COLORADO

Governor's Office of Information Technology

Endpoint Detection & Response

CATEGORY:
Cybersecurity

STATE:
Colorado

PROJECT INITIATION DATE:
May 2017

PROJECT END DATE:
October 2019

NASCIO STATE IT RECOGNITION AWARDS

Brandi Wildfang Simmons | Chief Communications Officer
brandi.simmons@state.co.us | 303.764.6897

Executive Summary

Finding out you are the victim of a ransomware attack is devastating news for business and cybersecurity professionals alike. In 2018, more than 200 million ransomware attacks were reported. In February of that year, the Colorado Information Security Office (CISO) with the Governor's Office of Information Technology (OIT) and the Colorado Department of Transportation (CDOT) learned first hand about the destructive nature of SamSam ransomware. OIT and CDOT didn't pay the cyber crooks a dime thanks to backup plans that were in place but business operations were offline for a month while the recovery effort was underway.

NEXT

More malicious activity on CDOT computers reported

Eight days into a ransomware attack, state information technology officials detected more malicious activity on computer systems at the Colorado Department of Transportation.

This was a situation where timing was everything. Had it been one week later, the attack would have been just a blip on the cybersecurity radar. An Endpoint Detection and Response (EDR) toolset that would have identified and prevented this attack was in place at four state agencies and CDOT was scheduled for implementation one week after the attack. All of CDOT's data was recovered and the agency returned to business as usual. But the attack highlighted the fact that even with the **Secure Colorado** cybersecurity strategy in place, security tools had to be implemented quickly to detect and stop future attacks.

By April 2018, just two months after the CDOT attack, the EDR toolset was deployed to all agency environments and it has been a game changer. The EDR toolset has improved how threats are identified and has prevented significant security incidents from occurring, including one that would have been on par with the CDOT ransomware incident.

Project Narrative

Concept

The State of Colorado experiences more than eight million security events each day. A security event may be as benign as a mistyped password or as serious as an actual indicator of an attack in progress. But without the right tools in place to identify the serious threats, security staff were spending most of their time attempting to discern which of the millions of daily security events required investigation. The volume of daily security events made it an almost impossible task to properly identify threats requiring urgent action and even as these high risk events were discovered, security staff were not able to investigate even a tiny fraction of the events they were alerted to each day. The complexity of the network (with 17 executive branch agencies) was adding hours of additional incident analysis to determine where specific incidents were occurring (i.e,. which agency, which network, and which device). Additionally, there was no way to automatically ingest indicators of compromise or to alert for attacks against the state network that are similar to attacks occurring against other states or other enterprises. All high-priority events appeared the same within the State of Colorado, and none (or all) stood out as "urgent" when monitored using the capabilities of the security toolset in place at that time.

The state's Chief Information Security Officer (CISO) understood that this was a risk that needed to be addressed and began the work of getting the right tools in place to detect and investigate suspicious activity. The search for what OIT called a security analytics solution involved the evaluation of twelve vastly different EDR solutions to find the best one to help our security analysts immediately discern and investigate the real threats in the state agency environments. The goals of the project included:

- ensuring the detection of actual threats;
- making those stand out over and above all of the noise in the environment;
- utilizing knowledge and threat intelligence across a large pool of non-related endpoints (those belonging to public sector, private sector, and higher education);
- using threat intelligence to inform the behavior of the tool; and
- taking preventive measures blocking actual threats without an analyst having to perform the work manually.

The cost to implement the Endpoint Detection and Response Toolset project as a cloud-based service using existing staff was $588,540. This initiative was successful in reaching its goal of 99% coverage across the state environment. Effectiveness of the controls were verified through the prevention of many attacks in the first few months after the tool set was implemented.

Significance

The EDR toolset was purchased during mid-2017 with implementation occurring in 2018 and 2019. Significant testing with pilot groups from each state agency was first conducted and then work with the vendor followed to ensure the tool was installed and configured for maximum effectiveness. Prior to the implementation of an EDR toolset, the volume of daily security events made it an almost impossible task to properly identify threats requiring urgent action. Even when the threats were identified, taking action to block the threat was a manual and time-consuming process. Once the EDR toolset was put in place, OIT was able to make better utilization of its security analysts. Analysts now perform more intelligent activities while the tool works to actively block threats and alert for human-required actions. The performance of the EDR tool has freed up time for security analysts to create incident response playbooks which document repeatable processes that have been put in place for commonly occuring types of security incidents.

