CASE STUDY

exabeam

WASHINGTON STATE UNIVERSITY: FASTER THREAT RESPONSE VIA COMPREHENSIVE DETECTION

Washington State University is a public research university with over $300 million in annual research grant expenditure. Founded in 1890, its far-reaching alumni network of 200,000 individuals spans all 50 states and 146 countries. Additionally, for every $1 the state invested, WSU delivered nearly $19 of economic impact, generating $3.4 billion in annual impact.

WSU engaged with Exabeam to better understand what types of information and insights a UEBA tool would show them about their environment. The WSU team increasingly found themselves relying on Exabeam as their go-to-tool to perform investigation around information they found in alerts of other security products. Exabeam quickly became a standard part of their daily operational flow.

Intitial Security Concerns

Organizations are increasingly under pressure from sophisticated cyber attackers, and the higher education industry is no exception. Prior to implementing Exabeam, WSU's security team noticed a growing trend of advanced threat actors deliberately changing their techniques to blend in with low-risk alerts, in order to avoid detection. The security team quickly realized the potential for other threats lurking in their environment, ones that required analysis beyond static correlation - especially in their large, sprawling network.

Investigating Incidents Before Exabeam

WSU maintains a complex IT environment with a network that includes a diverse assortment of end users and business units -- similar to managing IT for a small city. Each department operates fairly independently, which further complicated matters from a security point of view. The IT security team does not necessarily have authority over all of the sub-environments, but they are still responsible for protecting their systems and data.

From a situational awareness perspective, WSU wanted the ability to investigate its network and fully understand what actions taken, by whom, for what reason, etc. In particular, the team faced the challenge of performing IP-to-host-to-user-to-business-unit mapping. This particular type of attribution was required for every investigation or alert triage, and each mapping required at least 20 minutes. To compound the issue, the team often needed to perform this mapping multiple times while trying to identify lateral movement across their IT environment. This often consumed analyst resources which could have been spend on higher value tasks like threat hunting or incident response.

Exabeam-Enhanced Environment

Understanding that they needed to proactively detect complex threats, WSU's security team selected Exabeam to bolster their visibility and greatly improve SOC productivity. They leverage the Advanced Analytics (AA) solution to holistically analyze data from WSU's many security tools for threat detection, especially as pertains to malware.

WSU chose Exabeam based on several key criteria, including:

- **Automated Host to IP mapping** - Exabeam has become WSU's immediate go-to for incident response because of its host-to-IP-to-user mapping, overcoming previous infrastructure limitations. Exabeam performs this mapping in seconds instead of minutes, and WSU's response time has dropped by roughly 80% since implementing Exabeam.

- **Intelligent security alert prioritization** - WSU leverages Exabeam's ability to holistically analyze security alerts alongside data from other tools in an environment to yield more meaningful context. Users are provided instant access to information like what happened before and after an alert, and whether or not that activity was normal. This level of detail helps analysts easily determine which alerts which require the most attention and to focuses their efforts on the highest-risk alerts.

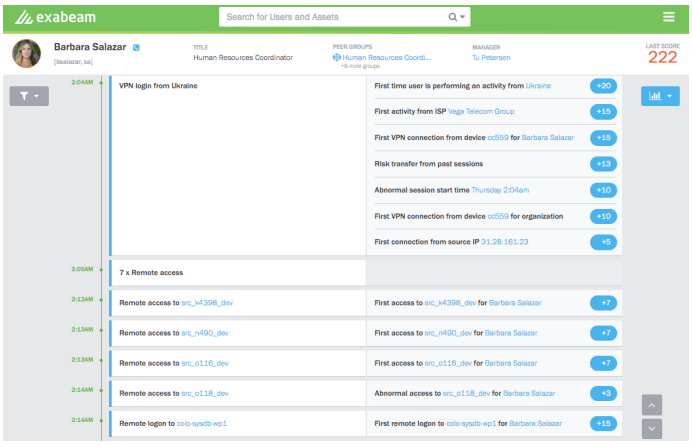
- **Pre-constructed session timelines** - Once the WSU uses used Exabeam to quickly perform attribution mapping, they can then review the pre-built incident timelines for any alerts they discovered. Exabeam connects disparate events to reveal a true incident timeline, which automates analyst investigation and makes proactive analysis faster and easier.

- **Detecting more than malice** - Exabeam Advanced Analytics is able to identify deviations from normal behavior, for both good and bad actors. This ensures that security teams capture true threats but also raise awareness of other issues that require attention, such as a misconfigured server, rule, or policy. Exabeam provides WSU with the ability to proactively identify and address these situations before they become more serious.

Benefits

Washington State University has seen specific benefits from its Exabeam deployment:

- ***Broader and deeper insight into risk***
- ***Decreased time-to-respond by roughly 80%***
- ***Clearer picture of sub-environments***



Pre-built incident timelines allow analysts to perform rapid incident investigation.

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