Commonwealth Office of Technology
Finance & Administration Cabinet

Budget Review Subcommittee on General Government, Finance, Personnel, and Public Retirement

David Carter, CISO
August 17, 2022

Security Approach

Based on Industry Trusted and Proven Frameworks

Security Program Frameworks

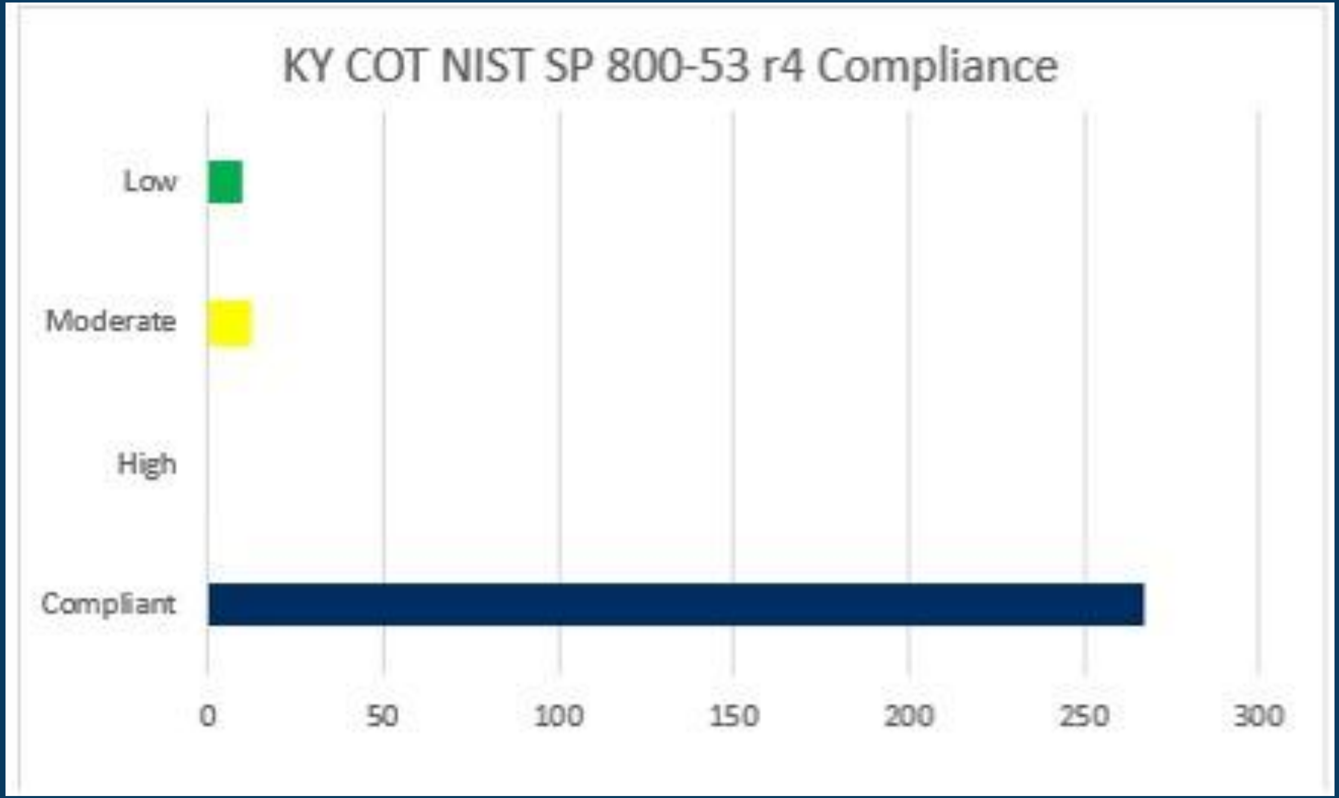
MITRE | ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

NIST
SP 800-53
Revision 4

NIST SP 800-53 is a comprehensive risk management framework that defines a set of standards for information security policies and technical controls for government agencies. It was created to heighten the security (and security policy) of information systems used in government operations. This framework spans 18 control families and 212 individual base controls.

