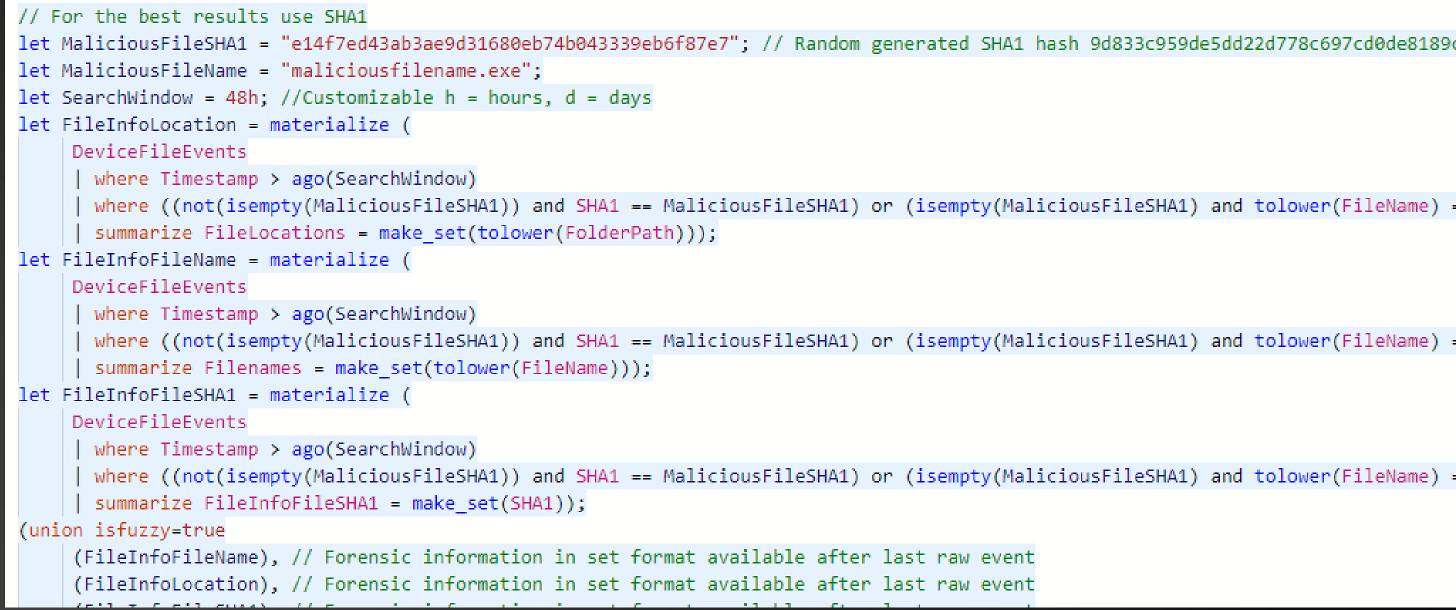


```
// For the best results use SHA1
let MaliciousFileSHA1 = "e14f7ed43ab3ae9d31680eb74b043339eb6f87e7"; // Random generated SHA1 hash 9d833c959de5dd22d778c697cd0de8189
let MaliciousFileName = "maliciousfilename.exe";
let SearchWindow = 48h; //Customizable h = hours, d = days
let FileInfoLocation = materialize (
     DeviceFileEvents
     | where Timestamp > ago(SearchWindow)
     | where ((not(isempty(MaliciousFileSHA1)) and SHA1 == MaliciousFileSHA1) or (isempty(MaliciousFileSHA1) and tolower(FileName) =
     | summarize FileLocations = make_set(tolower(FolderPath)));
let FileInfoFileName = materialize (
     DeviceFileEvents
     | where Timestamp > ago(SearchWindow)
     | where ((not(isempty(MaliciousFileSHA1)) and SHA1 == MaliciousFileSHA1) or (isempty(MaliciousFileSHA1) and tolower(FileName) =
     | summarize Filenames = make_set(tolower(FileName)));
let FileInfoFileSHA1 = materialize (
     DeviceFileEvents
     | where Timestamp > ago(SearchWindow)
     | where ((not(isempty(MaliciousFileSHA1)) and SHA1 == MaliciousFileSHA1) or (isempty(MaliciousFileSHA1) and tolower(FileName) =
     | summarize FileInfoFileSHA1 = make_set(SHA1));
(union isfuzzy=true
     (FileInfoFileName), // Forensic information in set format available after last raw event
     (FileInfoLocation), // Forensic information in set format available after last raw event
```

