WaTech
Washington Technology Solutions

Establishing a Strategic Threat Intelligence Center

Office of Cybersecurity

April 2024

This page intentionally left blank

Contents

Executive Summary

This document aims to provide an overview of a whole-of-state approach to cybersecurity and explain the urgent need to establish a Strategic Threat Intelligence Center (STIC) to act as a central cybersecurity intelligence and response hub for all state, local, and Tribal governments in Washington.

Cybersecurity threats constantly evolve, with state and local governments, educational institutions, and special service districts facing unprecedented challenges. Establishing a Strategic Threat Intelligence Center (STIC) in Washington state represents a pivotal step in enhancing our collective cybersecurity posture through a whole-of-state approach. This initiative seeks to address the fragmented visibility and response to cyber threats across various entities within the state, ensuring a coordinated and comprehensive defense mechanism is in place.

The need for a whole-of-state approach

Cybersecurity threats know no boundaries, affecting entities large and small across Washington state. With an alarming increase in cybercrime, particularly ransomware attacks, the need for a unified response has never been more critical. The whole-of-state approach fosters a collaborative environment where resources, information, and strategies are shared across all levels of government, educational institutions, and other organizations. This collective effort is crucial for breaking down silos and enhancing the state's overall cybersecurity resilience.

Strategic Threat Intelligence Center (STIC): A centralized solution

The STIC is envisioned as a central hub for cybersecurity intelligence and response. It differs from traditional Security Operations Centers by offering a broader range of services, including threat hunting, compliance management, and security awareness training. By pooling threat intelligence and resources, the STIC aims to provide a comprehensive view of the cybersecurity landscape, allowing for more proactive and effective defenses against cyber threats.

Key services and benefits

The STIC will offer a suite of essential services, including but not limited to:

- Security auditing, monitoring, and event correlation.
- Threat and vulnerability management.
- Incident response management.
- Security compliance management.
- Penetration testing and security awareness training.

This initiative is about protecting individual entities and safeguarding the state's critical information assets, infrastructure, and services. By enhancing threat management and minimizing the impact of successful attacks, the STIC will play a crucial role in improving compliance with regulatory requirements and reducing financial, legal, regulatory, and reputational risks.

Collaboration and funding models

Active participation and stakeholder support are vital for the STIC to succeed. Various funding models are being considered to ensure the initiative's sustainability and accessibility to municipalities of all sizes. The goal is to create a scalable, efficient, and innovative cybersecurity framework that addresses Washington state's current and future needs.

Conclusion

Establishing the Strategic Threat Intelligence Center (STIC) would signify a major advancement in Washington's dedication to cybersecurity. Adopting a whole-of-state approach, this initiative strengthens our cyber defenses and establishes a model for nationwide collaborative efforts in cybersecurity. Moving forward, the STIC will play a key role in fostering a safer, more secure digital landscape for all Washington residents.

Introduction

Having a complete picture of threats and vulnerabilities within any organization is an essential component of managing cybersecurity risks to information and information systems. This is essentially important for governmental entities. No single entity within Washington has a complete picture of the state's threat and vulnerability landscape, its local municipalities (cities, counties, and Tribes), educational institutions (K-12 and higher education), and special service districts. Many of these organizations do not even possess a centralized system to detect such indicators. The following document describes the development and implementation of a Strategic Threat Intelligence Center (STIC) and the benefits Washington would receive through a whole-of-state approach to addressing this problem.

What is "whole-of-state"?

WaTech defines whole-of-state as:

> **"An approach emphasizing partnership at all levels of government, educational institutions, Tribal nations, and other organizations in the public and private sectors to share resources and information breaking down silos within Washington state."**

The Legislature recognized this when it enacted RCW 43.105.450. Subsection 3(g) assigns the Office of Cybersecurity (OCS) the responsibility of *"serving as a resource for local and municipal governments in Washington in the area of cybersecurity."* This sets the stage for a whole-of-state strategy.

Applying a whole-of-state philosophy to cybersecurity enables state and local governments and their partners to pool resources to defend against cybersecurity threats.

Why is whole-of-state cybersecurity critical?

Local municipalities have challenges at various levels regarding cybersecurity. The smaller the municipality, the more challenges exist, from acquiring and deploying appropriate security controls to staffing resources and funding levels.

State and local governments have faced unprecedented cybercrime in recent years. For example, in 2020, local governments experienced a 485% increase in ransomware attacks, striking no less than 2,354 governments, healthcare facilities, and schools.[1].