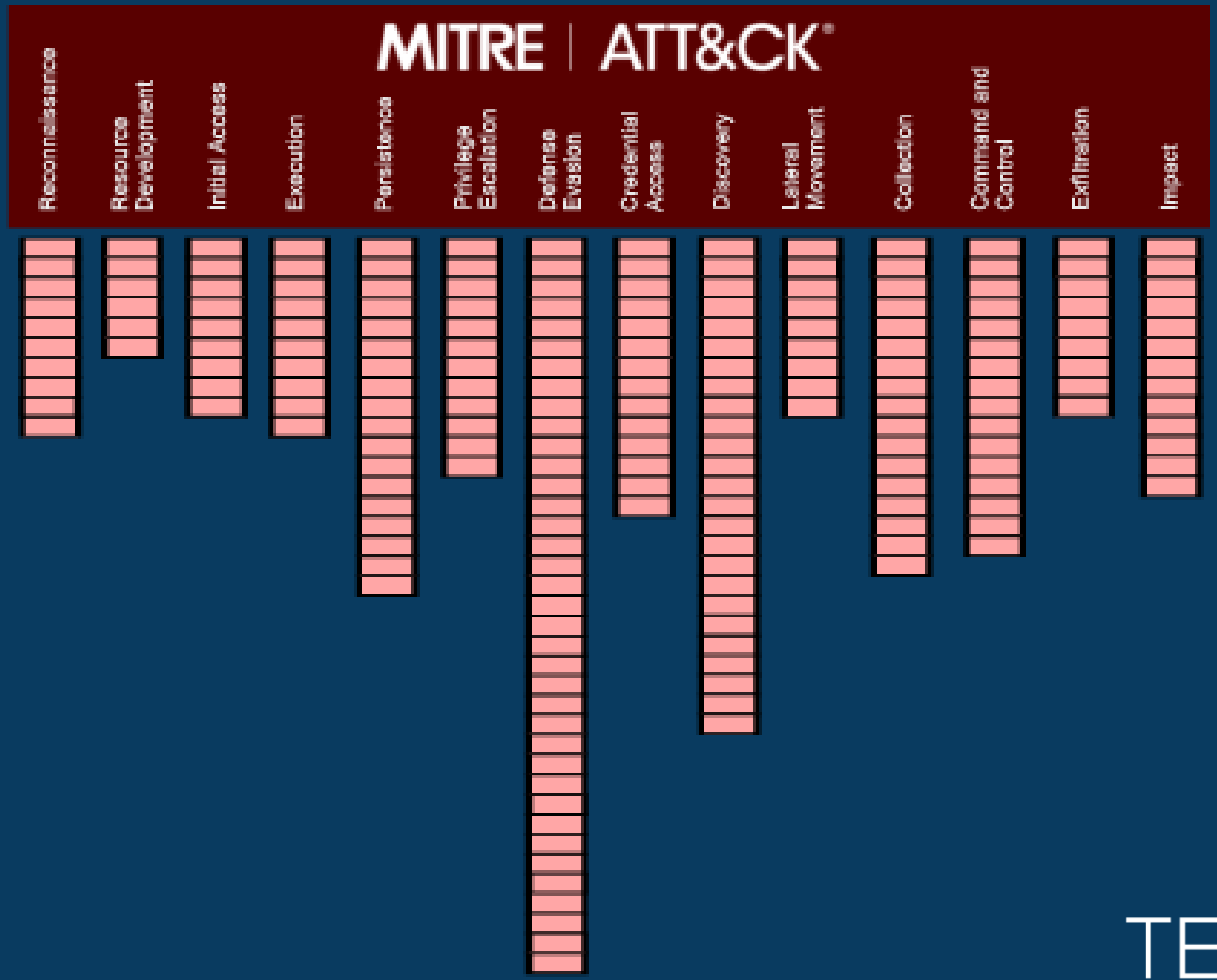
NIST 800-53 Framework Compliance



MITRE ATT&CK Framework Coverage

Where We Were

2018

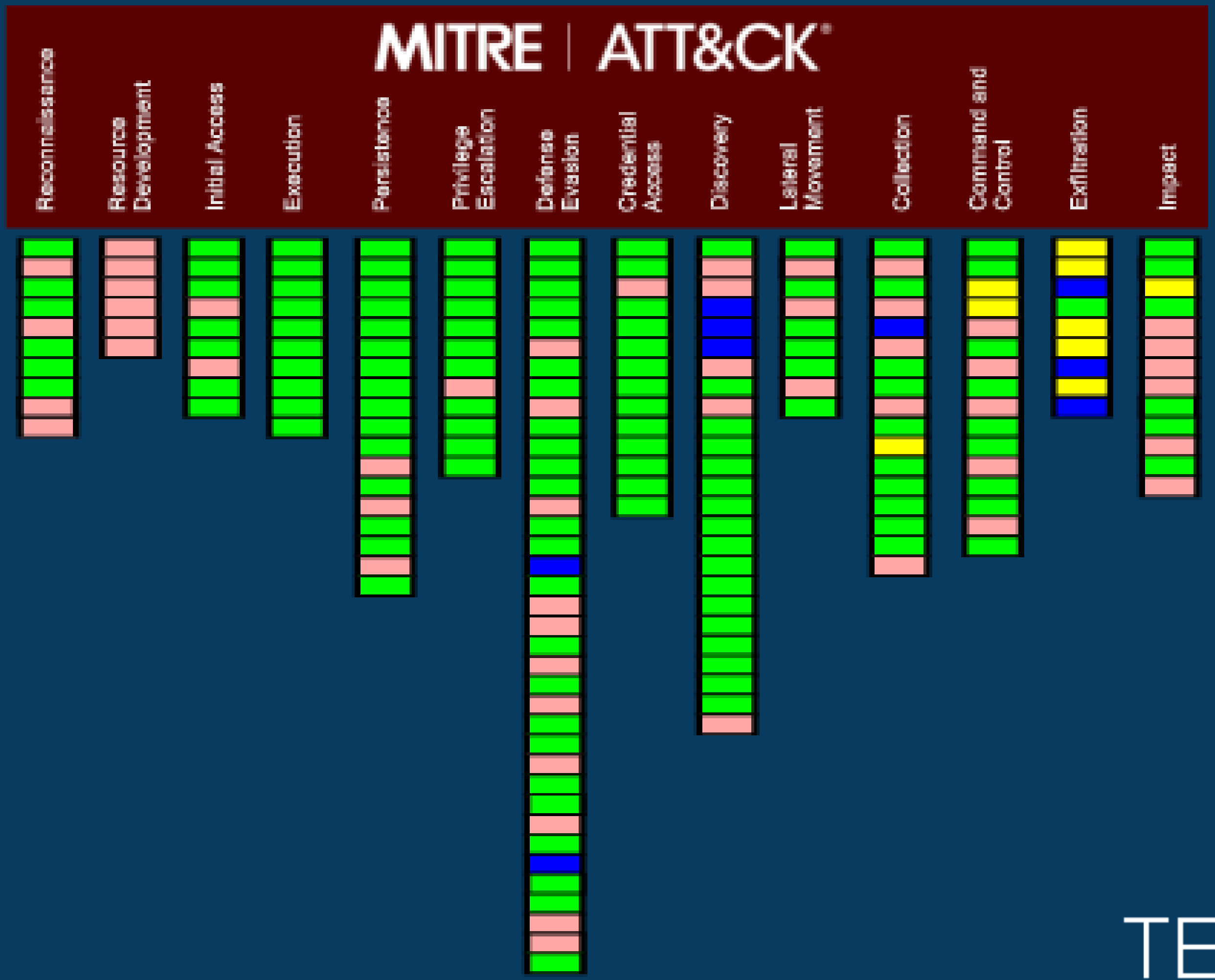


TEAM KENTUCKY™

MITRE ATT&CK Framework Coverage

2022+

Tactical (Blue) and Strategic (Yellow) Initiatives in the Strategic Plan



TEAM KENTUCKY™

Layered Security

Security Applied in a Serial Fashion

Layered Security

Employee

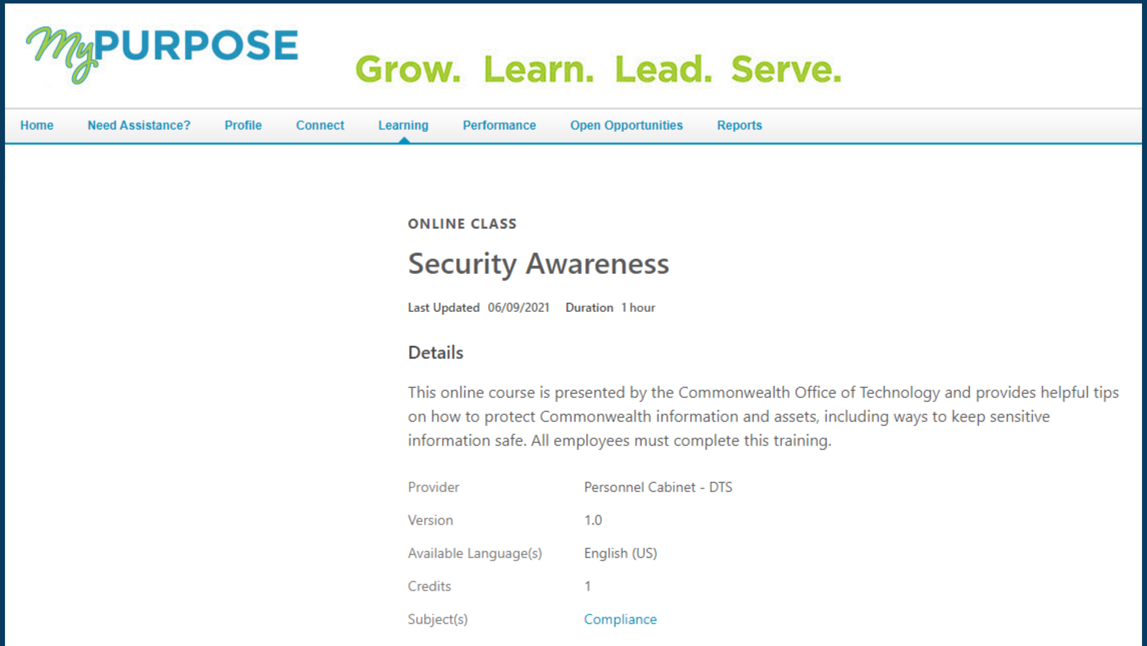
Network

Endpoint

Data

Employee Awareness - Training

In partnership with the Personnel Cabinet, the Commonwealth Office of Technology has established comprehensive security awareness training for all employees which has been incorporated into the onboarding and annual performance evaluation processes within the Executive Branch.



ONLINE CLASS

Security Awareness

Last Updated 06/09/2021 Duration 1 hour

Details

This online course is presented by the Commonwealth Office of Technology and provides helpful tips on how to protect Commonwealth information and assets, including ways to keep sensitive information safe. All employees must complete this training.

Provider	Personnel Cabinet - DTS
Version	1.0
Available Language(s)	English (US)
Credits	1
Subject(s)	Compliance

