29-Investment Strategy

Introduction:
In light of the escalating cyber threats faced by our organization and the imperative to safeguard against potential risks, our investment strategy centers on a holistic cybersecurity approach. This narrative outlines how the implementation of Cisco's Extended Detection and Response (XDR), Secure Endpoint, and Umbrella solutions aligns with the objectives of preventing, preparing for, protecting against, and responding to cyber incidents.

Program Objectives:

Preventing Cyber Incidents:

To proactively prevent cyber incidents, the implementation of Cisco XDR is paramount. Its advanced threat prevention capabilities, coupled with real-time threat intelligence and behavioral analytics, will fortify our defenses against sophisticated threats.
Preparing for Cyber Incidents:

Our strategy emphasizes the importance of preparedness through incident response planning and training. The integration of Cisco Secure Endpoint into our endpoint security measures will enhance our readiness, allowing for swift and effective responses to emerging threats.
Protecting Against Cyber Incidents:

The deployment of Cisco Secure Endpoint across all endpoints and the integration of Umbrella's cloud-delivered security will provide comprehensive protection. Secure Endpoint's advanced threat prevention and Umbrella's DNS-layer security will collectively strengthen our defense against a wide range of cyber threats.
Key Investment Elements:

Cisco XDR Integration:

Seamless integration of Cisco XDR into our security infrastructure will provide comprehensive visibility and response capabilities. Cross-layer correlation will enhance threat detection across networks, endpoints, and cloud environments.
Endpoint Security Enhancement:

Cisco Secure Endpoint will be deployed to offer advanced threat prevention, detection, and response capabilities at the endpoint level. Machine learning and behavioral analysis will identify and halt malicious activities in real time.
Cloud-Delivered Security with Umbrella:

Implementing Cisco Umbrella's DNS-layer security will fortify our defense against threats before they reach our network. Its cloud-delivered architecture ensures protection against malicious domains and provides visibility into internet activity.

Continuous Monitoring and Threat Intelligence:

Continuous monitoring using Cisco XDR will detect anomalous activities. The integration of threat intelligence from Cisco Talos and Umbrella will keep us ahead of emerging threats and provide insights for proactive security measures.

Collaboration with Cisco:

Establishing a partnership with Cisco ensures access to timely updates, threat intelligence feeds, and collaborative insights. Participation in Cisco's security community facilitates knowledge sharing and adherence to industry best practices.

Risk Reduction and Community Impact:

Through the deployment of Cisco XDR, Secure Endpoint, and Umbrella, our strategy aims to close identified core capability gaps, significantly reducing the risk of successful cyber incidents. This, in turn, contributes to the overall cybersecurity resilience of our community, state, or nation.

Monitoring and Evaluation:

Regular assessments of the effectiveness of Cisco XDR, Secure Endpoint, and Umbrella, coupled with periodic reviews of incident response plans, will be conducted to ensure alignment with emerging threats and evolving security landscapes.

Conclusion:

Our investment strategy, encompassing Cisco XDR, Secure Endpoint, and Umbrella, positions us to fortify our cybersecurity posture comprehensively. By addressing core capability gaps, reducing risks, and fostering community-wide resilience, we contribute to the overarching security goals of our community, state, or nation.

Collaboration Strategy

Introduction:

In recognition of the interconnected nature of cybersecurity threats, our project places a strong emphasis on collaboration at various levels — regional, statewide, and even at the multi-state level. By deploying Cisco's Extended Detection and Response (XDR), Secure Endpoint, and Umbrella solutions, our strategy aligns with a comprehensive approach that actively engages federal, state, and local governments. This narrative outlines the extent to which our project demonstrates a commitment to collaboration and risk reduction on a broader scale.

Regional and Statewide Collaboration:

To address cyber threats effectively, we recognize the importance of regional and statewide collaboration. Our organization actively participates in cybersecurity forums, collaborates with neighboring cities and counties, and engages with regional entities to share threat intelligence and best practices. Through workshops and joint training sessions, we aim to enhance collective preparedness and response capabilities.

Federal Collaboration:
Our project underscores a willingness to collaborate with federal government agencies, leveraging resources and expertise to strengthen our cybersecurity posture. By actively participating in programs offered by the Department of Homeland Security (DHS), such as information sharing initiatives and training programs, we ensure alignment with federal cybersecurity priorities.