The issue of cybercrime, specifically ransomware attacks against state and local governments, healthcare facilities, and educational institutions, remains a significant concern, with various studies highlighting the growing threat and exploring potential countermeasures. The increase in ransomware attacks is driven by easier access and more substantial financial payoff, targeting high-profile organizations, government entities, educational institutions, and healthcare organizations.

[1] What is Whole-of-State Cybersecurity Government Technology, July 10, 2023

These attacks are expected to continue due to the anonymity of ransom transactions and the high success rates achieved by targeting large organizations for bigger payouts[2].

The FBI has issued multiple warnings about rampant ransomware attacks on local government agencies, which have disrupted services, raised public safety risks, and caused financial losses. These attacks are particularly concerning because local governments oversee critical utilities, emergency services, and educational facilities that the public heavily relies upon. Following academia, local government entities were the second most victimized group in 2021.[3].

The impact of these attacks can be severe. Smaller counties and municipalities have been targeted, often constrained by limited cybersecurity resources and budgets. The aftermath of a ransomware attack on local government includes financial liabilities related to operational downtime, device costs, network expenses, and sometimes even paid ransoms. Underfunded public sector organizations with outdated systems may find themselves paying ransoms to retrieve their data.

Recent incidents have disrupted public and health services, emergency operations, and compromised personal data. These attacks strain financial and operational resources, putting residents at risk. For instance, in January 2022, a U.S. County had to take computer systems offline and rely on backup contingencies after a ransomware attack impacted local government operations.

The cybersecurity company Emsisoft observed 77 ransomware attacks involving local governments between January and December 2021. Emsisoft estimates the total cost of these attacks to taxpayers at $623 million. The cost of rectifying a ransomware attack, including resources, downtime, lost opportunity, and ransoms paid, averaged $1.64 million in 2021[4].

These facts show that many municipalities can stand to improve their defenses against cyber threats. Too often, these attacks succeed because municipal governments, K-12 schools, and other small government agencies need more staffing, tools, training, and expertise to defend themselves adequately. Many lack the contract purchasing power to achieve economies of scale and gain visibility of their interconnected systems.

What is a whole-of-state cybersecurity strategy?

In a whole-of-state strategy, the state government collaborates with smaller local governmental organizations to ensure everyone is protected from threats. As part of this collaboration, state governments share training, threat intelligence, tooling, and other resources with municipalities and other local organizations to strengthen cyber defenses.

Understanding the rise of whole-of-state cybersecurity.

Whole-of-state cybersecurity is gaining popularity for several reasons. One factor in this methodology acknowledges shared cyber risks between organizations in the same industry. Municipalities of all

---

[2] Responding to Ransomware Attacks.

[3] FBI Private Industry Notification, 30 March 2022 "Ransomware Attacks Straining Local US Governments and Public Services".

[4] EmiSoft Blog, 3 August 2022 "Ransomware cost US Local Governments $623 Million in 2021, but fewer incidents in 2022"

sizes and types share these risks, so by sharing resources, they can increase their level of defense individually and as a community.

Another factor is reduced duplication of effort. State, local, Tribal, and territorial entities can't manage shared cyber risks alone. They lack the resources or expertise to make it work, and the increasing interconnectivity of systems only makes the challenges more complex and difficult to contain.

Ten reasons why whole-of-state cybersecurity may be the way of the future.

1. **Shared cyber risks:** Cyber threat actors have proven they do not discriminate between state agencies or small municipalities. All share similar cyber risks.
2. **Economies of scale:** By applying cybersecurity solutions across multiple organizations, states can support state agencies and less-resourced municipalities together, helping to mitigate shared cyber risk.
3. **Reduced duplication of work and effort:** There is a tremendous amount of duplication of services, work, and effort from the state to county to municipal levels to defend against persistent and sophisticated cyber threats.
4. **Reduced cost:** Shared services and tools can reduce incremental licensing costs.
5. **Consistency of service:** Shared cybersecurity services or tools create a common culture and language across the state, creating a consistency of service that can benefit users.
6. **Knowledge sharing and collaboration:** Ease of communication and collaboration between state, county, and municipal personnel regarding challenges or insights.
7. **Standardized processes, methodologies, and technologies:** Alignment of processes, methodologies, and technologies across all levels of government and public organizations, allowing for collaboration.
8. **Greater efficiencies in training and human resources:** Less-resourced organizations succeed as services and needed training is available at all levels, regardless of the assigned information technology staff size.
9. **Streamlined visibility:** information technology leaders will have better visibility of service data because the services are applied across a broader range of organizations within the state.
10. **Improved measurement:** With access to more service data, leaders within the state can make more informed decisions on what services are working and where to spend future funds to continue to improve cybersecurity collectively.

