



**Office of the Washington State Auditor**  
**Pat McCarthy**

January 12, 2023

Dear Michael,

You have quickly adapted to life at SAO and demonstrated what it means to be a true team player.

You've flawlessly integrated into the Information Security team dived headfirst into our siem solution, Sentinel. You took training to understand the Kusto Query Language which is used to access logs in all things Azure. This allowed you to meaningfully look through and examine the data in Sentinel. Parsing through all this log data was no small task. Michael, you have taken eagerly to the task at hand to both understand the cryptic Microsoft Windows Security Event Log data and provide the Information Security team a dashboard in Sentinel. This dashboard provides the security team unprecedented insight into security events and analysis which we had little to no visibility before.

Michael, you have successfully partnered with and engaged Team Information Services to close a critical vulnerability on the CISA Known Exploited vulnerability list. You also assisted monitoring and communicating in response to our Nitro Pro removal as well as Oracle Java update cycles. Lastly, you were instrumental in communicating our requirements to TeamIS regarding uploading SAO Workstation data to Sentinel which provides us visibility into our largest attack surface.

Michael, you have improved the Agency's security program and overall posture.

Since your arrival you've:

- Taken training to learn the Kusto Query Language to successfully query Azure logs.
- Learned about the cryptic Windows Security Event Log and how to decipher it.
- Developed several queries surrounding potentially actionable Security issues.
- Constructed a dashboard in Sentinel to provide immediate visibility to the Information Security Team and executive management.
- Identifying areas where the agency has security gaps and recommending ideas on how to improve.
- Worked with TeamIS to remove, replace, and upgrade legacy software applications.

In your short time at SAO you've made an impressively positive impact and we thank you for that. Your eagerness to learn and dive in, combined with a teamwork mindset, friendly demeanor, can-do attitude, and approach to problem solving has become an invaluable asset to SAO.

Sincerely,

1/13/2023

**Shaun Marquardt**

Aaron Munn  
Chief Information Security Officer  
Signed by: Munn, Aaron (SAO)