Employee Awareness - Phishing

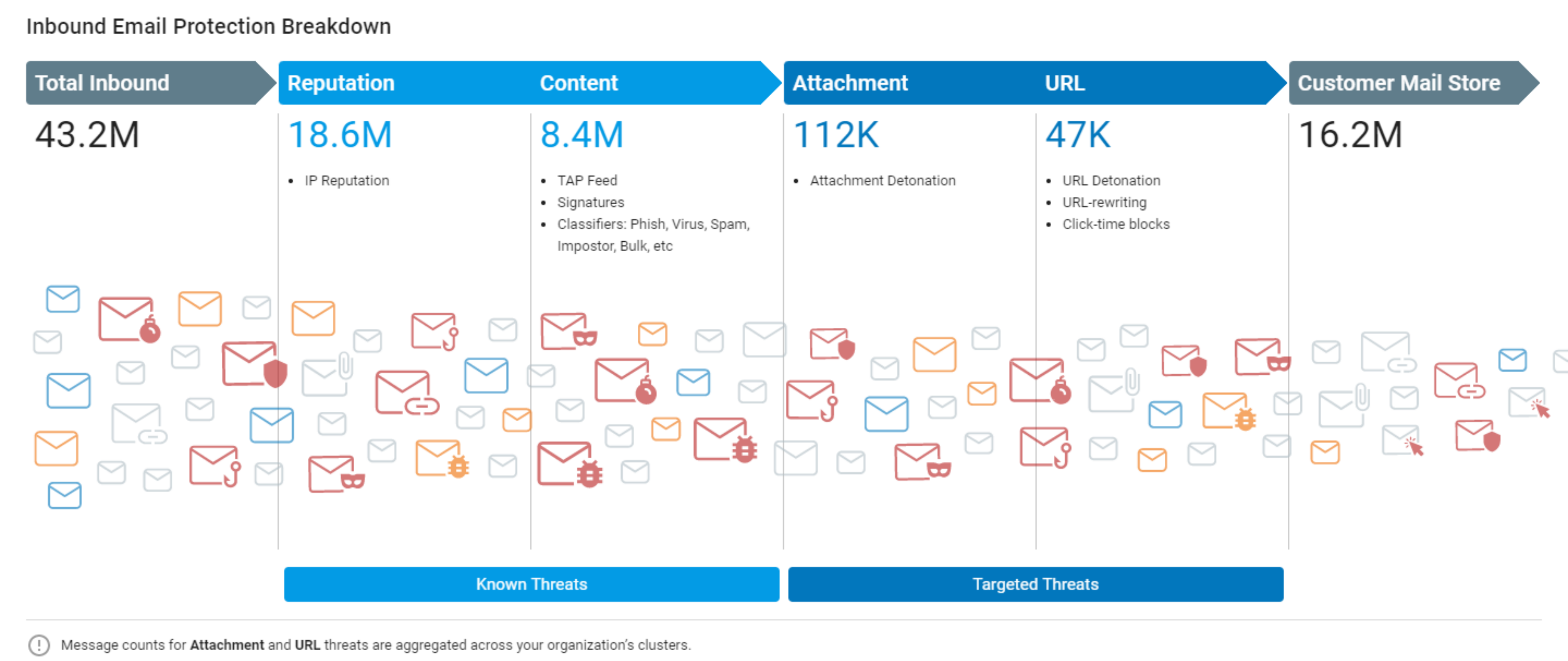
Phishing, the sending of emails by a bad actor to achieve system compromise, is the number one vector by which threats enter a computing environment. In early 2021, the Office of the CISO implemented an enterprise-wide phishing awareness program that sends phishing emails to all employees. Should employees fall victim to the phishing email, they are redirected to a 'teaching moment' to help educate them on what to watch out for. At the onset of this program, failure rates exceeded 12% but we have maintained steady improvement since inception.

Phishing Awareness Facts

- 93% of all attacks involve phishing at some stage.
- Estimates range between 45%, and up to 75%, of all email sent worldwide is SPAM or malicious.
- Industry average phishing click failure rate for government organizations is 11%, we are currently at 3.28% statewide average this quarter.
- The phishing click failure rate for the Commonwealth is better than 97% of organizations that use our phishing awareness vendor globally.

Email Defense

62.5% of All Email Destined for the Commonwealth is Blocked for Content or Reputation



