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.	• event.category: authentication • event.category: process • event.category: network • event.category: (malware or • intrusion_detection)
event.type	It serves as a sub-categorization that, when combined with the "event.category" field, allows for filtering events to a specific level	• event.type: start • event.type: creation • event.type: access • event.type: deletion
event.outcome	It indicates whether the event represents a successful or a failed outcome	• event.outcome: success • event.outcome : failure

Common search fields

Field	KQL Examples	Output
• @timestamp	• @timestamp: 2023-01-26 • @timestamp <= "2023-01-25" • @timestamp >= "2023-01-26" and • @timestamp < = "2023-01-27"	• Events that happened in 26th • Events that happened with a date less than or equal to 25th of Jan • Events that happened between 26th and the 27th of Jan
• agent.name	• agent.name : DESKTOP-*	• Look for events from the agent name that starts with DESKTOP
• message	• message : powershell	• Look for any message with the word powershell

Process related fields

Field	KQL Examples	Output
• process.name	• event.category: process and process.name: powershell.exe	• Look for powershell.exe as a process
• process.command_line	• event.category: process and process.command_line.text :*whoami*	• Look for a commandline that has whoami on it
• process.pid	• event.category: process and process.pid : 6360	• Look for process id: 6360
• process.parent.name	• event.category: process and process.parent.name: cmd.exe	• Looks for cmd.exe as a parent process
• process.parent.pid	• host.name : DESKTOP-* and event.category: process and process.command_line.text: powershell and process.parent.pid: 12620	• Looks for a process command line that has powershell and the parent process id is 12620 on a hostname that starts with DESKTOP

Network related fields

Field	KQL Examples	Output
• source.ip	• source.ip: 127.0.0.1	• Looks for any logs • originated from the • loopback IP address •
• destination.ip	• destination.ip: 23.194.192.66	• Looks for any logs • originating to IP • 23.194.192.66 •
• destination.port	• destination.port: 443	• Looks for any logs • originating towards port • 443 •
• dns.question.name	• dns.question.name: "www.youtube.com"	• Look for any DNS resolution towards www.youtube.com
• dns.response_code	• dns.response_code: "NXDOMAIN	• Looks for DNS traffic towards non existing domain names
• destination.geo.country_name	• destination.geo.country_name : "Canada"	• Looks for any outbound traffic toward Canada

Authentication related fields

Field	KQL Examples	Output
• user.name	• event.category : "authentication" and user.name:administrator and event.outcome: failure	• Looks for failed login attempt targeting username administrator
• winlog.logon.type	• event.category : "authentication" and winlog.logon.type: "Network" • event.category : "authentication" and winlog.logon.type: "RemoteInteractive"	• Look for authentication that happened over the network • Look for RDP authentication
• winlog.event_data.AuthenticationPackageName	• 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.AuthenticationPackageName: NTLM	• Look for successful network authentication events against the user administrator, and the authentication package is NTLM