This was the first cloud-only security deployment for the state. It ensured the protections that were implemented function consistently, incorporating evolving threat protections, whether the endpoint regularly connects to the state network or never connects to the state network.

“What makes this effort innovative and distinct from other security projects we’ve implemented, is the immediate and significant protections we began to experience. This tool has provided tangible threat protection with significant impact avoidance, while minimizing the effort and impact felt during the installation,” says Debbi Blyth, Colorado’s Chief Information Security Officer.

Once it was installed, functioning, and appropriately configured, the EDR toolset began to do its job, incorporating evolving threat intelligence and behaviors without significant analyst tuning or maintenance activities required. Other endpoint security tools have required two or more full-time analysts in addition to one or more full-time on-site vendor-provided product engineer(s). ***This product is easily managed by a single analyst saving the state money and allowing analysts to be directed to other important work***.

OIT has consistently prioritized cybersecurity among its topmost annual goals for the past six years. Supporting agency needs requires flexibility and the necessary security controls to allow state employees to do their jobs, while providing protections in case they make a mistake.

Impact

The Endpoint Detection and Response (EDR) tool is successfully blocking between 50 and 350 critical and high risk threats per month that were not being blocked previously by any of our other endpoint security tools. What the EDR tool is now blocking is truly impressive. It has prevented several security incidents that would have otherwise been extremely impactful to agency business operations and potentially to Coloradans who receive state services.

March 2019

A Colorado county was incapacitated by an Emotet infection. Upon examining the state's environment, several instances of active Emotet threats were discovered to be contained within our email system and within individual email messages. However, the State of Colorado was not experiencing any Emotet effects. The reason became clear as we investigated further and realized that our EDR tool was preventing the Emotet malware from executing on our endpoints. As we worked to assist the county with their recovery efforts, we supplied them with our EDR software and licensing to provide protection against future instances of Emotet and other types of malicious threats. This county (and the others for which we provided this software) have not experienced any type of security incidents since the installation of the EDR tool.

August 2019

The EDR tool alerted OIT security analysts to two systems attempting to run a command to execute scripts. The infection was successful in spreading to 18 total systems. However, because of the EDR alert, the analysts were able to quickly take action, using the EDR tool to quarantine infected systems and clean up the infection without it spreading further. Additionally, the EDR tool automatically detected the malware and prevented the execution of the malicious code on each of the 18 systems. Further investigation revealed that this malicious code was Trickbot, and had the EDR tool not been in place and fully installed on all systems, this would likely have resulted in another outbreak of similar scale and magnitude as the ransomware event that occurred at CDOT in 2018.

September 2019

The EDR tool alerted OIT security analysts of a malicious worm that was affecting a state agency. This worm had actually been detected more than two years ago and it was believed to have been eradicated at that time; however, OIT learned that it was lying dormant. The tool alerted the analysts, enabling them to forensically examine both the memory and storage, which led to the rapid identification of the infection, propagation, and persistence mechanisms. This attack was identified as a worm that creates a backdoor and attempts to download additional malware while aggressively spreading, using removable drives. Due to the alerting and prevention mechanisms contained within the EDR tool, the security analysts were able to quickly contain and permanently remediate the malware without any further spreading, and with no interruption to agency business operations.

Also in September, the EDR tool alerted analysts of a backing trojan (Qakbot or QBOT) being

present within an agency network. Again, the EDR tool prevented the execution of the malicious code while alerting analysts to take action. This malware would have established an outbound command and control channel allowing the attacker access to take action within this network and to potentially access systems within the network directly. OIT analysts using the tool were able to isolate and eradicate the malware without any interruption to business operations.

December 2019

The EDR tool **successfully detected and prevented 297 high-risk security incidents**. It is certain that had this tool not been in place, OIT analysts would have been very busy responding to an overwhelming number of security incidents during the month of December.

The success of the EDR implementation has allowed the State of Colorado to deprecate its costly legacy antivirus security solution, **eliminating more than $1 million per year in unnecessary and ineffective security expenditure as well as $350,000 in ongoing annual professional services** required to support the legacy tool. In the years since the CDOT ransomware incident, the data of Coloradans stored within state systems has been better protected and the threat of a successful ransomware attack is greatly reduced.