rules

Source: https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-client



Kuste Query Language

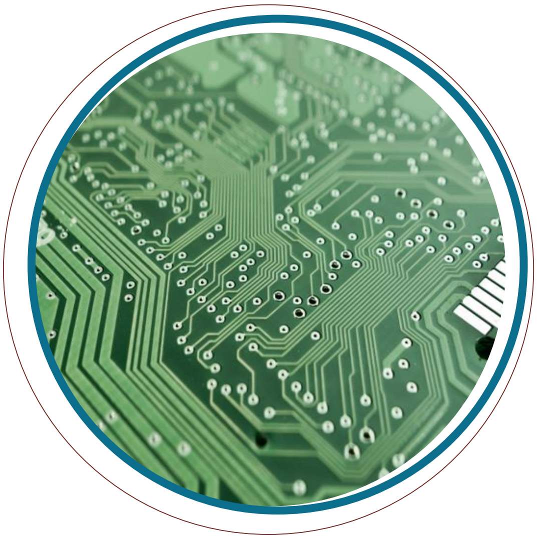
General

General

Some rules for KQL

- Case sensitivity
  - Tablenames
  - Fieldnames
  - Operators
  - Functions
- Comments: //
- Line breaks: before |
- Time: always saved as UTC

Source: https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-client



Data Flow pipeline

Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

Data Flow Pipeline

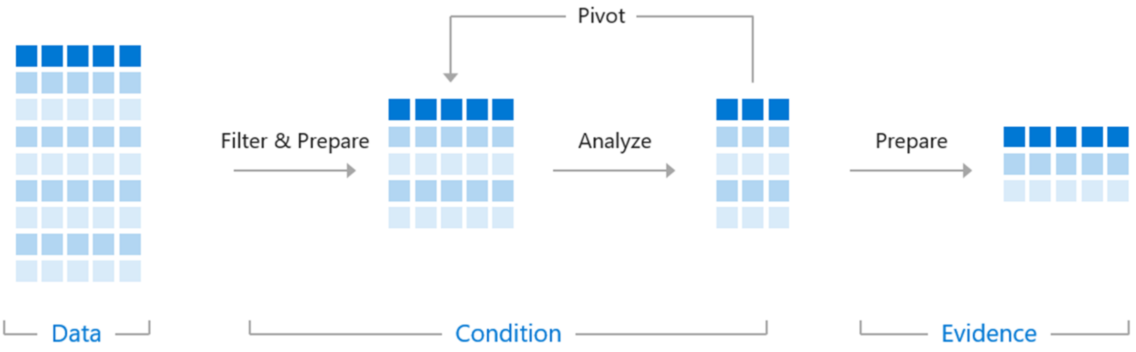
Overview

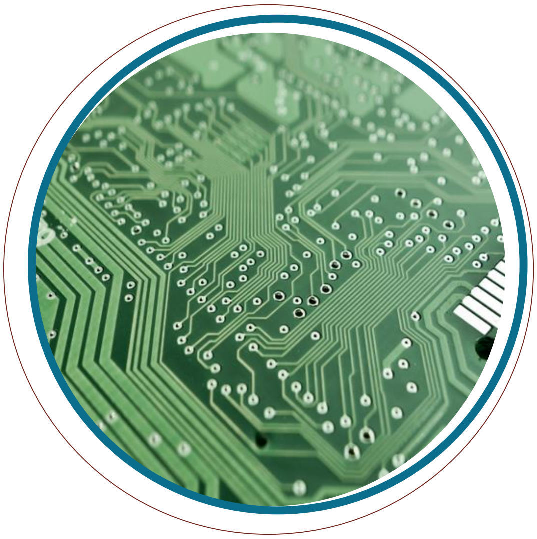
- Each statement starts with either a
  - Table
  - Variable(s) declaration(s)
  - Functions with result type table
- Variable declaration must end with ;
- Use | to pass data from table to operator
  - Multiple | are possible

Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

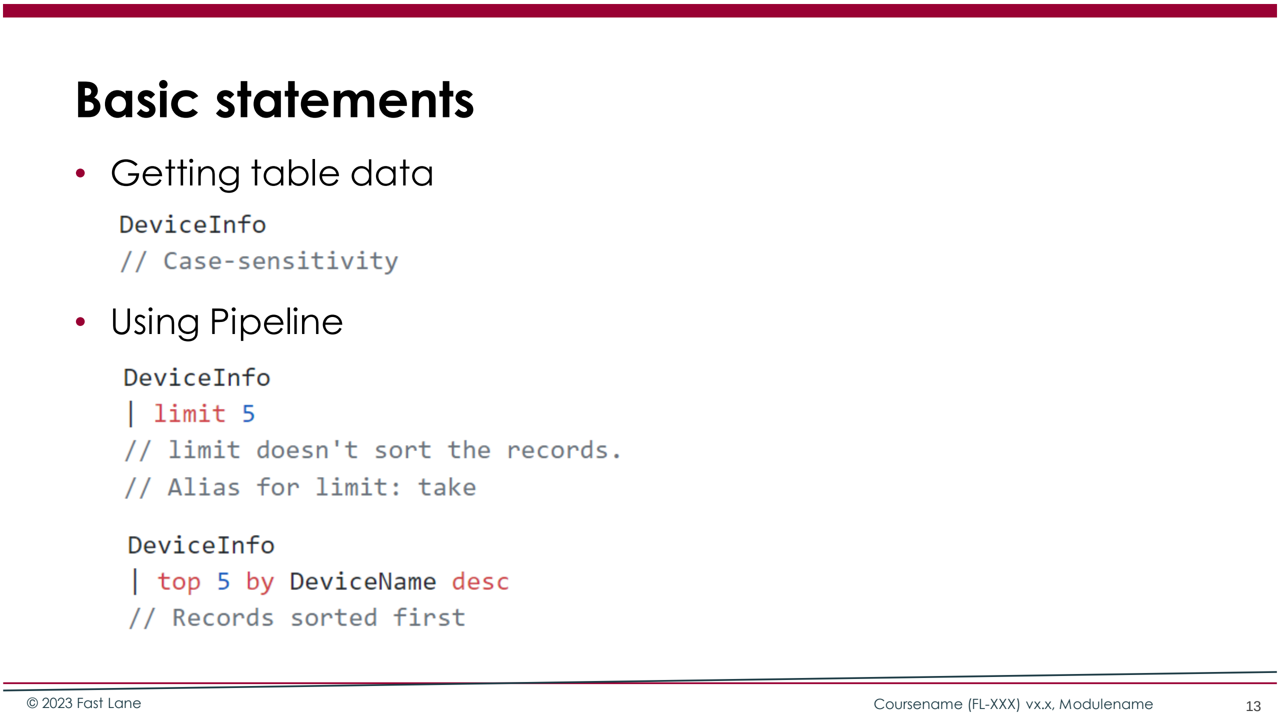
Data Flow Pipeline

```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```





Basic statements



Basic statements

- Getting table data

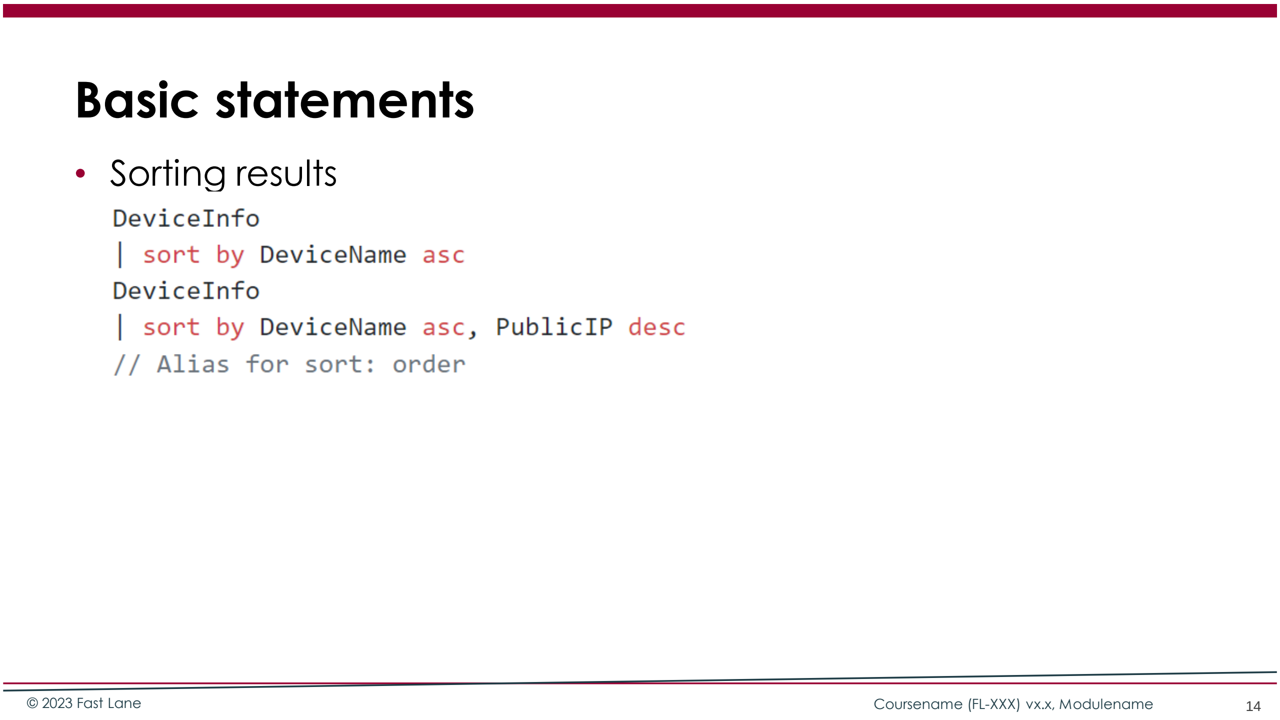
```
DeviceInfo
// Case-sensitivity
```

- Using Pipeline