What is a Strategic Threat Intelligence Center (STIC)?

A Strategic Threat Intelligence Center (STIC) is a centralized entity responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents. Its primary objective is to ensure information assets' confidentiality, integrity, and availability by identifying and mitigating security threats in real time.

As described in the remainder of this document, a STIC is different from a regular Security Operations Center (SOC) in many ways. One major difference is that a SOC is a part of the STIC.

Traditional SOC implementations incorporate security monitoring and event correlation with analysis through a log retention and management system, often called a Security Information Event Management (SIEM) system or service. The SOC will generally include 24/7/365 monitoring by trained personnel.

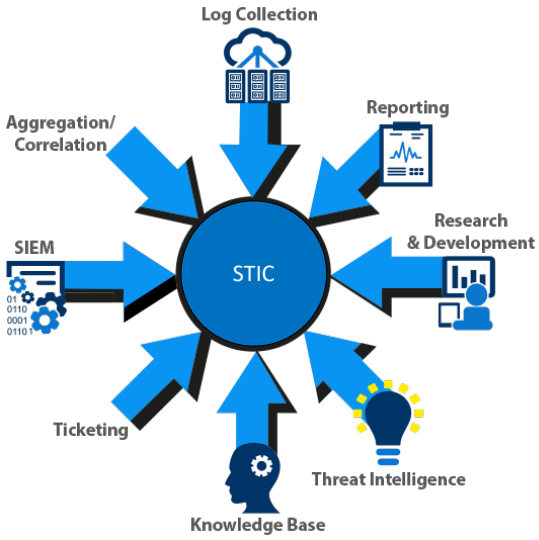
A STIC goes beyond a traditional SOC/SIEM service by incorporating the concepts of threat hunting, compliance management, penetration testing, training and awareness management, and more.

Services envisioned:

The STIC may include, but may not be limited to, providing the following services:

- Security auditing, monitoring, and event correlation.
- Network traffic analysis.
- Security incident response management (both automated and manual).
- Security device and platform management and maintenance.
- Threat and vulnerability management.
- Threat intelligence analysis and threat hunting.
- Security compliance management.
- Malware analysis.
- Forensic analysis.
- Risk analytics and attack path modeling.
- Countermeasure implementation.
- Remediation prioritization and coordination.
- Penetration testing.
- Security awareness training.
- Virtual CISO (vCISO) services.

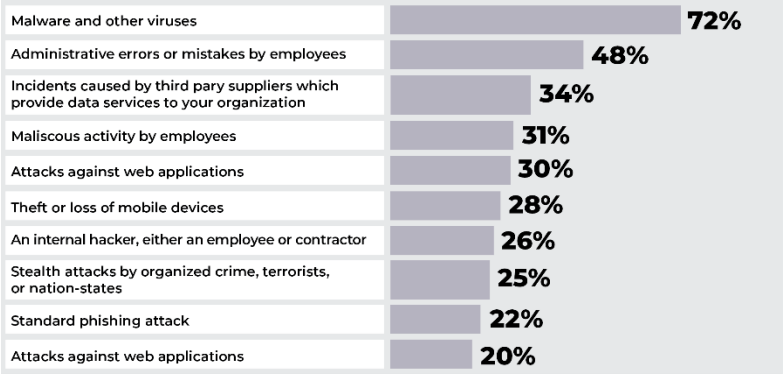
Figure 1: Conceptual Inputs to STIC



Why does the state of Washington need a statewide STIC?

