exabeam

CASE STUDY

ATLANTA PUBLIC SCHOOLS: INCREASING THREAT DETECTION AND AUTOMATING INCIDENT INVESTIGATION

ATLANTA PUBLIC SCHOOLS

Atlanta Public Schools is one of the largest school districts in the state of Georgia, serving approximately 52,000 students across 88 schools. The district is organized into nine K-12 clusters with 67 traditional schools, 17 charter schools, two citywide single-gender academies and two alternative programs.

The APS technology team prides itself on being an early adopter of technology—willing to test and implement many potential solutions as part of its security initiative.

Security Concerns

APS faces the same pressures as other similar organizations in relation to cyber threats. Such threats may come in the form of unknown external entities trying to access their network, systems and/or data. Threats may even come from tech-savvy students attempting to push the envelope to find out how far they can go.

Additionally, as a public institution, APS is a custodian of student records and data about its employees and staff. The district can therefore be a target for bad actor seeking to cause harm or damage.

Two years ago, the school districts' technology team, in trying to keep with its objective of securing student and staff information, hired the services of external consultants to conduct a full security assessment. The audit was designed to help the district improve its security posture. After a penetration test was performed, the audit recommended a 3-phased approach to harden its defenses. One of the key recommendations was to implement technology that would better equip the district to detect lateral movement and insider threats.

The Challenge of Insider Threats

At the time, the existing implementation at APS included several best-of-class point products to help monitor and secure various aspects of its network and infrastructure. While being useful for threat detection, these products did not aggregate the threats, and therefore, could not reveal the entire story regarding any given incident. Additionally, the security team did not have centralized logging from multiple sources, making threat investigation an arduous process. For each event it detected, the team had to painstakingly search multiple source systems, network accounts or end point devices to complete a forensic analysis. Being a manual process, it required logging into various security solutions to obtain and assemble several logs into a contiguous story.

Responses to law enforcement subpoenas, open records requests, or internal requests could result in lengthy investigations. While such requests were not necessarily security oriented, answering questions such as, "What did the user do during a specific time period," or "Which systems has the user interacted with," could create huge investigative workloads.

Exabeam-Enhanced Environment

After considering several legacy SIEM solutions, APS chose two products in the Exabeam Security Intelligence Platform—Exabeam Data Lake and Exabeam Advanced Analytics. These products provide centralized logging and UEBA-based insider threat and lateral movement detection, respectively.

APS selected Exabeam based on several key criteria, including:

- **Unlimited, centralized logging** – After testing several competitive SIEM solutions, the school district chose Exabeam Data Lake because of its ability to help its team centralize unlimited log data. Data Lake pulls disparate security solutions into a single, integrated security management platform.

- **Predictable, cost effective pricing** – Unlike volume-based pricing models used by all legacy SIEM vendors, Exabeam Data Lake's flat, user-based pricing model is cost effective and predictable. This ultimately enabled APS to use its budget from a single project to deploy two much-needed security solutions.

- **Increased visibility and detection** – Exabeam Advanced Analytics (AA) provides an analytics-led approach to threat detection, combining and holistically analyzing data from the entire APS ecosystem. In baselining all user and machine behavior in the district's environment, Exabeam AA automatically identifies anomalous activity. The latter may be indicative of advanced threats that include compromised and malicious insiders, as well as lateral movement.

- **Automated investigations** – Prior to implementing Exabeam, a single investigation could take the APS team 2 to 3 days (or longer, depending on the nature) to complete. With the help of Exabeam products, APS can now automate many of the manual tasks involved in performing their investigations using automatically created incident timelines. These timelines include all the data they would have otherwise needed to piece together by querying through a SIEM. This approach will save the APS technology team valuable time and reduce investigation times from days to hours, thereby greatly improving the security team's productivity.

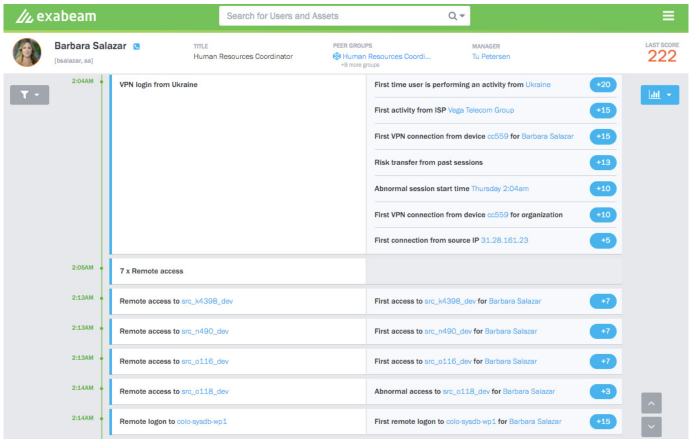
Benefits

APS has seen specific benefits from its Exabeam deployment:

- ***Improved visibility of user and system activity***

- ***Centralized log management***

- ***Decreased incident investigation duration***



Barbara Salazar
[bsalazar, sa]
TITLE Human Resources Coordinator
PEER GROUPS Human Resources Coordi... +8 more groups
MANAGER Tu Petersen
LAST SCORE 222

2:04AM VPN login from Ukraine
First time user is performing an activity from Ukraine +20
First activity from ISP Vega Telecom Group +15
First VPN connection from device cc559 for Barbara Salazar +15
Risk transfer from past sessions +13
Abnormal session start time Thursday 2:04am +10
First VPN connection from device cc559 for organization +10
First connection from source IP 31.28.161.23 +5

2:05AM 7 x Remote access

2:13AM Remote access to src_k4398_dev — First access to src_k4398_dev for Barbara Salazar +7
2:13AM Remote access to src_n490_dev — First access to src_n490_dev for Barbara Salazar +7
2:13AM Remote access to src_o116_dev — First access to src_o116_dev for Barbara Salazar +7
2:14AM Remote access to src_o118_dev — Abnormal access to src_o118_dev for Barbara Salazar +3
2:14AM Remote logon to colo-sysdb-wp1 — First remote logon to colo-sysdb-wp1 for Barbara Salazar +15

Exabeam: Detecting Lateral Movement and Account Switches

For more information, please contact Exabeam at info@exabeam.com