```
DeviceInfo
| limit 5
// limit doesn't sort the records.
// Alias for limit: take
```

```
DeviceInfo
| top 5 by DeviceName desc
// Records sorted first
```

13

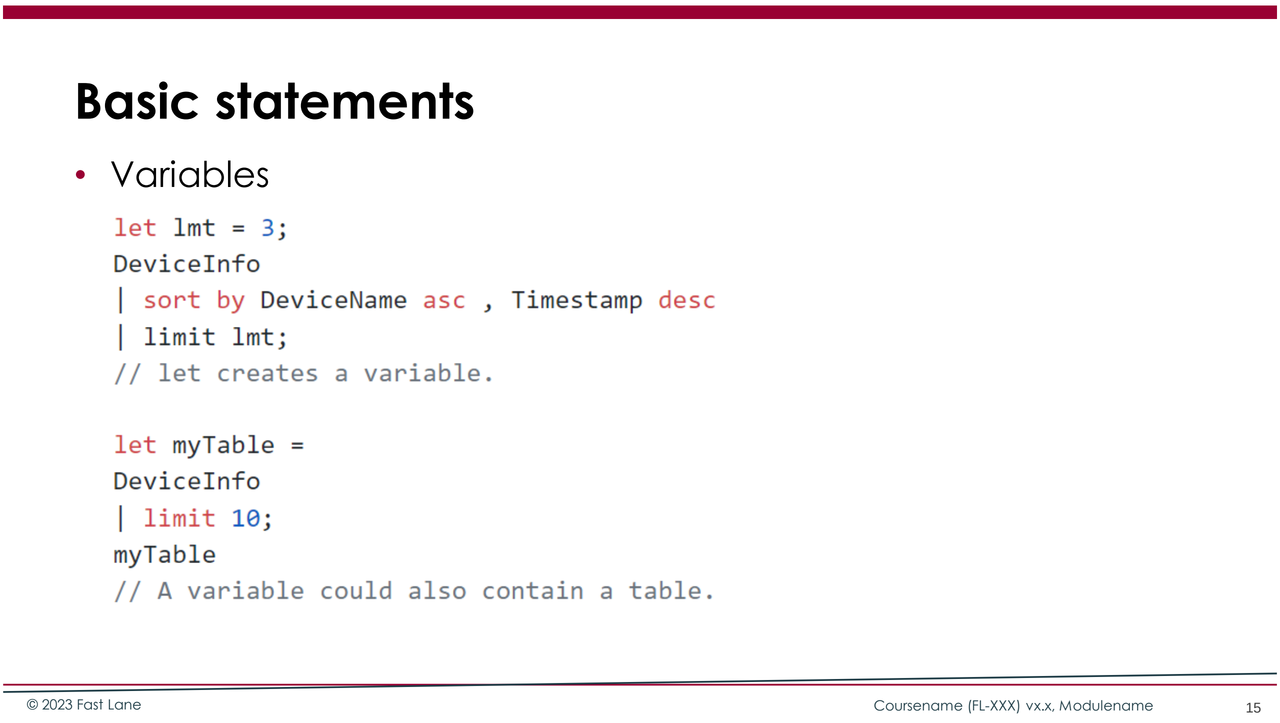


Basic statements

- Sorting results