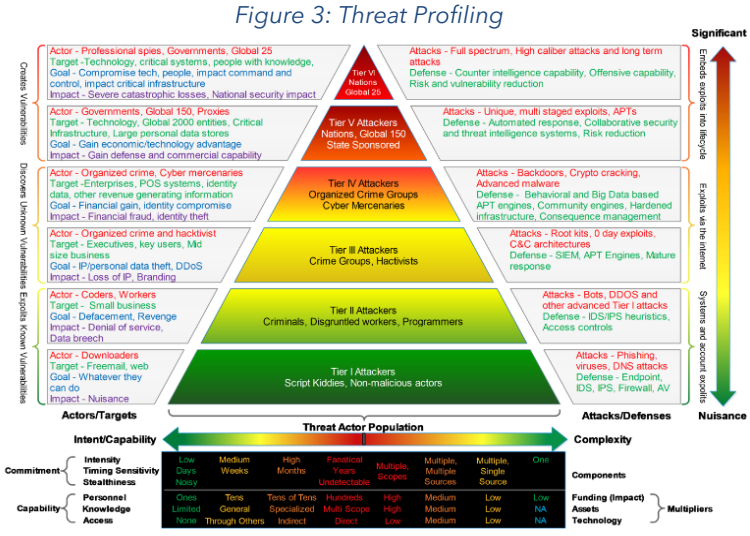
Cybersecurity risk management is the continuous process of minimizing and preventing internal and external threats from exploiting weaknesses in an organization's information technology systems, devices, processes, and infrastructure, benefiting all stakeholders who depend on these technologies. Figure 2 displays several common exposures facing organizations. Without a STIC, these are siloed within individual organizations, providing incomplete visibility, which leads to a weak security posture statewide.

Figure 2: Potential Exposures to an Organization



This also prevents proper profiling of organizations' threats, as depicted in Figure 3.

Figure 3: Threat Profiling



According to the 2018 Verizon Data Breach Investigation Report, "In 87% of cases, attackers can compromise an organization within minutes".[5] According to IBM, an organization takes 197 days to discover a breach and up to 69 days to contain it.[6]Waiting to react to a breach until after the damage has been done leads to an extremely costly recovery and loss of public trust. IBM also states that the average cost of a breach has reached an all-time high. In 2022, the data breach cost averaged $4.35 million, a 2.6% increase from 2021.[7]

The existing separation of municipalities' siloed and isolated monitoring systems, where such capabilities even exist, results in organizations functioning in a reactive, independent, isolated, and uncoordinated manner in relation to cyber events. With a properly designed, implemented, and operated statewide STIC offering services to municipal entities, the state and all participants could be more proactive, resolving discovered issues before a threat actor can take advantage of them, supporting a whole-of-state strategy.

[5] Verizon 2018 Data Breach Investigations Report

[6] Veronis report "Data Breach Response Times: Trends and Tips"

[7] IBM 2022 Report 29 July 2022 "Cost of a Data Breach at an All-Time High"

Why should local municipalities participate in the statewide STIC?

Municipalities should consider the following questions when evaluating their need to participate in the STIC:

With existing tools and technologies

- Can a compromise be detected?
- How can the severity of the compromise be judged?
- What is the magnitude and impact of the compromise?
- Who is responsible for detecting and reacting to a compromise?
- Who should be informed or involved, and how rapidly will a compromise be addressed once detected?
- How and when should a compromise be communicated internally or externally?

These questions are designed for leadership to consider the impact of an incident and judge their existing cybersecurity processes, controls, programs, and capabilities. If any of these questions cannot be adequately answered to the satisfaction of the entity's leadership, participation in the STIC should be a consideration.

Benefits to the state of Washington and its municipalities of creating a statewide integrated STIC include, but may not be limited to, the following:

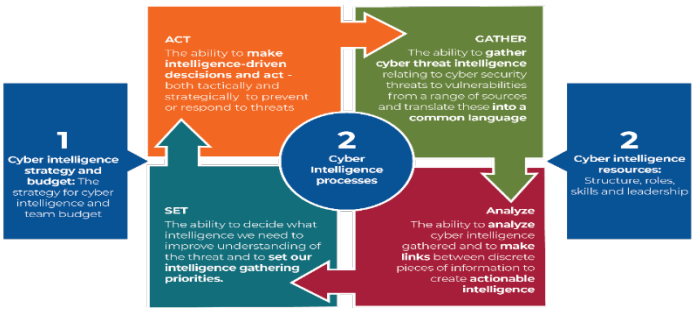
- Improved protection of critical information assets, infrastructure, and services.
- Improved threat management: By providing an accurate view of security, we can ensure more efficient and effective detection and response to cybersecurity threats.
- Minimize the impact and magnitude of successful cybersecurity attacks by reducing the time between attack, detection, and response.
- Help to improve compliance with regulatory requirements (e.g., the Health Insurance Portability and Accountability Act (HIPAA), the FBI's Criminal Justice Information Services (CJIS), the Payment Card Industry (PCI), etc.).
- Reduce financial, legal, regulatory, and reputational risk.
- Consolidating security functions to help achieve cost efficiencies, cost sharing, and economies of scale while maximizing expertise, skills, and resources. Incorporating organizational telemetry into the STIC platform is essential.
- The capability to exchange Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) with other local and national areas. Given the right tools, framework, and agreements, the STIC and Washington could also share and receive these indicators from those entities.

