Attack Disruption

The Cybereason platform empowers security teams to disrupt detected attacks by containing, remediating, and preventing threats from spreading throughout your organization.

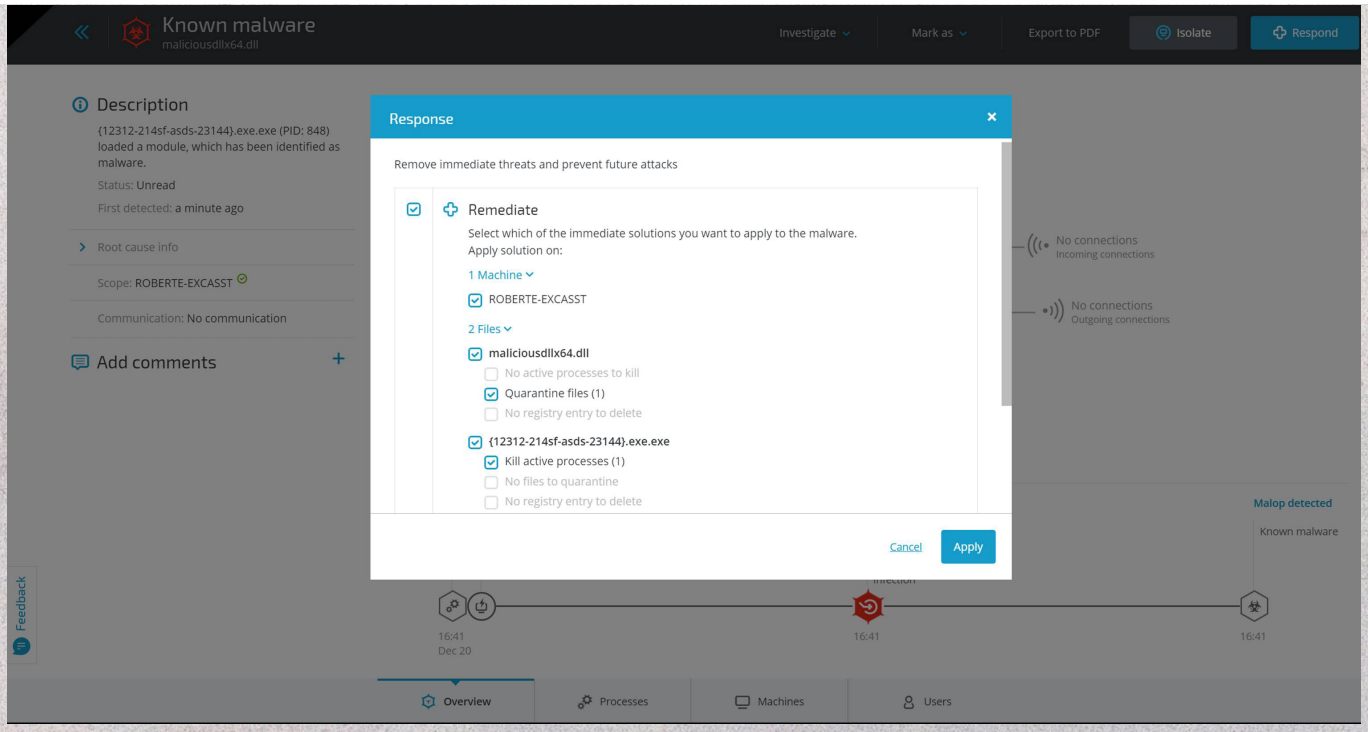
CONTAINMENT Cybereason stops attackers from gaining a wide footprint by enabling you to contain the threat to only compromised endpoints. The platform isolates infected machines by using native OS capabilities to block communication between the endpoint and anyone else. At the same time, your analysts can open a dedicated communication channel to conduct a deep analysis of the attack to fully understand their motives. Also, because your employees might be anywhere when they get attacked, Cybereason can isolate endpoints whether they are connected to the corporate network, or working remotely and directly accessing the Internet.

REMEDIATION The Cybereason platform automates the process of blocking malicious activities in your endpoint environment. With single-click remediation you can immediately kill processes, delete registry keys, and quarantine malicious files on any or all compromised endpoints in your environment, from a single operation within the Cybereason platform. This gives your analysts the power to disrupt the attack but still gain the visibility you need into the attacker's motives.

PREVENTION Once you've remediated the threat on the compromised machines, you can proactively prevent it from spreading to other machines in the organization. You can deploy an optional kernel level component to prevent malicious executables and modules from loading. Upon identification of the malware, you can blacklist it, and automatically instruct all endpoints in an environment to block the attack from spreading.

CYBEREASON ATTACK RESPONSE LETS YOU:

- Identify attacks early in the kill chain and detect malicious activities before an attacker can gain persistence with built-in statistical and behavioral analytics hunting.
- Expedite attack remediation by enabling SOC teams to quickly respond to detected threats directly from the Cybereason platform.
- Prevent an adversary from expanding their footprint by isolating compromised machines from communicating with anyone but your analysts.
- Conduct deep investigation of a compromised machine by gaining a comprehensive view of the attack including which machines, users, processes, connections, etc. were involved.
- Automatically remediate attack activities by blocking executables, killing processes, quarantining files, and removing persistence mechanisms.
- Proactively prevent the spread of malware by quickly sharing malops hashes with all endpoints in an environment within seconds of detection – on connected and disconnected devices.
- Enable remediation capabilities based on your needs either for a small batch of endpoints, or across the entire environment.
- Leverage Cybereason experts for advice on what actions to take in the response process.



cybereason