```
DeviceInfo
| sort by DeviceName asc
DeviceInfo
| sort by DeviceName asc, PublicIP desc
// Alias for sort: order
```

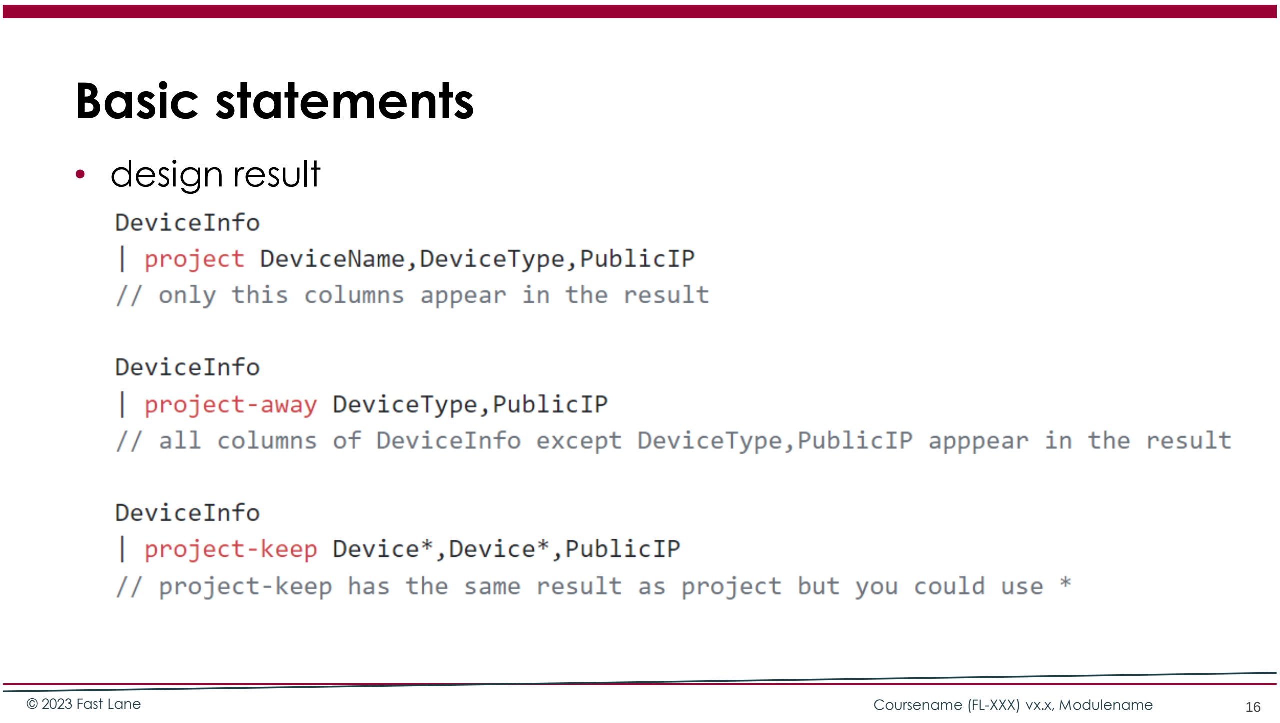
14



Basic statements

- Variables

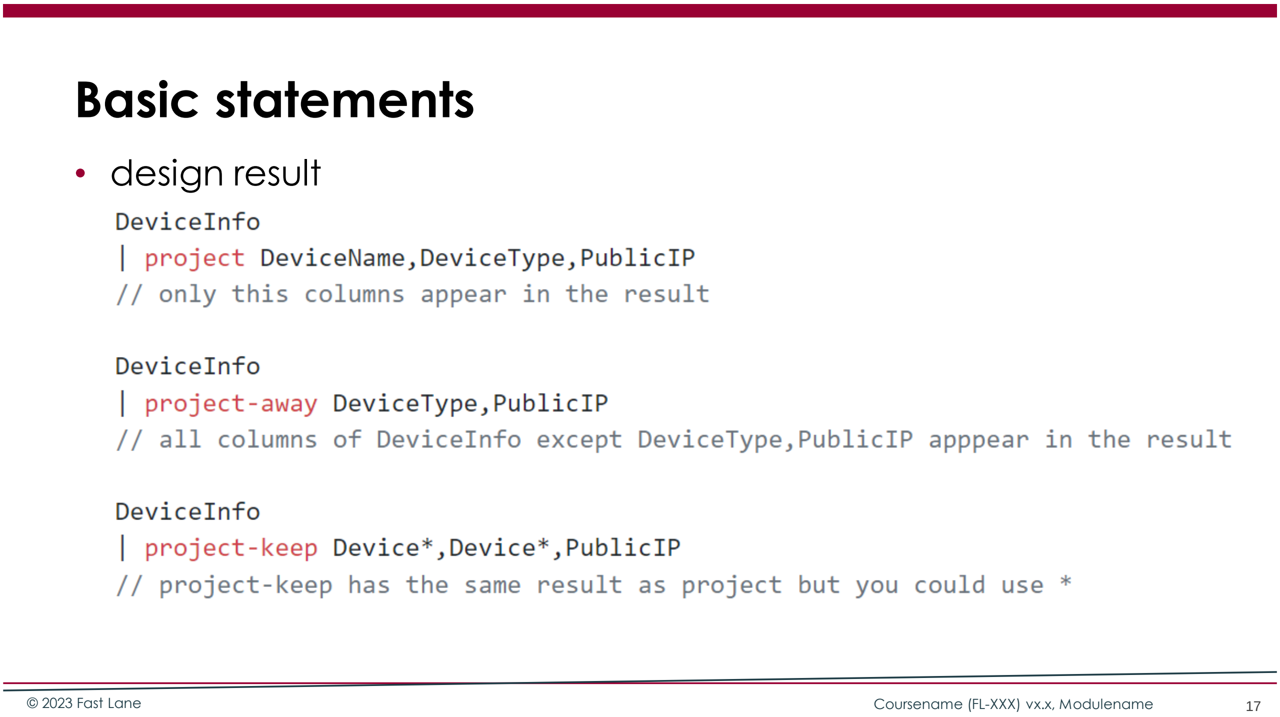
```
let lmt = 3;
DeviceInfo
| sort by DeviceName asc , Timestamp desc
| limit lmt;
// let creates a variable.