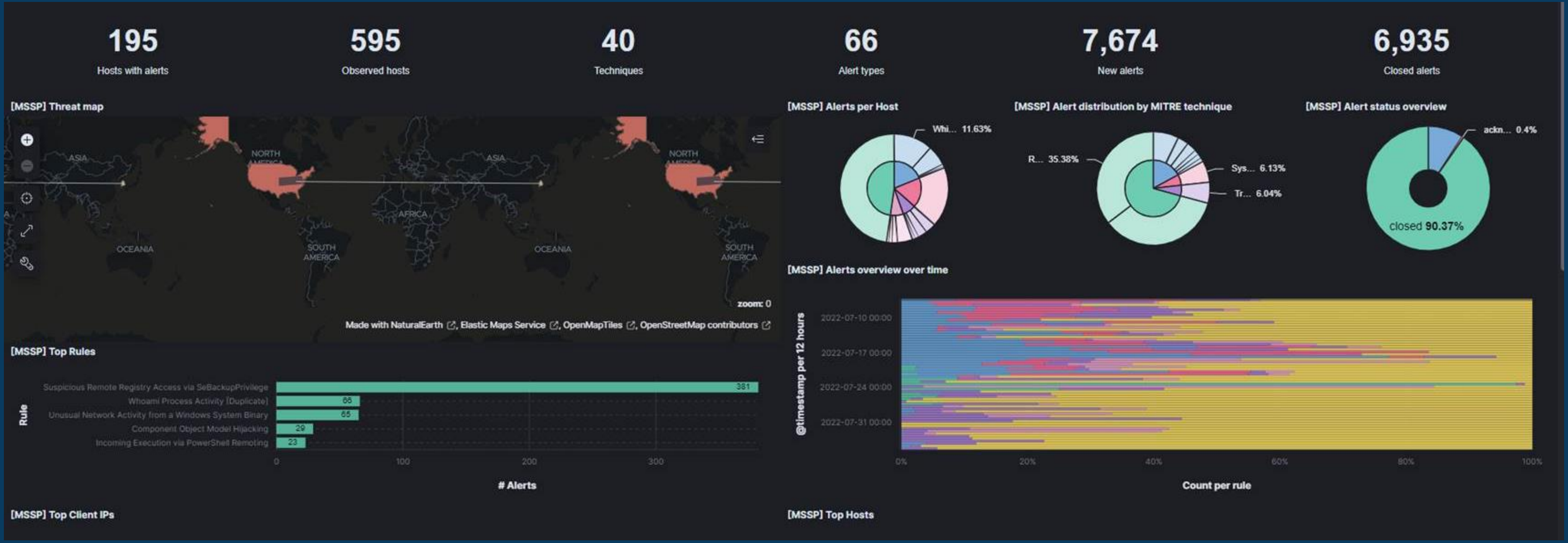
Inbound Email Protection Breakdown

Total Inbound	Reputation	Content	Attachment	URL	Customer Mail Store
43.2M	18.6M	8.4M	112K	47K	16.2M
	• IP Reputation	• TAP Feed • Signatures • Classifiers: Phish, Virus, Spam, Impostor, Bulk, etc	• Attachment Detonation	• URL Detonation • URL-rewriting • Click-time blocks	

Message counts for **Attachment** and **URL** threats are aggregated across your organization's clusters.

Network Defense

The Commonwealth has in place an advanced Security Incident and Event Management System (SIEM) that provides effective analytics to reduce noise to allow security analysts to focus on real threats can have a potential impact. This also allows data to be trended and correlated to link related events, which in turn allows the Commonwealth to constantly tune and improve defenses.



195 Hosts with alerts

595 Observed hosts

40 Techniques

66 Alert types

7,674 New alerts

6,935 Closed alerts

[MSSP] Threat map

[MSSP] Alerts per Host

[MSSP] Alert distribution by MITRE technique

[MSSP] Alert status overview

[MSSP] Alerts overview over time

[MSSP] Top Rules

[MSSP] Top Client IPs

[MSSP] Top Hosts

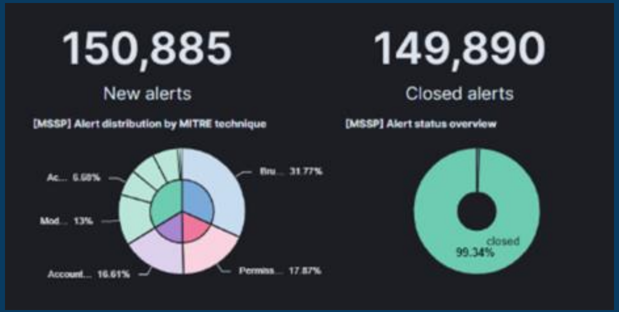
Made with NaturalEarth, Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

Network Defense

Continuous enhancement and tuning allows us to bring in more data while maintaining the highest level of effectiveness in identifying actionable intelligence. The captures below show that evolution as we enhance the quality and amount of data brought in for analysis and the investment made in tuning to ensure that we have focus on the items that matter most.

Starting Point

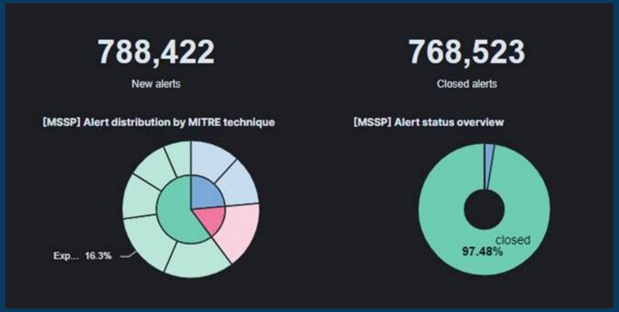
This is the SIEM Data before the addition of critical infrastructure logs beyond just the security architecture.



90 Days

Enhanced Visibility

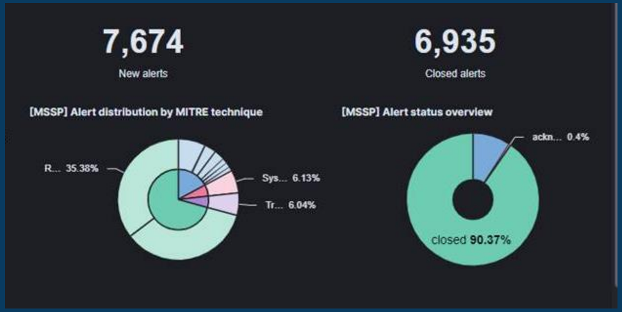
After inclusion of critical infrastructure logs that give us a holistic view of the computing environment as a whole.


788,422
New alerts
768,523
Closed alerts
[MSSP] Alert distribution by MITRE technique
Exp... 16.3%
[MSSP] Alert status overview
closed
97.48%