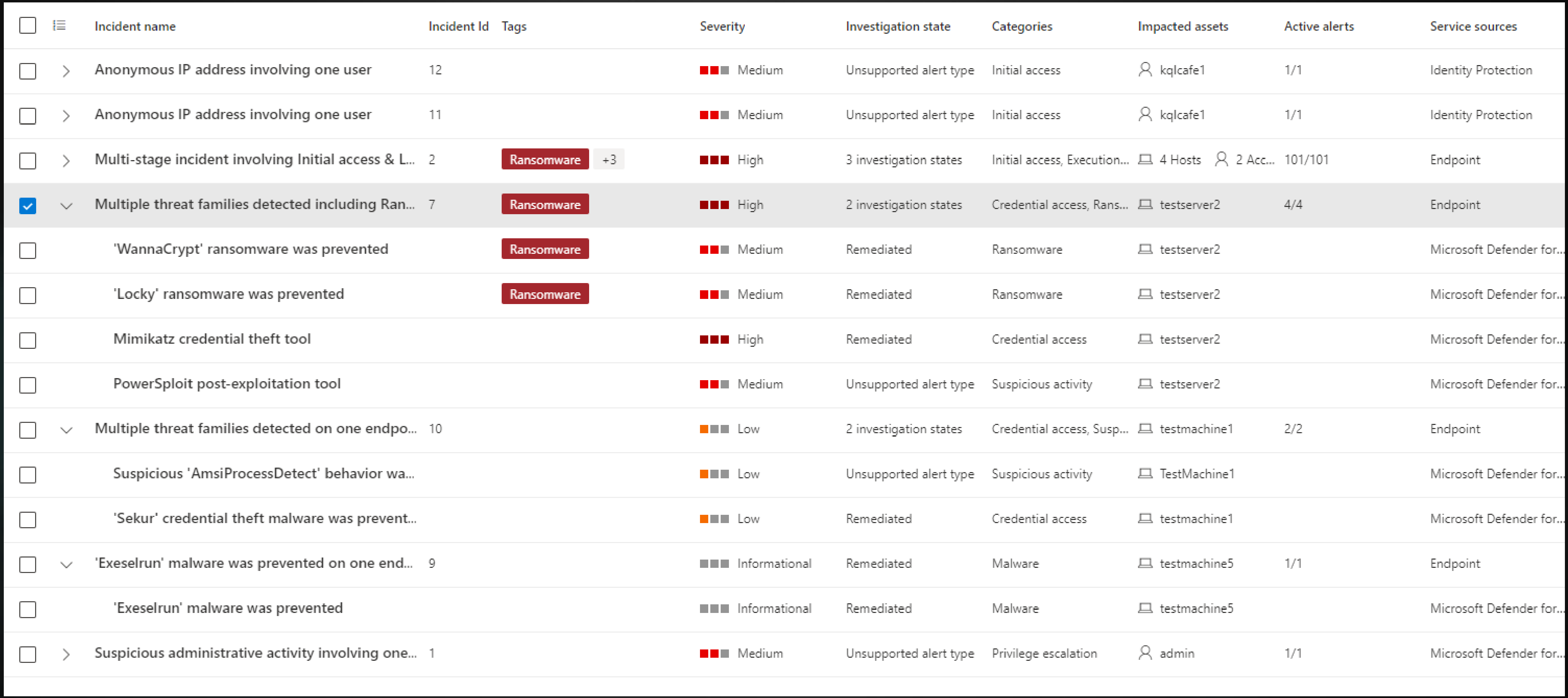
KQL DFIR

KQL CAFE | NOVEMBER 29, 2022

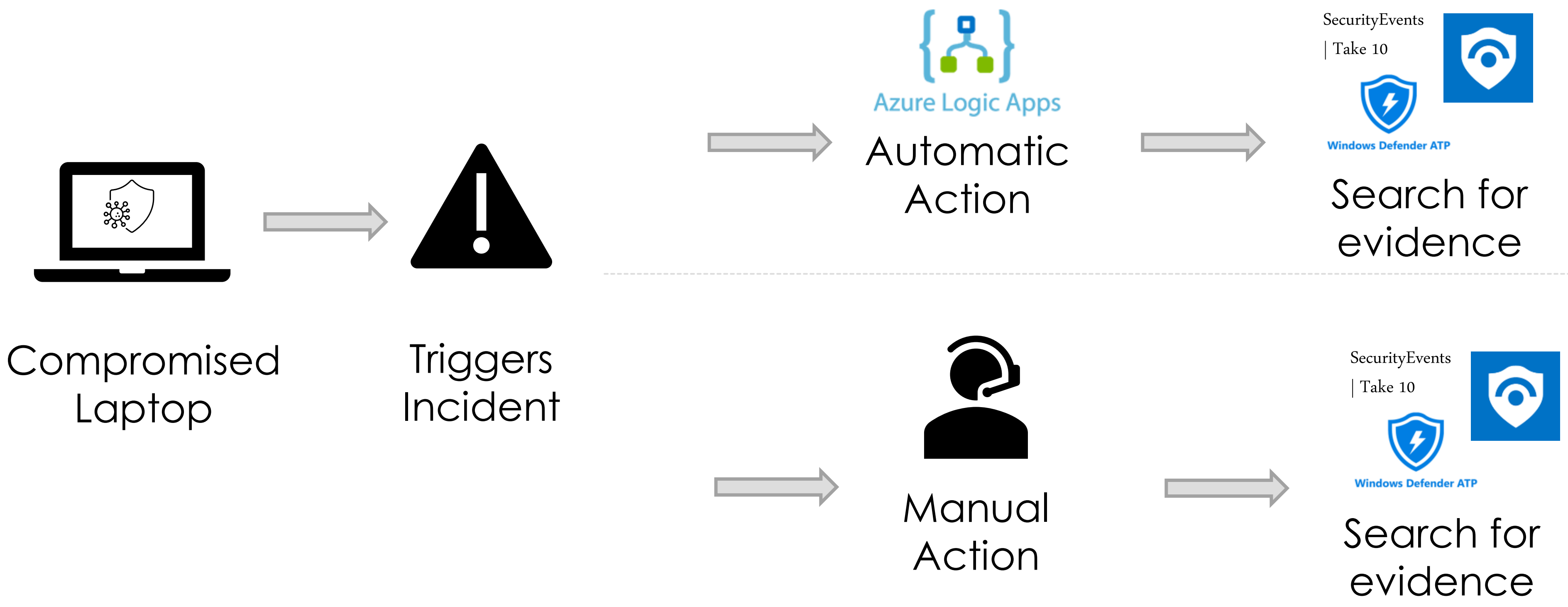
TWITTER: @**BERTJANCYBER**

GITHUB: GITHUB.COM/BERT-JANP

Starting point: Incidents



□		Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources
□	›	Anonymous IP address involving one user	12		■■■ Medium	Unsupported alert type	Initial access	kqlcafe1	1/1	Identity Protection
□	›	Anonymous IP address involving one user	11		■■■ Medium	Unsupported alert type	Initial access	kqlcafe1	1/1	Identity Protection
□	›	Multi-stage incident involving Initial access & L...	2	Ransomware +3	■■■ High	3 investigation states	Initial access, Execution...	4 Hosts 2 Acc...	101/101	Endpoint
☑	⌄	Multiple threat families detected including Ran...	7	Ransomware	■■■ High	2 investigation states	Credential access, Rans...	testserver2	4/4	Endpoint
□		'WannaCrypt' ransomware was prevented		Ransomware	■■■ Medium	Remediated	Ransomware	testserver2		Microsoft Defender for...
□		'Locky' ransomware was prevented		Ransomware	■■■ Medium	Remediated	Ransomware	testserver2		Microsoft Defender for...
□		Mimikatz credential theft tool			■■■ High	Remediated	Credential access	testserver2		Microsoft Defender for...
□		PowerSploit post-exploitation tool			■■■ Medium	Unsupported alert type	Suspicious activity	testserver2		Microsoft Defender for...
□	⌄	Multiple threat families detected on one endpo...	10		■■■ Low	2 investigation states	Credential access, Susp...	testmachine1	2/2	Endpoint