let myTable =
DeviceInfo
| limit 10;
myTable
// A variable could also contain a table.
```



Basic statements

- design result

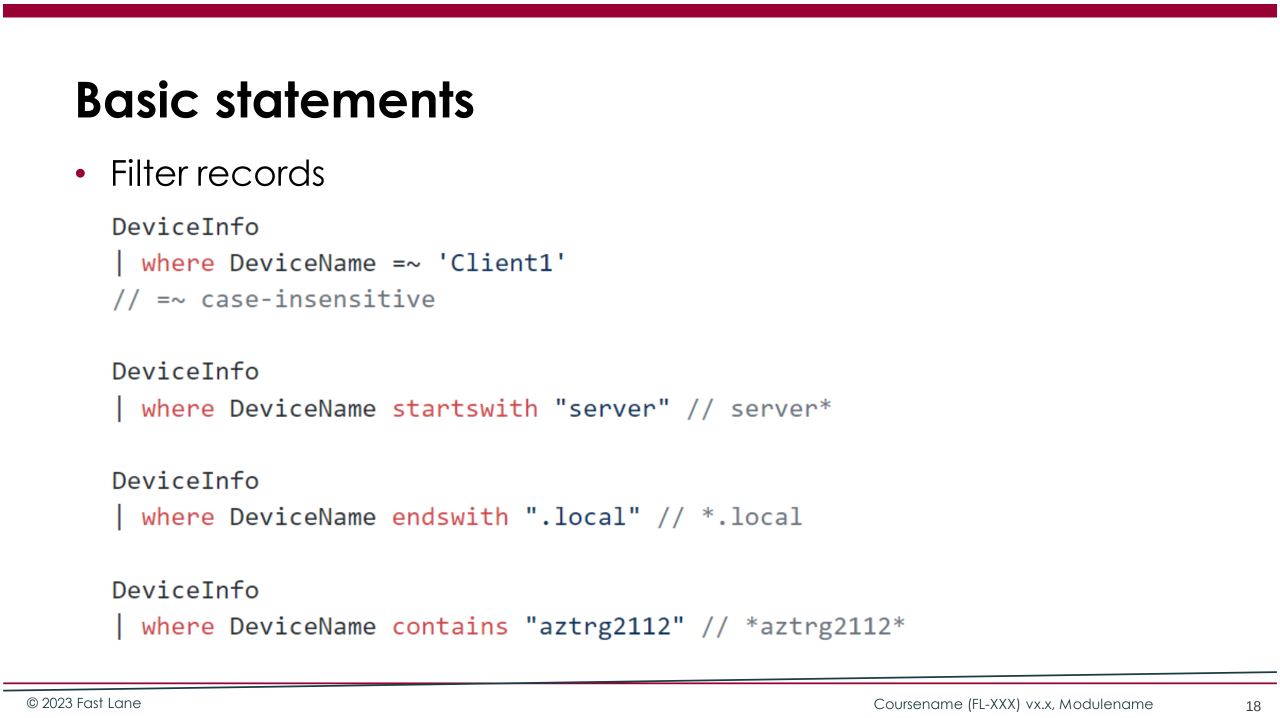
```
DeviceInfo
| project DeviceName,DeviceType,PublicIP
// only this columns appear in the result

DeviceInfo
| project-away DeviceType,PublicIP
// all columns of DeviceInfo except DeviceType,PublicIP apppear in the result

DeviceInfo
| project-keep Device*,Device*,PublicIP
// project-keep has the same result as project but you could use *
```



Basic statements

- design result

```
DeviceInfo
| project DeviceName,DeviceType,PublicIP
// only this columns appear in the result

DeviceInfo
| project-away DeviceType,PublicIP
// all columns of DeviceInfo except DeviceType,PublicIP apppear in the result

DeviceInfo
| project-keep Device*,Device*,PublicIP
// project-keep has the same result as project but you could use *
```



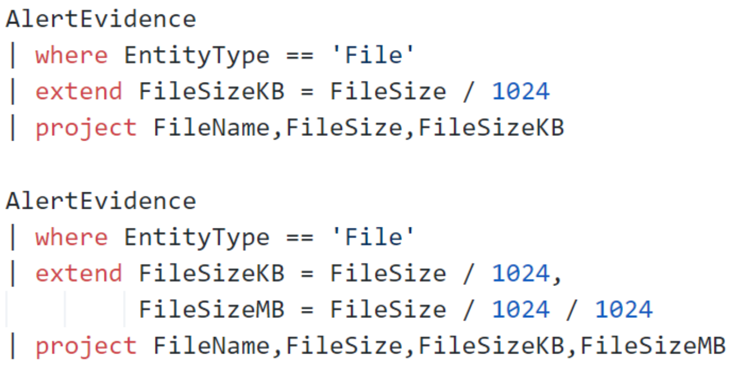
Basic statements

- Filter records