- Increased visibility into attempted and successful cyber-attacks that may otherwise go undetected; external entities identify 70% of all cyber-attacks against organizations[8].

Scope

The STIC must have a statewide enterprise view encompassing all state agencies and municipalities to succeed. Today, statewide visibility is fragmented jurisdictionally. The state is only as strong as its weakest link; lack of visibility into jurisdictions eliminates the possibility that IoCs or IoAs will be identified and addressed.

Figure 2: Intelligence Lifecycle



Design Principles

Establishing a statewide STIC with a focus on whole-of-state, emphasizing collaboration and coordination across all government agencies and municipal entities within the state, requires the establishment of goals, objectives, and requirements. Here are some goals, objectives, and requirements to consider:

Goals

1. **Enhanced cybersecurity resilience:** Strengthen the cybersecurity posture of the entire state infrastructure to effectively defend against cyber threats and minimize the impact of security incidents.
2. **Improved incident response coordination:** Establish seamless collaboration and coordination mechanisms among state agencies and municipalities to ensure a rapid and coordinated response to cybersecurity incidents, thereby reducing response times and mitigating damages.
3. **Proactive threat detection:** Implement advanced threat detection capabilities to identify and respond to emerging cyber threats in real-time, minimizing the likelihood and impact of successful cyberattacks.
4. **Comprehensive threat intelligence sharing:** Facilitate sharing threat intelligence and cybersecurity best practices among state agencies and municipal entities, enabling proactive threat mitigation and improving overall cybersecurity readiness.
5. **Enhanced compliance and regulatory alignment:** Ensure that state agencies and participating municipal entities adhere to relevant cybersecurity regulations, standards, and best practices,

[8] Microsoft Security Insider Threat Brief, October 2023

thereby fostering trust and confidence in their ability to protect sensitive data and critical infrastructure.

Objectives

1. **Establishment of a centralized STIC:** Create a centralized service that monitors, analyzes, and responds to cybersecurity threats across the entire state infrastructure.
2. **Interagency collaboration framework:** Develop a framework for interagency collaboration, including information-sharing protocols, incident response procedures, and communication channels to facilitate coordinated cybersecurity efforts.
3. **Implementation of advanced security technologies:** To enhance threat detection and incident response capabilities, deploy advanced security technologies such as SIEM platforms, threat intelligence feeds, endpoint detection and response (EDR) solutions, and network intrusion detection/prevention systems (NIDS/NIPS).
4. **Cybersecurity training and awareness programs:** Provide comprehensive cybersecurity training and awareness programs for participating entity personnel to ensure all employees have the knowledge and skills necessary to identify and respond to cyber threats effectively.
5. **Continuous improvement and evaluation:** Establish mechanisms for continuous improvement and evaluation of SOC operations, including regular assessments, performance metrics, and feedback mechanisms to optimize processes and enhance effectiveness over time.

Requirements

1. **Centralized infrastructure:** Establish a dedicated facility with the necessary services, hardware, software, and personnel to support STIC operations, including monitoring, analysis, and incident response activities.
2. **Secure data sharing platform:** Implement a secure data sharing platform to facilitate the exchange of threat intelligence and cybersecurity-related information among participating entities while ensuring confidentiality, integrity, and availability of shared data.
3. **Vendor-neutral platform:** Implement a platform to facilitate the ingestion of cybersecurity-related telemetry from diverse sources from participating entities, ensuring that participating entities are not required to replace expensive equipment to participate.
4. **Access control and privileged account management:** Implement robust access control and privileged account management mechanisms to restrict access to sensitive systems and data, reducing the risk of insider threats and unauthorized access.
5. **Incident response playbooks:** Develop comprehensive incident response playbooks outlining predefined procedures, roles, and responsibilities for responding to various types of cybersecurity incidents, ensuring a consistent and coordinated response.
6. **Regular training and exercises:** Conduct regular cybersecurity training sessions and simulated exercises to test STIC capabilities, improve incident response readiness, and ensure that personnel are well-prepared to handle cybersecurity incidents effectively.