90 Days

Tuning for Effectiveness

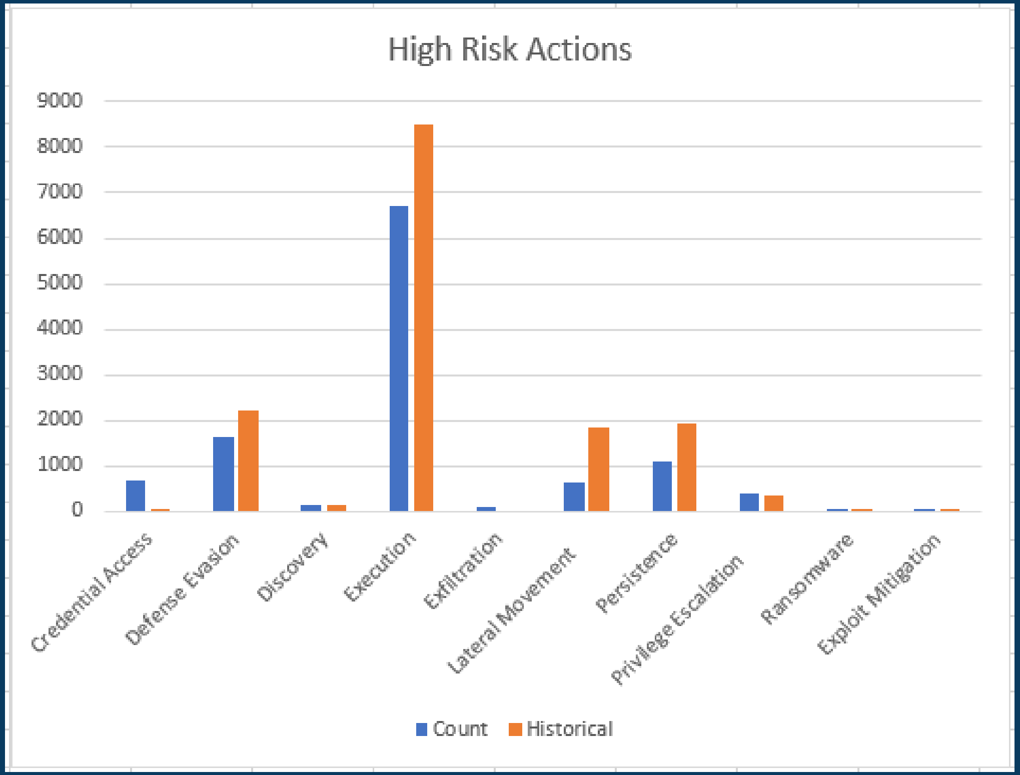
After applying advanced analytics and tuning of the system to reduce noise and eliminate noise and items already mitigated proactively.