```
DeviceInfo
| where DeviceName =~ 'Client1'
// =~ case-insensitive

DeviceInfo
| where DeviceName startswith "server" // server*

DeviceInfo
| where DeviceName endswith ".local" // *.local

DeviceInfo
| where DeviceName contains "aztrg2112" // *aztrg2112*
```

Basic statements

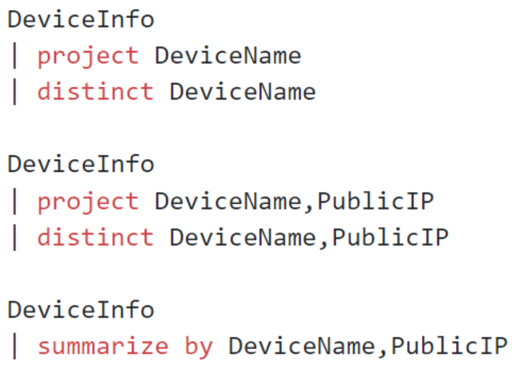
- Extends result



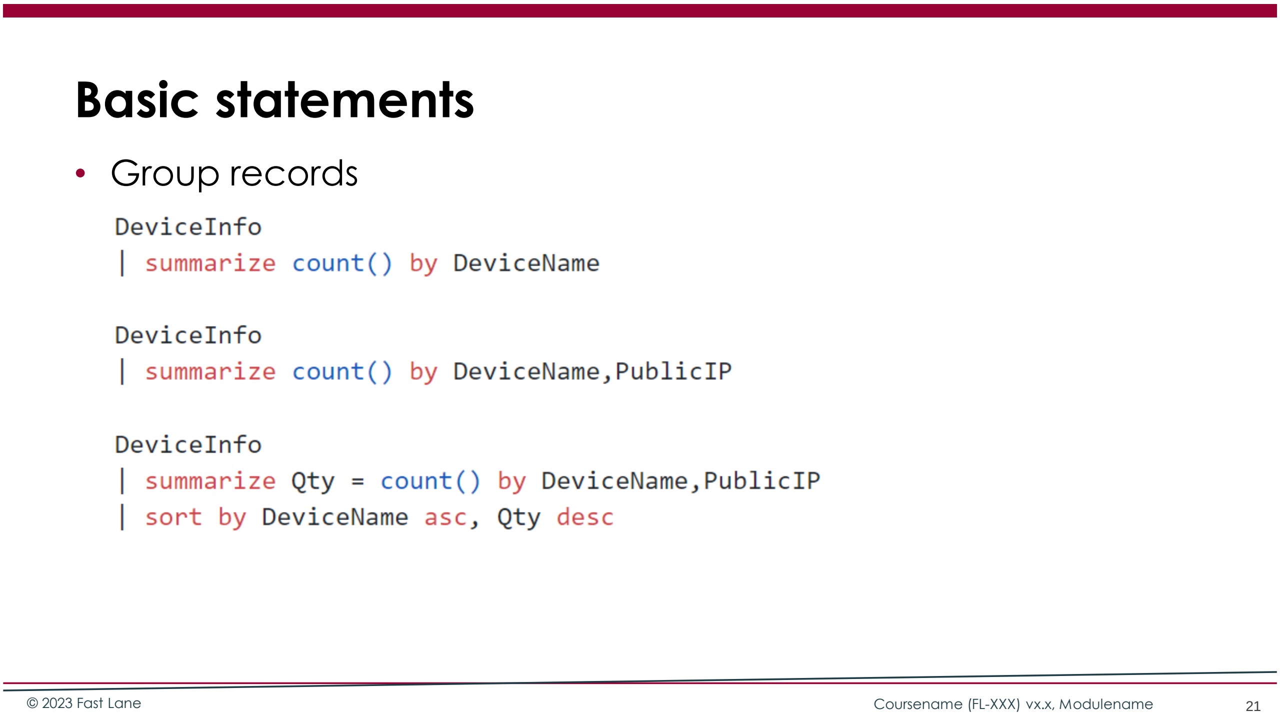
```
AlertEvidence
| where EntityType == 'File'
| extend FileSizeKB = FileSize / 1024
| project FileName,FileSize,FileSizeKB