7. **Regulatory compliance:** Ensure compliance with relevant cybersecurity regulations, standards, and frameworks applicable to government agencies, including, but not limited to, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, HIPAA, CJIS, etc.
8. **Continuous monitoring and threat intelligence integration:** Implement continuous monitoring capabilities to detect and respond to cybersecurity threats in real time, integrating threat intelligence feeds from external sources to enhance threat detection accuracy and efficacy.
9. **Executive support and funding:** Secure executive sponsorship and adequate funding to support the establishment and ongoing operations, including personnel, technology investments, and training initiatives.

By aligning goals, objectives, and requirements with the whole-of-state concept, the statewide STIC can effectively leverage collaboration and coordination among state agencies and participating municipal entities to enhance cybersecurity resilience and protect critical assets and infrastructure throughout the state.

Technology

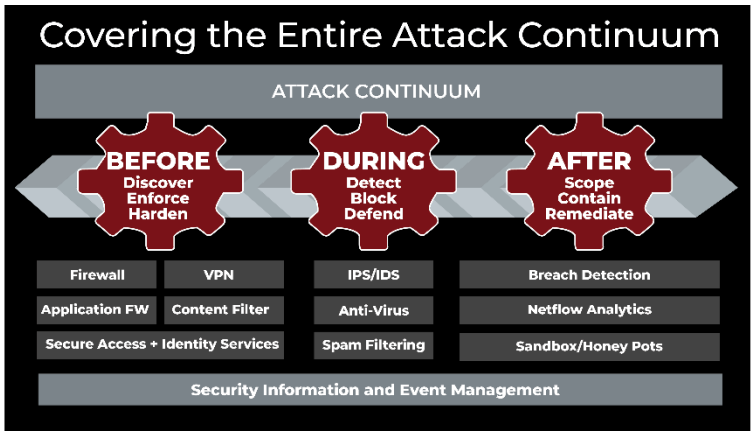
Services described here are typically based on a Security Information and Event Management (SIEM) system. SIEMs aggregate and correlate data from security feeds, creating a centralized view from which security analysts can monitor networks and systems. Other technologies and capabilities such as Network Behavioral Analysis, Intrusion Detection and Prevention (IDS/IPS), Extended/Endpoint Detection and Response (XDR/EDR) that need to be evaluated and considered to support the STIC include:

- **Asset Discovery**
  - Active and Passive Network Scanning
  - Asset Inventory
  - Host-Based Software Inventory
- **Network Traffic Monitoring**
  - Threat Activity Monitoring
  - Network Performance Telemetry
- **Vulnerability Assessment**
  - Host and Network Vulnerability Testing
  - External Attack Surface Monitoring
  - Application Vulnerability Testing
- **Endpoint Detection and Response**
  - Anti-malware detection
  - Host Intrusion Detection and Prevention Systems (IDS/IPS)
  - File Integrity Monitoring

- **Network Threat Detection**
  - Network Intrusion Detection and Prevention Systems (IDS/IPS)
  - Wireless Intrusion Detection and Prevention Systems (IDS/IPS)
  - Web Application Firewalls (WAF)
- **Behavioral Monitoring**
  - Log Collection
  - NetFlow Analysis
  - User Behavior Analytics
  - Service Availability Monitoring
- **Security Intelligence**
  - SIEM Correlation
  - Threat Intelligence platform
  - Incident Response platform
- **Identity**
  - Active Directory / Azure AD or Lightweight Directory Access Protocol (LDAP)
  - Remote Authentication Dial-in User Service (RADIUS)
  - Network Access Control (NAC)

There are many flavors of security technologies; however, best practice involves ensuring the approach chosen leverages layered capabilities so that if a defense measure fails to *detect* an attack, another measure is available to help *prevent* the attack. Figure 5 to the right depicts an example of technologies designed to address different parts of the attack continuum.

Figure 3: Defense in Depth



People

STIC staff typically includes analysts, security engineers, and managers who should be seasoned information technology and network security professionals. Skillsets and ongoing training are critical to the success of an STIC; staff should be skilled, trained, and certified in areas such as incident response, cyber forensics, cryptography, network engineering, and application security.

A staffing plan must be developed based on defined goals, objectives, and requirements of the STIC. For example, does the STIC need to be staffed 24x7 or 5x8? The requirements of the participating entities will be the primary driver for the staffing model. Service levels, including response time expectations, must also be developed based on defined incident severity levels. This will significantly impact the number and composition of staff needed to support the STIC.

Process

STIC functions, processes, and procedures must be formally defined, including clearly spelled-out roles, responsibilities, and escalation profiles. These processes include business, technology, operational, and analytical processes. They will outline the steps to be taken in the event of an alert, including escalation, reporting, and response procedures.

