A Tradition of Stewardship
A Commitment to Service

Agenda Date: 11/10/2020
Agenda Placement: 6Q

NAPA COUNTY BOARD OF SUPERVISORS
Board Agenda Letter

TO:	Board of Supervisors
FROM:	Jon Gjestvang - Chief Information Officer Information Technology Services
REPORT BY:	Shawn Smith, Supervising Staff Services Analyst - 707.259.8665
SUBJECT:	Agreement with Arctic Wolf Networks, Inc.

RECOMMENDATION

Chief Information Officer requests approval of and authorization for the Chair to sign an agreement with Arctic Wolf Networks, Inc., for a maximum of $720,971 for the term of November 20, 2020 through November 19, 2023 for a subscription-based service to manage and monitor logs, devices, clouds, network and assets for internal IT teams.

EXECUTIVE SUMMARY

In order to improve the County's information security risk posture, ITS needs increased visibility into activity within cloud-based and on-prem computing environments. This is important because timely detection of malicious cyber activity is critical to preventing or minimizing the impact of an attack. This has traditionally been done by setting up an on-premises security operations center (SOC) and a security information and event management tool (SIEM) to collect and analyze data. The challenge with that approach is that it requires significant staffing resources and expertise. In addition, more of the County's applications are in the cloud, making an on-prem solution less feasible. ITS seeks to purchase this capability from Arctic Wolf, a cloud-based managed detection and response service provider, that can provide 7x24 security operations capabilities.

Arctic Wolf was selected from a formal RFP process. Approval will establish a professional services agreement with Arctic Wolf Networks for subscription based services associated with the security operations and managed detection and response. Approval of this purchase and professional services agreement will allow ITS to use the security platform to more effectively detect and respond to cyber attacks.

Today's recommended action is to enter into an agreement with Artic Wolf Networks, Inc. for hosted security operations center and managed detection & response services in the amount of $720,971. The agreement has a three year term and includes all implementation services.

Arctic Wolf Networks, Inc. is not a local vendor.

FISCAL & STRATEGIC PLAN IMPACT

Is there a Fiscal Impact?	Yes
Is it currently budgeted?	No
What is the revenue source?	ITS budget
Is it Mandatory or Discretionary?	Mandatory
Is the general fund affected?	No
Future fiscal impact:	Ongoing costs will be included in the ITS budget.
Consequences if not approved:	If not approved, ITS will have to look for other ways to manage cybersecurity risks, which could cost more.
County Strategic Plan pillar addressed:	Effective and Open Government

Additional Information:

ENVIRONMENTAL IMPACT

ENVIRONMENTAL DETERMINATION: The proposed action is not a project as defined by 14 California Code of Regulations 15378 (State CEQA Guidelines) and therefore CEQA is not applicable.

BACKGROUND AND DISCUSSION

In order to improve the County's information security risk posture, ITS needs increased visibility into activity within cloud-based and on-premises (on-prem) computing environments. This is important because timely detection of malicious cyber activity is critical to preventing or minimizing the impact of an attack. This has traditionally been done by setting up an on-premises security operations center (SOC) and a security information and event management tool (SIEM) to collect and analyze data. The challenge with that approach is that it requires significant staffing resources and expertise. Retaining talent with expertise in building and sustaining a SOC is very expensive. In addition, more of the County's applications are in the cloud, making an on-prem solution less feasible.

In April 2020, the County released an Request for Proposal (RFP) to procure a managed security service provider (MSSP) to provide security operations center as a service (SOC-as-a-service) and managed detect & response (MDR) services. The RFP had over 150 questions.

Through the months of May and August the ITS Information Security Team (consisting of the Chief Information Security Officer and the Information Security Analysts) reviewed the RFP responses and interviewed five finalists. A detailed analysis and scoring was completed. The evaluation ranked each vendor in five main areas consisting of implementation approach, functionality, technology, technical expertise and service levels. Due to the significant role this investment will play in the County’s information security program, cost was only considered a factor if the five areas ended in a close tie. One vendor was selected unanimously by the team to be the best overall fit for the

County. With the support of the Chief Information Officer, the Information Security Team initiated contract negotiations with the assistance of County Counsel.

Today's recommended action is to enter into an agreement with Arctic Wolf Networks, Inc. for hosted SOC-as-a-service and MDR services in the amount of $720,971. The agreement has a three year term and includes all implementation services.

Approval will establish a professional services agreement with Arctic Wolf Networks for subscription based services associated with the security operations and managed detection and response. Approval of this purchase and professional services agreement will allow ITS to use the security platform to more effectively detect and respond to cyber attacks.

Arctic Wolf Networks, Inc. is not a local vendor. Arctic Wolf is considered an industry leader in cybersecurity and offers a customized security strategy for organizational needs.

SUPPORTING DOCUMENTS

None

CEO Recommendation: Approve

Reviewed By: Samuel Ross