AlertEvidence
| where EntityType == 'File'
| extend FileSizeKB = FileSize / 1024,
         FileSizeMB = FileSize / 1024 / 1024
| project FileName,FileSize,FileSizeKB,FileSizeMB
```

Basic statements

- Remove duplicates



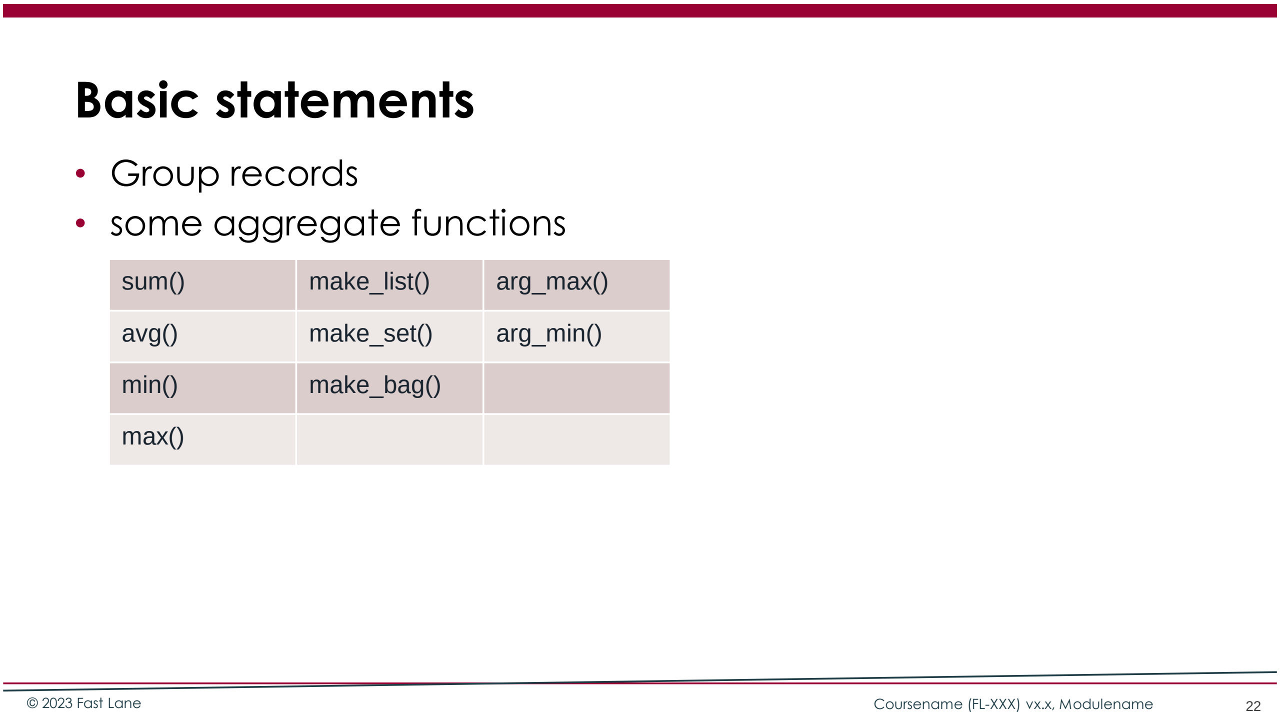
```
DeviceInfo
| project DeviceName
| distinct DeviceName

DeviceInfo
| project DeviceName,PublicIP
| distinct DeviceName,PublicIP

DeviceInfo
| summarize by DeviceName,PublicIP
```



Basic statements

- Group records

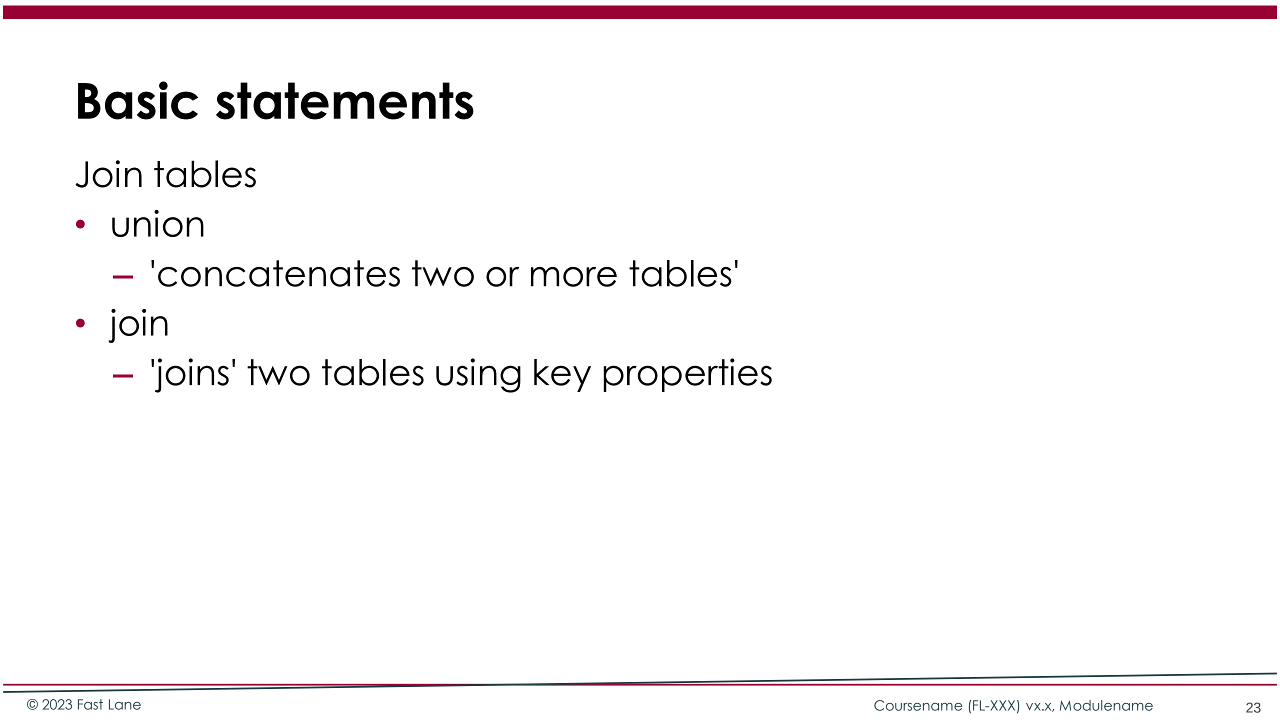
```
DeviceInfo
| summarize count() by DeviceName