Facilities

Figure 4: Typical Intelligence Center

The physical facilities of the STIC must be well-protected with physical, electronic, computer, and personnel security safeguards. Such facilities are often dedicated and purpose-built to enable operational security. Due to the sensitive nature of incident investigations and the potential for tampering with evidence and obfuscation of malicious tracks, physical access to the facility is restricted to authorized personnel only. The command control infrastructure should be heavily segmented away from the production network to prevent internal breaches affecting the operations of the STIC. Ideally, the STIC's technology infrastructure for monitoring and investigations should be isolated and separated from the Internet. Finally, the STIC will often have independent internet connectivity to continue to operate and perform investigations even if the network is compromised.

Traditional facilities were often laid out with desks facing a video wall, which displayed significant status, events, alarms, and ongoing incidents. A corner of the wall is frequently used to display news or weather television broadcasts. These broadcasts are intended to keep the STIC staff aware of current events that may affect information systems. Security engineers and analysts generally have multiple computer monitors on their desks.

With the proliferation of remote work since the COVID-19 pandemic, such facilities have become significantly more distributed without affecting analyst performance.

Metrics

Metrics for the STIC operations must be established, tracked, and reported. Detection rates, time to detection, open tickets per analyst, and ticket closure rates are some potential metrics.

Funding

Sustainable funding for the first two to five years of STIC operation is essential. It is expected that sufficient municipalities will adopt the service for the STIC to become self-sustaining, which will take two to five years. Approximately the first two years will be spent establishing the services, people, processes, and technology to be "embedded" and delivering results reasonably proficiently.

Organization of the statewide STIC

Several models could be considered for the organization of the proposed statewide STIC. These models include, but may not be limited to:

- State managed and operated.
- Managed and operated independently from the state, with enterprise involvement.

State-managed and operated

As Arizona, New York, and North Dakota have done, cities and towns could join the state's STIC and get the same services that state agencies use. This model offers several advantages. However, considering the current state of the SOC environment, the negatives likely outweigh these advantages.

The advantages include:

- Accelerated onboarding and adoption.
- State staff are familiar with the existing technology.
- The managed security services provider is already under contract.
- Successful onboarding of municipalities into the existing state SOC can enhance WaTech's reputation as a service provider, leading to more opportunities for growth.
- Working with new municipal clients would expose WaTech staff to different technologies and challenges, providing valuable learning opportunities that can be applied to future projects.
- Bringing in municipalities may create opportunities to scale existing services, allowing WaTech to invest in infrastructure, personnel, and processes to support growth.

Obvious disadvantages include:

- The existing SOC was designed to meet the needs of state agencies. Therefore, it is unlikely that all municipalities could seamlessly integrate.
- The current state SOC was not established to meet this document's goals, objectives, and requirements.
- The current infrastructure is not sufficiently vendor agnostic.
- Costs could be prohibitive for many smaller municipal entities.
- Reluctance on the part of municipalities to participate. Their perceptions would focus on the state's needs being served above theirs.
- As it exists currently, the state SOC does not provide all the services outlined in this document.
- Onboarding new clients, such as municipal entities, requires significant time, effort, and resources, which can strain the existing team and infrastructure, especially if the growth is rapid.

- Maintaining consistent service quality across a growing client base can be challenging, particularly if the current team struggles to meet increased demand.
- Managing multiple municipalities with different needs, priorities, and expectations can increase the complexity of operations, leading to potential inefficiencies and conflicts.
- Not all municipalities may align with WaTech's values, culture, or working practices, leading to potential conflicts or dissatisfaction.

Managed and operated independently from the state, with enterprise involvement.

This model would be unique to state implementation, necessitating considerable involvement, supervision, and financial backing. In this model, the state would be a significant participant in the STIC as a peer participant rather than the "owner/manager." As with any model, this one also provides advantages and disadvantages.

Some advantages include:

- This model does not have preconceived assumptions. Essentially, it would be a greenfield approach. The STIC can be designed to meet the goals, objectives, and requirements outlined in this document and any others that the community of municipalities wishes to include.
- The model could be created in collaboration with municipalities, increasing adoption.
- As a greenfield implementation, participants would be free to design and implement STIC services according to the needs and requirements of participating entities without being limited by legacy systems or outdated technologies.
- Starting from scratch allows for a scalable infrastructure that can easily accommodate future growth and expansion without significant reengineering or retrofitting.
- Greenfield projects allow leveraging the latest technologies, methodologies, and best practices, fostering innovation.
- Streamlined processes could be established from the outset. Optimized processes and workflows can be designed and developed as a completely new service, eliminating inefficiencies in older systems and improving overall operational efficiency.

