Clayton State University
Budget Priority Request
Budget Period 2023

Division/Department: Information Technology & Services

Priority Title: Cybersecurity Operations Managed Services (Artic Wolf)

Priority Number: #1

Funding Requested: $17,324 ☒ Permanent □ One-Time

1) Description of Request:

   ITS is proposing to partner with a managed services security vendor (Arctic Wolf) for cybersecurity operations, monitoring, detection, managed risk, and breach assistance. While ITS employs a robust set of security tools to protect the University's technology environment, there is an inability for us to easily discern our security posture nor the ability to identify the medium/high security risks that need to be addressed in real-time. Moreover, we are unable to fund the associated expense to hire personnel to provide 24x7x365 monitoring of our technology environment. To overcome this fact, we propose employing Arctic Wolf, who can consume and analyze our various system logs and correspondingly identify security threats or breaches. The system logs to be shared include those associated with our security tools (Cylance, Palo Alto firewalls), endpoints (operating systems), technology infrastructure (network, operating systems, VMware (servers), and collaboration tools (Microsoft O365). The service will be focused on our most sensitive environments, which include data center operations, business offices, College of Health Services, and Office of the President. The annual cost of the managed services agreement is $131,974. The cost will be offset by eliminating an existing Information Security Professional role (Position #10033239) (Savings of $91,650 w/Fringe (41%)) and not renewing the Tenable.io vulnerability management tool ($23,000). The offsets reduce the total funding request to $17,324. ITS will self-fund this expense.

2) Justification: Please provide a justification that discusses such things as support of the University's strategic plan or other institutional objectives. What impact will this request have on university programs and services? Can you redirect funds to meet this need?

   Justification:

   CSU is required to comply with the University System of Georgia–Information Technology Handbook requirements. The USG IT Handbook calls-out specific responsibilities as it relates to institutional cybersecurity programs. Section 5.1.3-USG Organizational Responsibilities identifies the need to establish and maintain an information technology and cybersecurity risk management program, including a risk assessment, analysis, planning mitigation, and a continuous monitoring process. Section 5.1.4-Policy and Procedure Management Requirements identifies the need to establish and maintain processes for the assessment and analysis of risks associated with USG information assets. It also states the need to conduct continuous monitoring to identify and verify the effectiveness of implemented protective measures. Based upon current staffing and resources, ITS is unable to meet the aforementioned requirements.

Universities are targets for cyber-attacks and, specifically, ransomware due to the large volume of data that is collected, used, and stored. If Clayton State were to suffer a breach or ransomware attack, the impact on university programs and services would be significantly impacted for an extended period of time. Securing the campus is more challenging than ever as the frequency and sophistication of attacks are increasing exponentially. The ITS-Information Security team is lean; consisting of a Cybersecurity Compliance Manager and a staff member who splits their time between networking and firewall administration needs. Arctic Wolf's ability to utilize the output (logs) of our current security and infrastructure products and the assignment of a dedicated, two-person team to Clayton State will significantly enhance our security posture and provide the support needed to respond to serious threats, vulnerabilities, and risks.

Arctic Wolf provides assurance through a combination of two services - Managed Detection Response (MDR) and Managed Risk (MR) services. The services include:

- Managed Detection and Response (MDR)
    - 24x7 data and network traffic monitoring (Concierge security team – dedicated to the university) and guided response to stop threats before they do harm
        - Eliminates false positives to promote a faster response time
    - Identify threats across network, endpoints, and cloud.
    - Discover vulnerabilities and misconfigurations.
    - Guidance and prioritization for remediating threats, vulnerabilities, and risks.
    - Provides detailed recovery and hardening recommendations
        - Investigations
        - Forensics
        - Find root cause
        - Validate remediation
    - Hunts for advanced threats across endpoints and networks.

- Managed Risk (MR)
    - Network vulnerability assessment
    - Host-based vulnerability assessment
        - Continuously scans the network, endpoints, and cloud environments to quantify digital risk, discover risks beyond vulnerabilities, benchmark the current state of our environment
        - Risk management processes that harden our security posture

  - Account takeover risk
    - Identifies and categorizes risky software, assets, and accounts
  - Cloud security posture management (CSPM)

Arctic Wolf will also provide financial assistance in the event of a cybersecurity incident:

- *Ransomware or Business Email Compromise (BEC)* ($100,000) support costs associated with a ransomware incident or business email compromise that leads to funds transfer or other fraud.
- *Compliance* ($100,000) supports regulatory penalties, fines, or other related costs triggered by a cybersecurity incident.
- *Cyber Legal Liability* ($250,000) supports lawsuit costs resulting from a cyberattack, related to privacy, security, data loss or misuse, or more.
- *Business Income Loss* ($50,000) supports the fiscal impact of a cybersecurity incident that results in lost business income.

3) Metrics: Please describe how you plan to determine the effectiveness and measure the impact of the proposed funding.

Exploitability metrics reflect the ease and means by which the vulnerability can be exploited and impact metrics that reflect the impact of an attack that exploits the vulnerability through quantitative scoring (higher the score, greater the risk). Through the Arctic Wolf dashboard, Information Security will have access to reports that assesses and provides metric data on Clayton State's overall security posture through security vulnerability reports (events discovered during scanning, current security level), weekly security reports (detailing overall security score, any open ports or misconfigurations on the network, investigations into potential incidents as well as reported incidents brought to the university's attention), and monthly assessment reports to name a few.

Clayton State University
Budget Priority Request
Budget Period 2023

Division/Department: Information Technology Services

Priority Title: Palo Alto Firewall Service Subscription

Priority Number: 2

Funding Requested: $81,797.26 X Permanent □ One-Time

1) Description of Request:

   ITS purchased Palo Alto firewalls three years-ago. At the time of acquisition, ITS pre-paid three years of subscription services. The initial three years of service will expire in November 2022. The one-year renewal cost for the Palo Alto firewall service is $81,797.26. This expense will be an on-going, recurring need.

2) Justification: Please provide a justification that discusses such things as support of the University's strategic plan or other institutional objectives. What impact will this request have on University programs and services? Can you redirect funds to meet this need?

   The Palo Alto firewalls represent the Clayton State front-line of defense regarding cybersecurity. The firewalls sit at the border between the internet and the campus network. We have a pair of firewalls arranged in a high availability configuration. The firewalls are used to specify the type of network traffic allowed in and/or out of the CSU network. Moreover, the firewall subscription includes threat prevention to help block known cybersecurity malicious activity. The threat prevention service is updated continuously by Palo Alto as new threats are identified.

   The service subscription fee is a must pay as the firewall is a fundamental to ensure a high-level of security protection. ITS is choosing to self-fund this cost; however, this fact will greatly diminish our ability to absorb a potential FY'23 reduction without decreasing services or personnel.

3) Metrics: Please describe how you plan to determine the effectiveness and measure the impact of the proposed funding.

   There are several metrics that can be tracked to determine overall effectiveness such as firewall policy enforcement, intrusion prevention blocking, application control execution, and up-time.