CUSTOMER CASE STUDY

Large State Judiciary System Customer Case Study

How Security On-Demand identified malicious network traffic on a large state judiciary system.

The Breach

Security On-Demand's ThreatWatch behavioral analytics service detected an anomaly when a suspicious outbound FTP connection found access through the firewall to an abnormal destination. The event was sent to the Threat Reconnaissance Unit (TRU) to be further evaluated by a SOC analyst. After further analysis, TRU determined that the event was potentially malicious with possible data exfiltration. The TRU team sent the client an urgent notification to further investigate the questionable activity.

The Result

Ultimately, the client did not recognize the FTP connection and determined the activity to be malicious, which resulted in immediately changing the firewall rules to block the traffic. Security On-Demand's SOC added the attacker's profile to their consolidated threat reputation monitoring to improve future alert confidence. This enabled the SOC to be on the lookout for similar threats that may arise in the future.