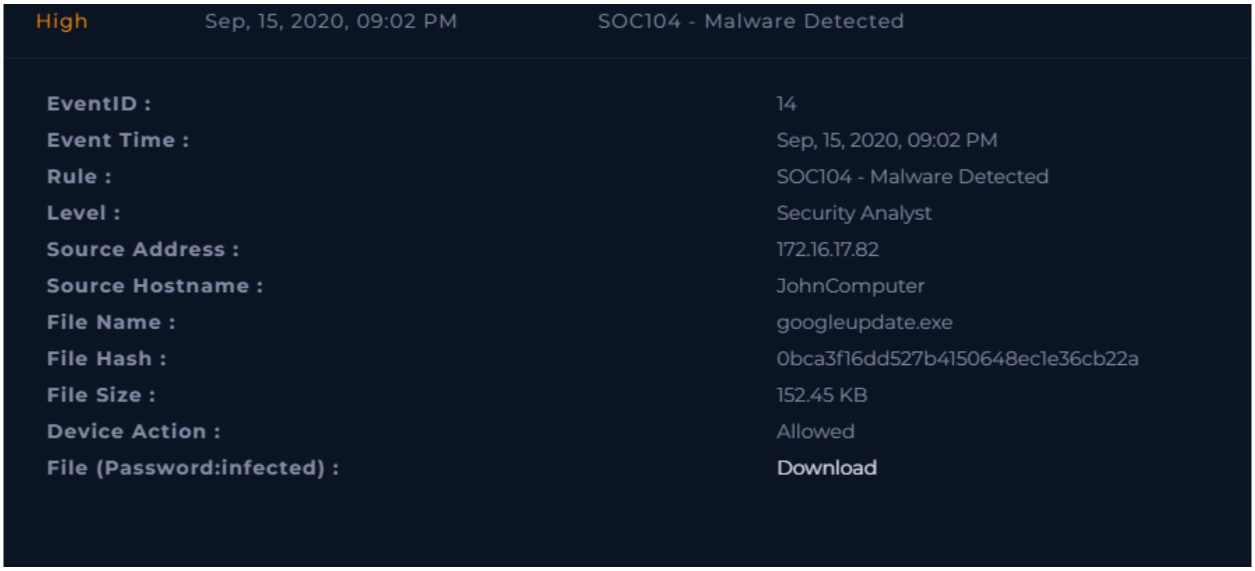
Malware Detected on JohnComputer

The alert and details:



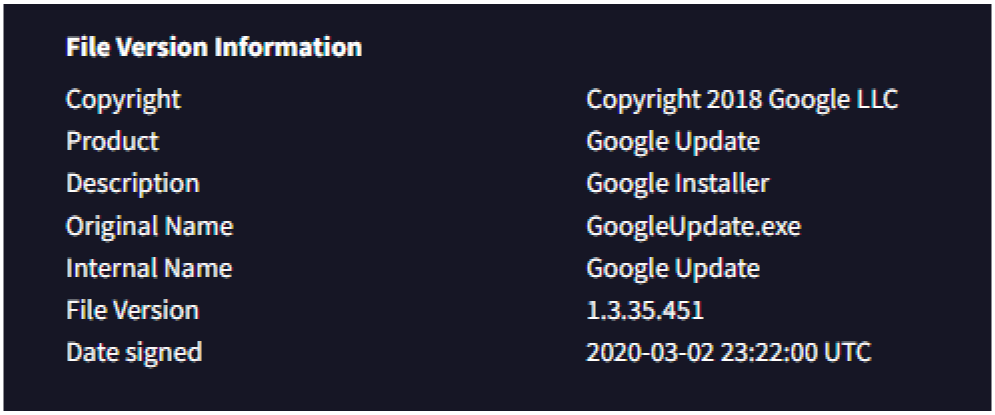
High Sep, 15, 2020, 09:02 PM SOC104 - Malware Detected

EventID :	14
Event Time :	Sep, 15, 2020, 09:02 PM
Rule :	SOC104 - Malware Detected
Level :	Security Analyst
Source Address :	172.16.17.82
Source Hostname :	JohnComputer
File Name :	googleupdate.exe
File Hash :	0bca3f16dd527b4150648ec1e36cb22a
File Size :	152.45 KB
Device Action :	Allowed
File (Password:infected) :	Download

Let's look at what happened at the Host named JohnComputer in the **EDR**.

- Filter details for given filename and Hash.
- The parent process for this is tasking.exe

Gone through processes, network events and terminal history. Other than that, there is no evidence for malicious activity. And also verified the hash value on virus total, no traces of malware.
On further investigating the file, we can say that it is a genuine process.



File Version Information

Copyright	Copyright 2018 Google LLC
Product	Google Update
Description	Google Installer
Original Name	GoogleUpdate.exe
Internal Name	Google Update
File Version	1.3.35.451
Date signed	2020-03-02 23:22:00 UTC

Thus, It is a false positive. The alert must be tuned accordingly.