Partnerships with Similar Agencies:
Consultations with similar agencies, both at the city and county levels, facilitate the exchange of insights and lessons learned. Collaborative efforts with entities facing similar cybersecurity challenges enhance our collective ability to prevent, prepare for, protect against, and respond to cyber incidents.

Collaboration with Cisco:
Establishing a strong collaboration with Cisco is integral to our strategy. We actively engage with Cisco's collaborative security community, participate in joint exercises and training programs, and leverage their expertise to enhance our cybersecurity measures. This partnership ensures that we stay informed about the latest threats and industry best practices.

Utilizing DHS, MS-ISAC, and CISA Services:
Our organization is an active participant in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and engages with the Cybersecurity and Infrastructure Security Agency (CISA). We leverage these memberships to access threat intelligence, participate in training sessions, and engage in incident response exercises. This collaboration enhances our situational awareness and response capabilities.

Integration of Cisco Technologies:
The integration of Cisco XDR, Secure Endpoint, and Umbrella aligns with the broader collaborative framework. These solutions not only contribute to our organization's cybersecurity resilience but also enhance our ability to share threat intelligence seamlessly with federal, state, and local partners.

Impact on Risk Reduction:
Through these collaborative efforts, we aim to reduce the overall risk to the state and the nation. By sharing information, resources, and expertise, we create a networked defense that is more resilient and adaptive to emerging cyber threats.

Monitoring and Continuous Improvement:
Our commitment to collaboration extends beyond the implementation phase. We actively seek feedback, participate in joint exercises, and continuously refine our cybersecurity strategy based on shared insights and experiences within the collaborative network.

Conclusion:

In conclusion, our project, fortified by the integration of Cisco XDR, Secure Endpoint, and Umbrella, is a testament to our commitment to collaboration. By engaging with various government entities, similar agencies, and leveraging DHS, MS-ISAC, and CISA services, we contribute to a more robust and interconnected cybersecurity ecosystem that is better equipped to prevent, prepare for, protect against, and respond to acts of cybercrime at regional, statewide, and national levels.

31-Budget Narrative

Introduction:
Our project envisions a robust cybersecurity infrastructure fortified by the implementation of Cisco's Extended Detection and Response (XDR), Secure Endpoint, and Umbrella solutions. The budget plan is designed to maximize cost-effectiveness, ensuring that grant expenditures are strategically allocated to address key project components and support long-term financial sustainability.

Budget Table:
The budget table provides a detailed breakdown of anticipated costs associated with the acquisition, implementation, and maintenance of Cisco XDR, Secure Endpoint, and Umbrella solutions. It encompasses expenses related to licensing, training, integration, and ongoing operational costs.

Licensing	Cisco XDR, Secure Endpoint, Umbrella	$132,858	5yr Term
Operational Costs	Ongoing monitoring, support, and updates	28,700	Yearly after Term
Total Grant Expenditure		$132,858	

Budget Narrative:
The budget is structured to align with the strategic objectives of the project. Licensing costs account for a significant portion, reflecting the investment in cutting-edge cybersecurity solutions provided by Cisco. Training expenses are allocated to ensure that our team is well-versed in operating and maximizing the benefits of the deployed technologies. Integration costs cover the seamless implementation of Cisco XDR, Secure Endpoint, and Umbrella into our existing infrastructure. Operational costs encompass ongoing monitoring, support, and updates to sustain a resilient cybersecurity posture.

Financial Sustainability:
To ensure the financial sustainability of the project beyond the grant period, operational expenses have been classified as operational expenditures (OpEx). This approach allows for the continued allocation of resources to maintain and enhance the cybersecurity infrastructure as part of regular operating costs. By embedding these costs into our ongoing budget, we mitigate the risk of service interruptions and maintain the effectiveness of the implemented technologies.

Local Matching Funds:

While local matching funds are not available for this project, the budget has been meticulously crafted to optimize the use of the grant funds and maximize the impact of the cybersecurity enhancements. The absence of local matching funds is mitigated by the careful allocation of resources and a focus on long-term financial sustainability.

In-Kind Match and Match Waiver:
No in-kind match is proposed for this project, and we will not be submitting a match waiver. The budget has been designed to leverage the grant funds effectively without relying on in-kind contributions.