□		Suspicious 'AmsiProcessDetect' behavior wa...			■■■ Low	Unsupported alert type	Suspicious activity	TestMachine1		Microsoft Defender for...
□		'Sekur' credential theft malware was prevent...			■■■ Low	Remediated	Credential access	testmachine1		Microsoft Defender for...
□	⌄	'Exeselrun' malware was prevented on one end...	9		■■■ Informational	Remediated	Malware	testmachine5	1/1	Endpoint
□		'Exeselrun' malware was prevented			■■■ Informational	Remediated	Malware	testmachine5		Microsoft Defender for...
□	›	Suspicious administrative activity involving one...	1		■■■ Medium	Unsupported alert type	Privilege escalation	admin	1/1	Microsoft Defender for...



Compromised Laptop

Triggers Incident

Automatic Action

Search for evidence

Manual Action

Search for evidence

Goal of the IR queries

- Enrich Incidents
  - Easier decision making
- Find related (malicious) activities
  - IOCs
  - Input for additional investigations

Taking a step back

- ✓ Get to know your data sources
  - ✓ Summarize: count(), dcount(), make_set()
  - ✓ Build in KQL functions: base64_decode_tostring()
- ✓ Prepare for Incident Response cases
  - ✓ What information do I want to collect when an incident is triggered?
  - ✓ Build queries before incidents take place (yourself or community queries)
  - ✓ Validate the quality of the queries
  - ✓ Automate if possible

- Ref: https://techcommunity.microsoft.com/t5/microsoft-security-experts/leveraging-the-power-of-kql-in-incident-response/ba-p/3044795