

# Certified CyberDefender Cheat Sheet [IR]

This cheat sheet is for CCD students who are getting ready for the exam.

---

## Elastic Common Schema (ECS)

Field	Description	KQL Examples
event.category	It looks for similar events from various data sources that can be grouped together for viewing or analysis.	<ul style="list-style-type: none"><li>• event.category: authentication</li><li>• event.category: process</li><li>• event.category: network</li><li>• event.category: (malware or intrusion_detection)</li></ul>
event.type	It serves as a sub-categorization that, when combined with the "event.category" field, allows for filtering events to a specific level	<ul style="list-style-type: none"><li>• event.type: start</li><li>• event.type: creation</li><li>• event.type: access</li><li>• event.type: deletion</li></ul>
event.outcome	It indicates whether the event represents a successful or a failed outcome	<ul style="list-style-type: none"><li>• event.outcome: success</li><li>• event.outcome : failure</li></ul>

## Common search fields

Field	KQL Examples	Output
<ul style="list-style-type: none"><li>• @timestamp</li></ul>	<ul style="list-style-type: none"><li>• @timestamp: 2023-01-26</li><li>• @timestamp &lt;= "2023-01-25"</li><li>• @timestamp &gt;= "2023-01-26" and</li><li>• @timestamp &lt; = "2023-01-27"</li></ul>	<ul style="list-style-type: none"><li>• Events that happened in 26th</li><li>• Events that happened with a date less than or equal to 25th of Jan</li><li>• Events that happened between 26th and the 27th of Jan</li></ul>
<ul style="list-style-type: none"><li>• agent.name</li></ul>	<ul style="list-style-type: none"><li>• agent.name : DESKTOP-*</li></ul>	<ul style="list-style-type: none"><li>• Look for events from the agent name that starts with DESKTOP</li></ul>
<ul style="list-style-type: none"><li>• message</li></ul>	<ul style="list-style-type: none"><li>• message : powershell</li></ul>	<ul style="list-style-type: none"><li>• Look for any message with the word powershell</li></ul>

## Process related fields

Field	KQL Examples	Output
<ul style="list-style-type: none"><li>• process.name</li></ul>	<ul style="list-style-type: none"><li>• event.category: process and process.name: powershell.exe</li></ul>	<ul style="list-style-type: none"><li>• Look for powershell.exe as a process</li></ul>
<ul style="list-style-type: none"><li>• process.command_line</li></ul>	<ul style="list-style-type: none"><li>• event.category: process and process.command_line.text : *whoami*</li></ul>	<ul style="list-style-type: none"><li>• Look for a commandline that has whoami on it</li></ul>
<ul style="list-style-type: none"><li>• process.pid</li></ul>	<ul style="list-style-type: none"><li>• event.category: process and process.pid : 6360</li></ul>	<ul style="list-style-type: none"><li>• Look for process id: 6360</li></ul>
<ul style="list-style-type: none"><li>• process.parent.name</li></ul>	<ul style="list-style-type: none"><li>• event.category: process and process.parent.name: cmd.exe</li></ul>	<ul style="list-style-type: none"><li>• Looks for cmd.exe as a parent process</li></ul>
<ul style="list-style-type: none"><li>• process.parent.pid</li></ul>	<ul style="list-style-type: none"><li>• host.name : DESKTOP-* and event.category: process and process.command_line.text: powershell and process.parent.pid: 12620</li></ul>	<ul style="list-style-type: none"><li>• Looks for a process command line that has powershell and the parent process id is 12620 on a hostname that starts with DESKTOP</li></ul>

## Network related fields

Field	KQL Examples	Output
<ul style="list-style-type: none"><li>source.ip</li></ul>	<ul style="list-style-type: none"><li>source.ip: 127.0.0.1</li></ul>	<ul style="list-style-type: none"><li>Looks for any logs</li><li>originated from the</li><li>loopback IP address</li><li></li></ul>
<ul style="list-style-type: none"><li>destination.ip</li></ul>	<ul style="list-style-type: none"><li>destination.ip: 23.194.192.66</li></ul>	<ul style="list-style-type: none"><li>Looks for any logs</li><li>originating to IP</li><li>23.194.192.66</li><li></li></ul>
<ul style="list-style-type: none"><li>destination.port</li></ul>	<ul style="list-style-type: none"><li>destination.port: 443</li></ul>	<ul style="list-style-type: none"><li>Looks for any logs</li><li>originating towards port</li><li>443</li><li></li></ul>
<ul style="list-style-type: none"><li>dns.question.name</li></ul>	<ul style="list-style-type: none"><li>dns.question.name: "www.youtube.com"</li></ul>	<ul style="list-style-type: none"><li>Look for any DNS resolution towards www.youtube.com</li></ul>
<ul style="list-style-type: none"><li>dns.response_code</li></ul>	<ul style="list-style-type: none"><li>dns.response_code: "NXDOMAIN"</li></ul>	<ul style="list-style-type: none"><li>Looks for DNS traffic towards non existing domain names</li></ul>
<ul style="list-style-type: none"><li>destination.geo.country_name</li></ul>	<ul style="list-style-type: none"><li>destination.geo.country_name : "Canada"</li></ul>	<ul style="list-style-type: none"><li>Looks for any outbound traffic toward Canada</li></ul>

## Authentication related fields

Field	KQL Examples	Output
<ul style="list-style-type: none"><li>• user.name</li></ul>	<ul style="list-style-type: none"><li>• event.category : "authentication" and user.name:administrator and event.outcome: failure</li></ul>	<ul style="list-style-type: none"><li>• Looks for failed login attempt targeting username administrator</li></ul>
<ul style="list-style-type: none"><li>• winlog.logon.type</li></ul>	<ul style="list-style-type: none"><li>• event.category : "authentication" and winlog.logon.type: "Network"</li><li>• event.category : "authentication" and winlog.logon.type: "RemoteInteractive"</li></ul>	<ul style="list-style-type: none"><li>• Look for authentication that happened over the network</li><li>• Look for RDP authentication</li></ul>
<ul style="list-style-type: none"><li>• winlog.event_data.AuthenticationPackageNames</li></ul>	<ul style="list-style-type: none"><li>• event.category : "authentication" and event.action : logged-in and winlog.logon.type: "Network" and user.name.text:administrator and event.outcome : success and winlog.event_data.AuthenticationPackageNames: NTLM</li></ul>	<ul style="list-style-type: none"><li>• Look for successful network authentication events against the user administrator, and the authentication package is NTLM</li></ul>