Funding Request:
We are requesting $132,858 in grant funding to support the acquisition, implementation, and maintenance of Cisco XDR, Secure Endpoint, and Umbrella. This investment is critical to enhancing our cybersecurity resilience and contributing to the overall security posture of our organization.

Conclusion:
The budget plan demonstrates a strategic and efficient use of grant funds to implement and sustain a state-of-the-art cybersecurity infrastructure. By incorporating ongoing operational costs into regular expenditures, we ensure the long-term effectiveness of the cybersecurity measures beyond the grant period. The absence of local matching funds is offset by careful budgeting and a commitment to financial sustainability. This comprehensive approach positions our organization to maximize the impact of the grant and achieve lasting cybersecurity enhancements.

36-Impact and Outcomes

Project Description:
This project centers on the implementation of Cisco's cybersecurity solutions - Extended Detection and Response (XDR), Secure Endpoint, and Umbrella. The objective is to fortify our organization's cybersecurity posture comprehensively, addressing identified threats and hazards while enhancing our capabilities to prevent, prepare for, protect against, and respond to cyber incidents.

Procedures Implemented:

Advanced Threat Prevention: Cisco XDR will be deployed to proactively identify and block sophisticated threats through advanced threat prevention measures, including real-time threat intelligence and behavioral analytics.

Endpoint Security Measures: Cisco Secure Endpoint will enhance our endpoint security measures by providing advanced threat prevention, detection, and response capabilities. This

includes machine learning and behavioral analysis to identify and halt malicious activities in real time.

Cloud-Delivered Security: Cisco Umbrella's DNS-layer security will be integrated to protect against threats before they reach our network. This cloud-delivered security architecture ensures a robust defense against malicious domains and provides visibility into internet activity.

Enhanced Capabilities:

Comprehensive Threat Visibility: Integration of Cisco XDR provides comprehensive visibility across networks, endpoints, and cloud environments, enhancing our ability to detect and respond to threats at multiple layers.

Real-time Incident Response: Cisco's technologies enable real-time incident response capabilities, allowing our cybersecurity team to swiftly and effectively mitigate the impact of cyber incidents.

Cross-Layer Correlation: The cross-layer correlation capabilities of Cisco XDR contribute to a more cohesive cybersecurity strategy, enabling a unified defense against threats at different levels of the infrastructure.

Threats and Hazards Mitigation:

Malware and Ransomware: Cisco Secure Endpoint's advanced threat prevention capabilities mitigate the risks associated with malware and ransomware attacks.

DNS-Based Threats: Cisco Umbrella's DNS-layer security mitigates the risks associated with DNS-based attacks and provides an additional layer of defense against malicious domains.

Sophisticated Cyber Threats: Cisco XDR's behavioral analytics and real-time threat intelligence address the challenges posed by sophisticated cyber threats, providing proactive identification and mitigation.

Measurement and Evaluation:

Effectiveness Metrics: The effectiveness of the project will be measured through key performance indicators (KPIs), including the reduction in the number of successful cyber incidents, response times to incidents, and the overall improvement in threat detection capabilities.

Incident Response Exercise: Regular incident response exercises will be conducted to evaluate the readiness and effectiveness of the response procedures implemented with Cisco's technologies.

Continuous Monitoring: Ongoing monitoring using Cisco XDR will contribute to the continuous evaluation of the cybersecurity landscape, enabling adjustments to the strategy based on emerging threats.

NOFO Objectives and Required Elements:

Objective 1: Enhance Prevention Capabilities: The project aligns with Objective 1 by implementing advanced threat prevention measures through Cisco XDR and Secure Endpoint.

Objective 2: Strengthen Preparedness and Response: The project aligns with Objective 2 by enhancing incident response capabilities with real-time response measures facilitated by Cisco's technologies.

Objective 3: Foster Information Sharing and Collaboration: Collaboration is facilitated through Cisco's collaborative security community, and the project aligns with Objective 3 by participating in information sharing initiatives and collaborative programs.

Required Elements (1-16): The project addresses all 16 required elements, including risk assessments, cybersecurity training, incident response planning, and the integration of advanced cybersecurity technologies.

Conclusion:
This project's impact is significant — a fortified cybersecurity posture, enhanced capabilities, and a proactive approach to mitigating identified threats and hazards. The outcomes will be measured through defined metrics, evaluations, and the alignment with NOFO objectives and required elements, ensuring a comprehensive and effective response to the dynamic cyber threat landscape.