Threat Hunting

Find Malware and Avoid Reinfection

When ransomware attacks happen, it's essential to respond quickly. But identifying the chronology of the attack can itself delay incident response. With malware dwell times that often span weeks, selecting a recovery point prior to the introduction of the malware is critical to avoid the risk of reintroducing and reinfecting production systems. To ensure a safe recovery without risking a reinfection, you need to be able to pinpoint at what point in time the malware was introduced to your organization.

Identifying the entry point of the threat in the environment and pinpointing the time when it occurred can be nearly impossible without insights about backup snapshots. Threat Hunting analyzes historical backup data to help pinpoint when indicators of compromise first impacted the environment to help avoid malware reinfection during data recovery.

AVOID RISK OF REINFECTION DURING DATA RECOVERY

Using Threat Hunting, you can use the widely accepted YARA rules to scan your backups for traces of intrusion and pinpoint exactly when the specific indicator of compromise was introduced, thus recovering your data from the latest clean snapshot.

SCAN FOR THREATS

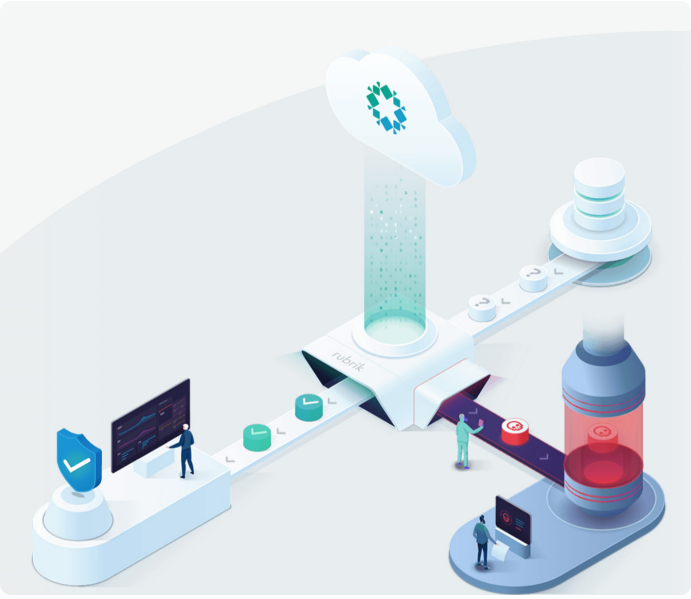
Scan backup snapshots using file hashes and YARA rules to define Indicators of Compromise (IoC).

IDENTIFY RECOVERY POINTS

Analyze backups to surface clean snapshots and identify earliest instance of IoC.

AVOID MALWARE REINFECTION

Utilize the insights to quickly recover with a lower risk of re-introducing malware.



HOW THREAT HUNTING CAN BE USED

Threat Hunting can be used to facilitate threat intelligence efforts as well as to respond quickly to a cyber incident.

1. Scan your backups using the publicly available threat indicators to take preventive measures and minimize impact.
2. Scanning your backups as you investigate your ransomware attack helps you in reacting quickly and identifying the latest available clean snapshot to recover your operations and thus reduce the overall cost of recovery from the attack.

HOW WE ARE DIFFERENT

1. No impact on production environment
2. Process multiple rules across multiple points in time
3. No learning curve: Intuitive UI to execute complex searches for insights

ds-threat-hunting / 20220503