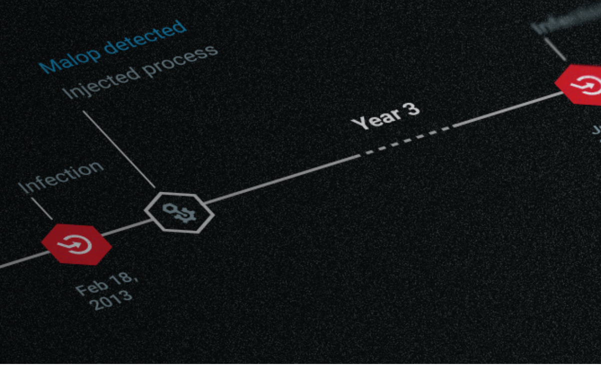
# CYBEREASON REPLAY_

Go back in time & investigate the root cause



## UNIQUE FEATURES

**USER-FRIENDLY INTERFACE**

**SCOPE THE ATTACK:** REPLAY THE PAST AT WILL

**DO NO HARM ON ENDPOINT PERFORMANCE**

**REDUCE OPERATIONAL COST**

## ABOUT CYBEREASON

The Cybereason solution combines endpoint prevention, detection, and response all in one lightweight agent. The solution delivers multi-layered endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Combine the best platform on the market with active monitoring and response from our expert security team to receive a comprehensive defense.

**VISIT OUR WEBSITE TO GET A DEMO OF OUR SECURITY SOLUTION**

CYBEREASON.COM

## DO YOU KNOW HOW YOUR LAST INCIDENT HAPPENED?

One of the most important steps an enterprise can take after containing a breach is to understand the root cause of an incident. Post-incident review, especially one that provides historical data, can answer crucial questions like, how were you breached? What happened before the incident? Is there evidence of threats lurking in the system that existed previously, but are no longer visible? These questions can offer crucial insight into the root cause of an incident and simultaneously save your enterprise money, as the majority of cybersecurity costs come after an incident occurs.

Unfortunately, many enterprises overlook the crucial step of post-incident review due to a lack of necessary tools, resources, or time. Most tools do not provide data far enough back to scope a more sophisticated attack that takes months or years to result in an incident.

For example, your security team is investigating a new incident and is able to identify unknown malware on five machines. Through their investigation, they discover the malware infiltrated via a phishing email. However, they have also identified a sixth machine, but have no evidence of how it was infected. In order to address this, they need access to historical data, which they don't have through traditional security tools. How do you prevent another breach when you don't know what started your last one?

## REPLAY THE PAST AT WILL

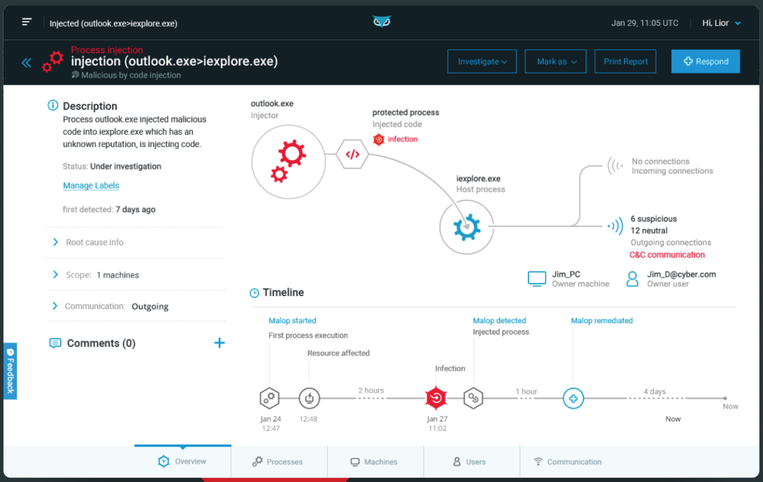
Cybereason Replay provides your security team on-demand, retrospective hunting as part of post-incident review. Your security team can look at your environment as if they had a time machine. Replay takes remediation to the next level by giving your security team the ability to investigate the entire lifecycle of the attack.

With Cybereason Replay, your team can replay specific time periods on selected endpoints, all within the Cybereason platform. Teams can investigate all data, including the entire process tree, timeline, and all activity across machines. Apply the latest understanding of the threat to historical data and investigate past attacks the same way as if it was real time.

# SEE THE ENTIRE ATTACK FROM START TO FINISH_

Replay allows you to investigate the entire attack story, from before it happened to after. Leverage the Cybereason solution's ability to correlate a complex series of events going back months or years in a fully automated way.

The increased visibility of Replay lets your security team thoroughly analyze what happened during a breach, so they can apply the latest understanding of threats to historical data. This includes the entire process tree, timeline, and all activity across machines.



Description
Process outlook.exe injected malicious code into iexplore.exe which has an unknown reputation, is injecting code.

Status: Under investigation

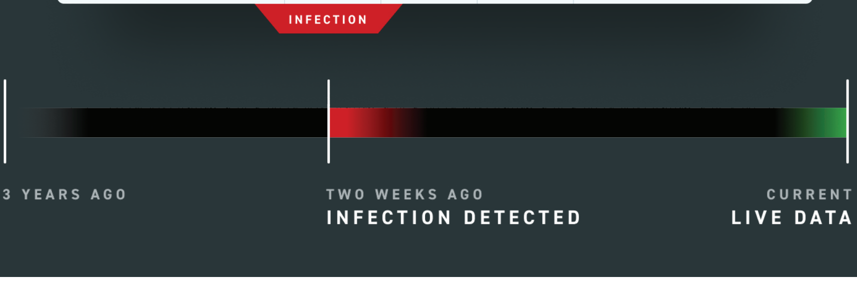
first detected: 7 days ago

Scope: 1 machines

Communication: Outgoing

Comments (0)

**SEE WHAT GAPS IN YOUR DEFENSE NEED TO BE CLOSED.**



## WITH REPLAY YOU CAN:

### INVESTIGATE WITHOUT TIME LIMITS

Investigate and correlate a sophisticated, multi-wave attack.

### INVESTIGATE PRIOR TIME PERIODS

Investigate for bad hashes, IP connections or exercise new threat intel or detection logic to validate a clean environment.

### SCOPE ATTACKS AUTOMATICALLY

Once a detection is raised, scope the full attack no matter how far back and stop all infection vectors.

### COLLECT AUDIT DATA

Go back in time to collect all data required for compliance or audit reasons.

## INVESTIGATE WITH EASE

Take advantage of Cybereason's user-friendly interface to conduct deep investigations into historic events. When your analyst investigates with Replay, they get all the advantages of the real-time platform over defined time windows. They can easily access and drill down into suspicious activities, while simultaneously pivoting between users and machines. All of this is possible without affecting the performance of your endpoints.

## REDUCE OPERATIONAL COST

Determine the data retention window that best suits your needs, whether it is one time, monthly, or an annual subscription. Access what you need, and only what you need.

## KEEP PERFORMANCE HIGH

Investigate historical activity while simultaneously maintaining performance on your endpoints and on the core solution. Cybereason Replay has no impact on the performance of your endpoints or core solution.