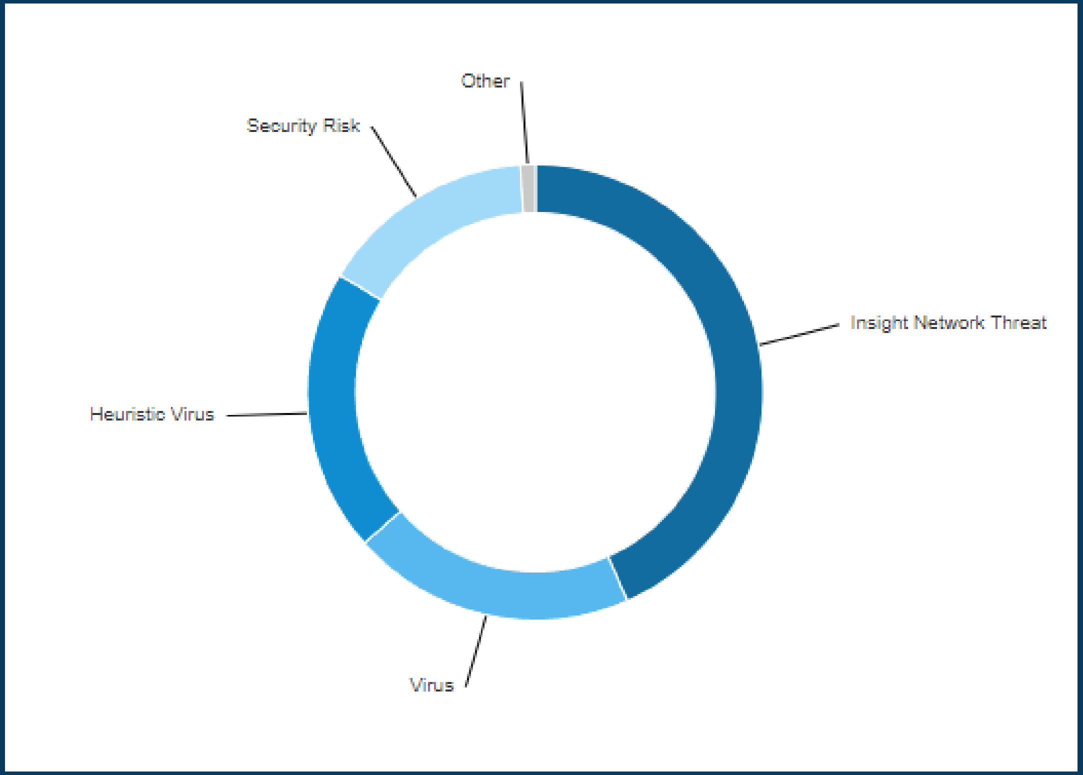
30 Days

Endpoint Defense

Endpoint Response Defenses



Malicious Code Defenses

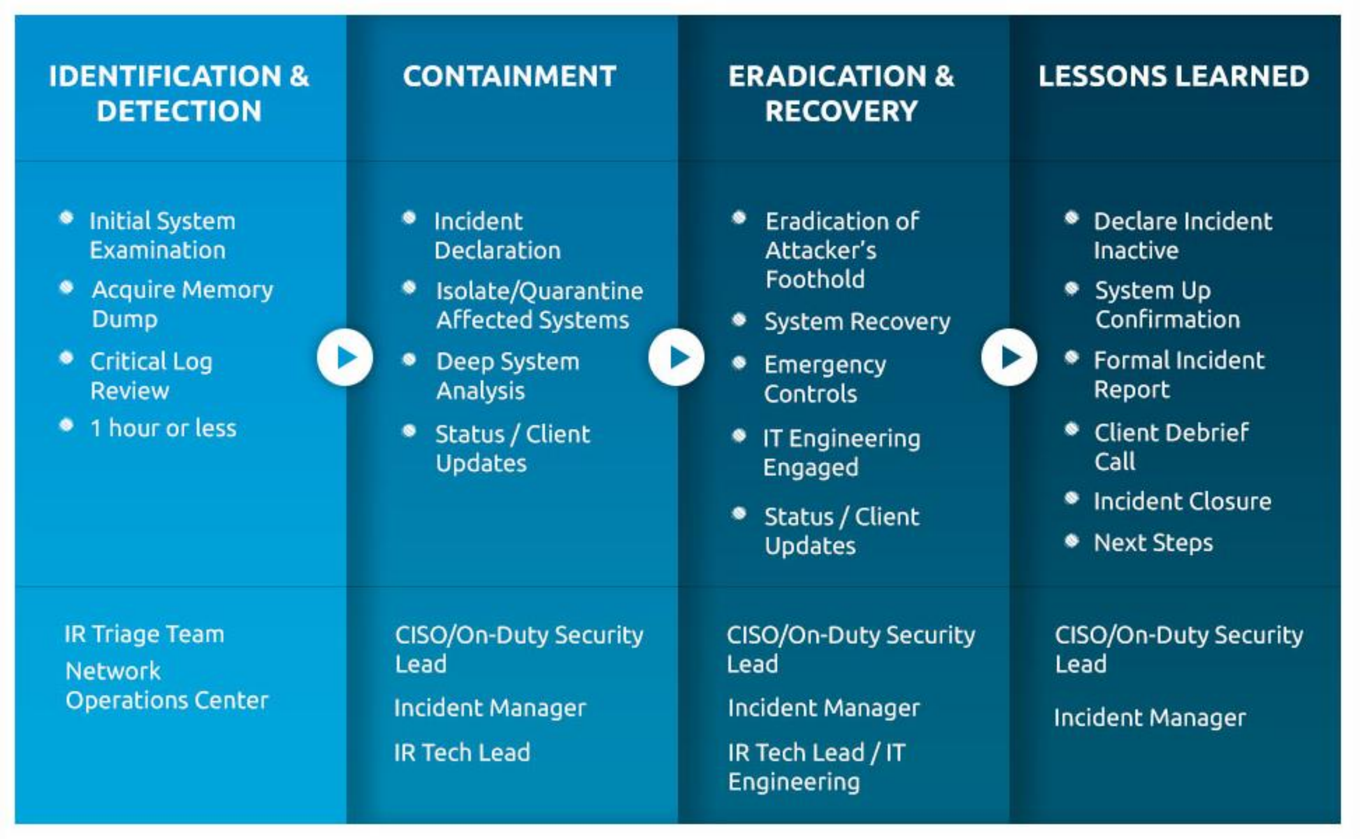


Incident Response

Strength in Planning

Incident Response

COT has in place a mature incident response plan that encompasses the entire incident response life cycle. To ensure effectiveness, the plan is tested at least annually to ensure staff and processes are tuned and effective when a real event occurs.



IDENTIFICATION & DETECTION	CONTAINMENT	ERADICATION & RECOVERY	LESSONS LEARNED
• Initial System Examination • Acquire Memory Dump • Critical Log Review • 1 hour or less	• Incident Declaration • Isolate/Quarantine Affected Systems • Deep System Analysis • Status / Client Updates	• Eradication of Attacker's Foothold • System Recovery • Emergency Controls • IT Engineering Engaged • Status / Client Updates	• Declare Incident Inactive • System Up Confirmation • Formal Incident Report • Client Debrief Call • Incident Closure • Next Steps
IR Triage Team Network Operations Center	CISO/On-Duty Security Lead Incident Manager IR Tech Lead	CISO/On-Duty Security Lead Incident Manager IR Tech Lead / IT Engineering	CISO/On-Duty Security Lead Incident Manager

The Strategic Plan

Continuous Improvement

Looking Forward – The Strategic Plan

- Enhanced Monitoring

  Introducing advanced security technologies to allow greater visibility and analytic capabilities. Items such as network traffic decryption and advanced threat hunting capabilities will enhance the data currently available for analysis. This will result in faster response to threats by finding issues earlier in the attack chain or proactively before the threats can be realized.

- Data Defense

  Adding capabilities that will aid in the identification, classification, and access control of data will move security down to the data level to add an additional layer to the existing network and endpoint layers. This includes concepts such as data loss prevention, data cataloging, and entitlement management. This is an extensive effort that will require partnership within COT as well as our customer agencies.

- Identity Protection

  Enhancing the defenses and protections around the digital identities is critical in an overall security program. Without exception, impactful security events, such as breaches, involve the compromise or misuse of digital identities. Enhancing the usage of MFA, adding central identity management around citizen identities, and greater management of privileged identities are high priority initiative in the strategic plan.