DeviceInfo
| summarize count() by DeviceName,PublicIP

DeviceInfo
| summarize Qty = count() by DeviceName,PublicIP
| sort by DeviceName asc, Qty desc
```



Basic statements

- Group records
- some aggregate functions

sum()	make_list()	arg_max()
avg()	make_set()	arg_min()
min()	make_bag()	
max()		

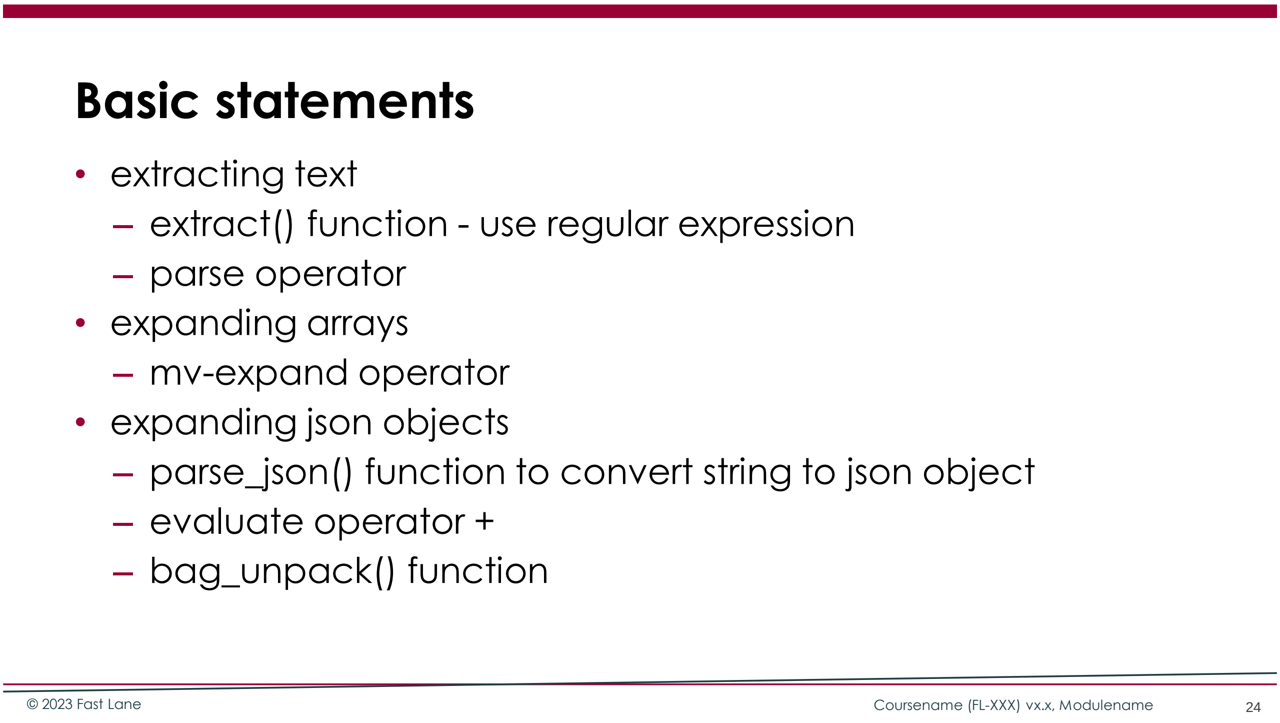


Basic statements

Join tables

- union
  - 'concatenates two or more tables'
- join
  - 'joins' two tables using key properties

23



Basic statements

- extracting text
  - extract() function - use regular expression
  - parse operator
- expanding arrays
  - mv-expand operator
- expanding json objects
  - parse_json() function to convert string to json object
  - evaluate operator +
  - bag_unpack() function

24

Try to read the query

End of Module 6