Case Study

# How an Unprecedented 24-Hour Investigation Helped a Multi-Billion Dollar Pharmaceutical Company Avoid a Massive Ransomware Attack

The security team at a multi-billion dollar pharmaceutical company identified suspicious behavior that couldn't be ignored. A server was trying to reach some IP addresses that were part of an incident that occurred months earlier. In addition, a privileged user account was compromised. They immediately called their Managed Security Service Provider (MSSP) to take a deeper look.

**Parallel processing enabled the investigation to begin right away, wasting no time to identify root cause and remediate impacted systems.**

The MSSP assessed the situation and identified 11 systems that required deeper analysis. Upon collecting and importing those systems into an AWS S3 bucket, they quickly imported the data to their cloud-native investigation platform, Cado.

## Results

### Within 24 hours

The security team collected data from eleven remote systems, processed the data in parallel, and analyzed the findings to complete a thorough incident response investigation in under one day.

### Within 48 hours

Root cause was identified and affected machines were remediated. Just in the nick of time before the attackers were likely planning to execute a follow-up ransomware attack.

## In under three hours, the Cado platform processed all of the data and presented interesting findings including:

- Loads of suspicious activity related to the previous incident
- Unknown malware
- Indicators of Cobalt Strike
- Known ransomware
- Malicious domains

Leveraging Cado's flexible pivot and search capabilities, the team was able to quickly pull all activity connected to the username that was associated with the malware from the earlier attack. With all historical data at their fingertips in a single timeline, it was easy to follow exactly what had happened in the original incident and what was happening more recently. A detection tool alone would not show this level of detail that was required to fully remediate the incident.

Between the client and provider, there were approximately six security analysts working on this investigation who were all located in different countries across the globe. With Cado, they were able to work together on the investigation, noting interesting findings, and help each other to identify root cause. This unprecedented ability to collaborate enabled the team to expedite their investigation in a way that was impossible prior to using the Cado platform.

***"Cado helped us move at the speed we needed to in order to stop this threat. If the investigation took longer than the weekend, I'm certain that our client would have been ransomwared again and we'd all be in a much worse place today as a result."***

-DFIR team lead at MSSP