The disadvantages are:

- It will take longer to adopt managed security services due to the need to establish a suitable environment since extensive planning, development, and testing phases would be involved.
- The cost of the establishment may be higher than other alternatives.
- The absence of existing infrastructure means no proven solutions or precedents to follow, increasing the risk of project failure or delays.
- Greenfield projects require specialized knowledge and expertise in designing and implementing complex IT systems, which may not be readily available within the state or participating municipalities and may need to be sourced externally.

Service Design

As the service is designed, certain services should be considered essential. These essential services could include:

- SOC/SIEM Monitoring, alerting, and triage. This could include automated event response based on the escalation profile established by the participating entity.
- Vulnerability and External Attack Surface Management platform. This implementation would not necessitate the participating municipality abandoning existing technology but incorporating the resulting information from existing platforms into a standardized analysis and prioritization platform.
- Network behavior analytics.
- Extended/Endpoint Detection and Response (XDR/EDR). This aspect could include providing the XDR/EDR platform or using the participating municipality's existing platform.
- Incident response assistance.
- Forensic analysis assistance.

As an essential service to all participating municipalities, the STIC would have consistent telemetry, resulting in consistent correlation and alert response capabilities.

Other services could be considered "optional," such as Virtual CISO (vCISO) and penetration testing services, which could be provided on an "as needed" basis.

Funding Models

Initial funding

In states such as Arizona, New York, and North Dakota, where such services have been established, the legislature provided initial funding. A similar method should be strongly recommended for expediency and potential success.

Long Term Funding

For the states previously mentioned, the legislature also provides long-term funding to maintain the service to municipalities. In the case of Arizona, the legislature has allocated $10 million annually to provide SOC services to all municipalities that wish to participate; no municipality is charged an annual fee. However, the Arizona model is established by the state, with municipalities having little to no input into the services provided.

In Washington, a more flexible funding model is envisioned. Washington would prefer to have input from participating municipalities in designing and providing beneficial services to each participating entity. To that end, the following funding models are put forth.

Fully state-funded

As Arizona has done, the legislature could provide earmarked funds to provide STIC services to all state municipalities. This could become costly as more municipalities become participants. This model would also require clear scoping related to which categories of municipalities were eligible to participate (i.e., cities, counties, Tribal nations, educational institutions, special service districts, etc.).

Per ingestion/per FTE model

This is the most straightforward model for determining funding. Each participating entity would be charged annually based on its full-time equivalent (FTE) staffing and monthly for the capacity of the telemetry incorporated into the system. Vendors currently providing such services commonly use such billing models.

Tiered model

A subsidized tiered model could be established. This model could be based on aspects of the per ingestion/per FTE model described above but subsidized by the state. Smaller entities with fewer resources (i.e., staffing, funding, etc.) could be fully subsidized by the state. Mid-range participants could pay partially subsidized fees. Large entities could pay the entire fee structure for the services. Multiple tiers could be established.

This could be a complex model to manage. However, such a scheme could better support the smaller municipalities. As with the fully state-funded model, clear scoping related to entity category participation would be essential.

Conclusion

As we stand on the threshold of a new era in cybersecurity within Washington state, establishing the Strategic Threat Intelligence Center (STIC) marks a pivotal moment in our collective efforts to safeguard our digital frontiers. This document shows the importance of adopting a whole-of-state approach to cybersecurity, emphasizing the necessity and urgency of collaborative defense strategies.

The STIC will streamline threat intelligence, enhance cybersecurity response mechanisms, and foster a culture of shared vigilance and proactive defense across state agencies, municipalities, educational institutions, and beyond. By pooling resources, sharing intelligence, and coordinating responses, we are not just fortifying individual entities but reinforcing the security posture of Washington state.

The STIC represents a foundation to build on. The path forward requires sustained commitment, ongoing collaboration, and the willingness to innovate and adapt. As cyber threats evolve, so too must our strategies and defenses.

Moving forward, we must work together to operationalize the STIC and ensure it becomes an integral part of our cybersecurity infrastructure. This involves not just the technical implementation but also fostering a culture of cybersecurity awareness and preparedness across the state.

Together, as a state, we stand on the precipice of change, ready to embark on a collective mission to secure our digital future. The Strategic Threat Intelligence Center represents a bold step forward in this mission, a testament to Washington state's commitment to cybersecurity excellence.