Looking Forward – The Strategic Plan

- Risk Management

  Understanding the totality of risk and weakness in the computing environment is of paramount importance for establishing the right security around our systems and data. The strategic plan includes focus on the development of the mechanisms and process for the establishment of a comprehensive risk register, a catalog of risks throughout the environment. This will allow us to quantify and measure these risks to assist in making the right risk management decisions. Risk management is not risk elimination. It is the empowerment of leadership with dependable information about risk level, complexity, probability, impact, and cost to make informed decisions about the direction and investment in security strategies.

- Staff Development

  Security is not static and a big part of the strategic plan is investment in our staff to ensure that we keep pace with the threat landscape and evolution of technology. State salaries struggle to be competitive, and we need to adapt our approach to obtaining and building the right workforce. Providing the opportunity for professional development and growth is an attractor that will help us recruit the right talent and provide the ability for us to 'grow our own' by bringing in staff early in their careers and building on their passions with the right training.

- Doing More With What We Have

  Continuation of the accomplishments of the program to date to utilize them to their fullest potential. The Commonwealth has an effective security program, and we will continue to mature the technologies in the processes to continuously improve those capabilities.

Infrastructure Investment and Jobs Act Funding

Maximizing the Federal Investment

The State and Local Government Cybersecurity Grant Program (SLCGP)

TEAM KENTUCKY™

SLCGP Funding – State Opportunity

- Privileged Access Management

  Implementation of a new solution for the management and protection of the accounts in the environment that have the highest levels of privilege. These are the accounts most sought after by threat actors and represent the highest level of risk.

- Email Fraud Defense

  We have formidable defenses internally around email but need to implement broader defenses that protect the integrity and trust in email communications both internally and externally. Enhanced email defenses will make it challenging for threat actors to spoof, or masquerade, phishing or malicious emails as official Commonwealth communications.

- Security Monitoring Enhancement

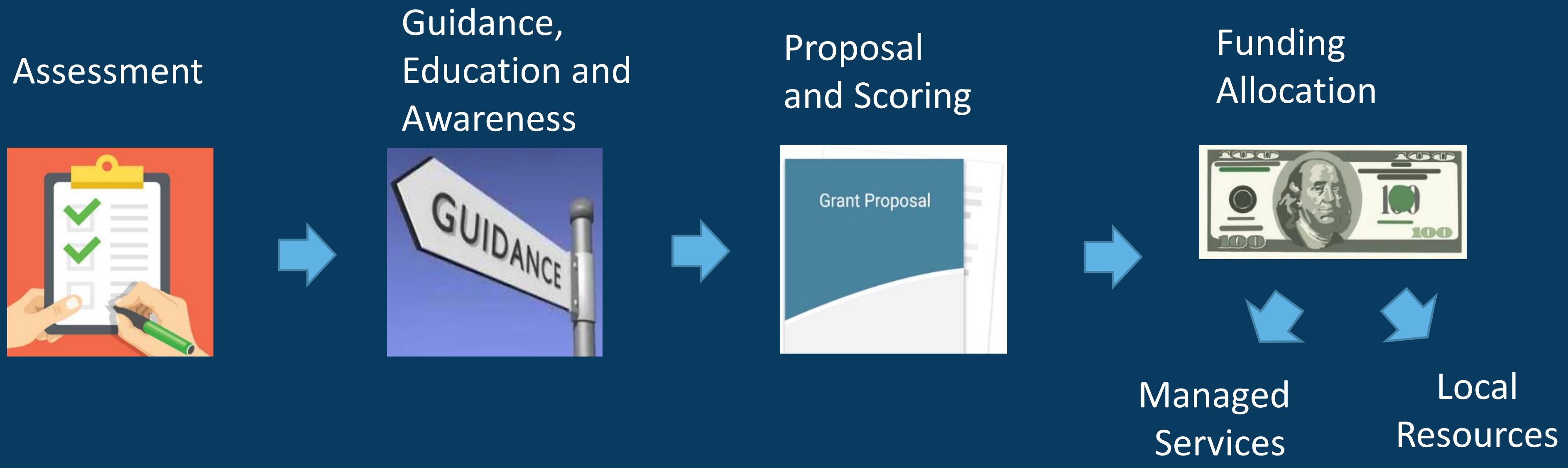
  There is a need to continue to increase not only the amount of detail gathers by the security architecture, but also the depth of retention. The average time a threat actor is in an environment before detection is 6 months and having the detail forensic data available not only allows for more effective investigative efforts around an incident, but also the ability to have a in depth understanding of how an event unfolds. This gives us the ability to harden defenses and close gaps, resulting in stronger defenses.

- Security Architecture Program

  The Commonwealth has made the right investments in security specific technologies but has also made great investments in modernizing IT in general. As a result, many technologies now include enhancements that aid in the overall security of the computing environment. The goal of an effective Security Architecture Program is to look holistically at all technology investments and capabilities to ensure that we are realizing the maximum security benefit from all investments and forming a cohesive security strategy that encompasses all available capabilities.

SLCGP Funding – Local Government Opportunity

The vision for the local government component of the SLCGP is the establishment of a Cyber Grant Committee that will work closely with local government entities through assessments and outreach to build effective grant proposals. The committee will score these proposals and make final determinations as to allocation of the funding, looking at the opportunity for managed services and/or local resource investments.



Assessment

Guidance, Education and Awareness

Proposal and Scoring

Funding Allocation

Managed Services

Local Resources

Thank You

Questions?

Contact Information

David Carter

Chief Information Security Officer
Commonwealth Office of Technology
Email: davidj.carter@ky.gov

TEAM
KENTUCKY™