

Introducing OK-ISAC

“Securing Oklahoma through the Power of Community”





OMAG IT Expo

7/28/2022



OKLAHOMA
OMES Cyber Command

Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>



Oklahoma Cyber Strategy

Resiliency:

- Prevent attacks wherever possible.
- Respond rapidly.
- Return to a good state quickly.
- Manage bad outcomes.
- Learn from the incident.
- Return stronger and better because of incident.

Targeted end state – be able to ignore attacks because:

- Defenses are so good.
- Architecture is so strong.
- Attacks have no serious effect.

“Semper Vigilo, Resiliens ad Infinitum”

TLP: WHITE

OKCYBERCOM Objectives

- Protect Oklahoma's information assets and maximize access to data.
- Develop robust and collaborative risk reduction and risk management strategies.
- Advance a statewide approach to cybersecurity, privacy, and compliance.
- Foster a security- and risk-minded culture throughout Oklahoma's workforce.

TLP: WHITE

Our Responsibility

- Oklahoma Cyber Command is charged with protecting state users and their devices, networks, data and applications from malicious acts. OMES Information Services supports OKCYBERCOM in their objectives.
- What we protect.
- Numerous sensitive data sets. Estimated record count is approx. 36 million.
 - Personally Identifiable Information (PII).
 - Protected Health Information (PHI).
 - Federal Tax Information (FTI).
 - Criminal Justice Information (CJI).
 - Personal Card Industry (PCI).
- Corporate intellectual property.
- Education data.
- 120,000 endpoints across the state.
- 1,200 applications.

TLP: WHITE

OKCYBERCOM Teams

Cybersecurity is a lot like football ...

“Football is one-third offense, one-third defense and one-third special teams” – George Allen

Special teams:

- Compliance.
- Privacy.

Defense:

- Engineers.
- Operations

Offense:

- Hunt and Incident Response Team.
- Cyber Operations .
- OK-ISAC.



TLP: WHITE

Threat Intel Brief - SLTT

- State employees can assist in mitigating security threats by staying aware on secure practices, especially when it comes to sensitive information and phishing attempts.
- Phishing attacks – as an example, can be mitigated by looking out for red flags, if they're asking you to click on a link:
 - Is the email expected (i.e., a password reset link is sent despite an employee never requesting one in the first place)?
 - Is there proper spelling?
 - Check the sender. Is the organization's name spelled correctly, or are there small typos (i.e., omes.okk.gov instead of omes.ok.gov)?



TLP:GREEN



OKLAHOMA
OMES Cyber Command

Threat Intel Brief - SLTT

- Oklahoma Cyber Command can advise on mitigation strategies for VLAN, Protocol management, VPN usage, Phishing/Security Awareness training, Patch and Asset management, Vulnerability identification and remediation, etc.
- As a result, Cybercommand can advice organizations on how to defend against threat actors and ensure that security policies and trainings are put into place to minimize and/or eliminate security incidents from occurring.

TLP:GREEN

Threat Intel Brief – Weak Security Controls

- MFA is not enabled.
- Poorly applied privileges or permissions; and errors within Access Control Lists.
- Use of vendor-default configurations, and default login credentials.
- Remote services lacking sufficient controls to prevent unauthorized access.
- Weak password policies; or poor implementation of password policies.
- Cloud services are unprotected.
- Open ports and misconfigured services that are exposed to the internet.
- Failure to detect and/or block phishing attacks.
- Poor endpoint detection and response.
- How do we correct these controls?

TLP:GREEN

Threat Intel Brief - Mitigations

- Adopt a zero-trust security model, that continuously verifies systems, accounts and processes utilizing multiple sources.
- Limit the ability of a local admin account to login remotely – prevent access via RDP, use dedicated admin workstations.
- Implement multifactor authentication – apply MFA on all VPN solutions.
- Change/disable vendor supplied usernames and passwords.
- Access control – give personnel access only when needed to perform their job.

TLP:GREEN

Threat Intel Brief - Mitigations

- Implement multifactor authentication – apply MFA on all VPN solutions.
- Change/disable vendor supplied usernames and passwords.
- Access control – give personnel access only when needed to perform their job.
- Set up monitoring to detect the use of compromised credentials on your system.
 - Implement password controls to prevent and detect the usage of compromised and/or weak passwords used on your network.

TLP:GREEN

Threat Intel Brief – Mitigations

- Deploy an anti-malware solution on machines to prevent spyware, adware and other malware as part of the OS baseline.
- Monitor antivirus scan results on a regular basis.
- Implement endpoint and detection response tools.
- Employ an IDS/IPS.
- Conduct penetration testing.
- Conduct vulnerability scanning to detect and system vulnerabilities.
- Use cloud service provider tools to detect overshared storage and monitor for abnormal access to these tools/systems.
- Always operate open services with secure configurations.
- Implement a patch and asset management program.

TLP:AMBER



Cybersecurity is a Team Sport



LAW ENFORCEMENT

- Oklahoma Department of Public Safety
- Oklahoma State Bureau of Investigation
- Federal Bureau of Investigation
- Oklahoma Department of Corrections
- Oklahoma Attorney General
- Local Police Departments
- Sheriffs Offices



FEDERAL AGENCIES

- MS-ISAC
- E-ISAC
- Intelligence Community



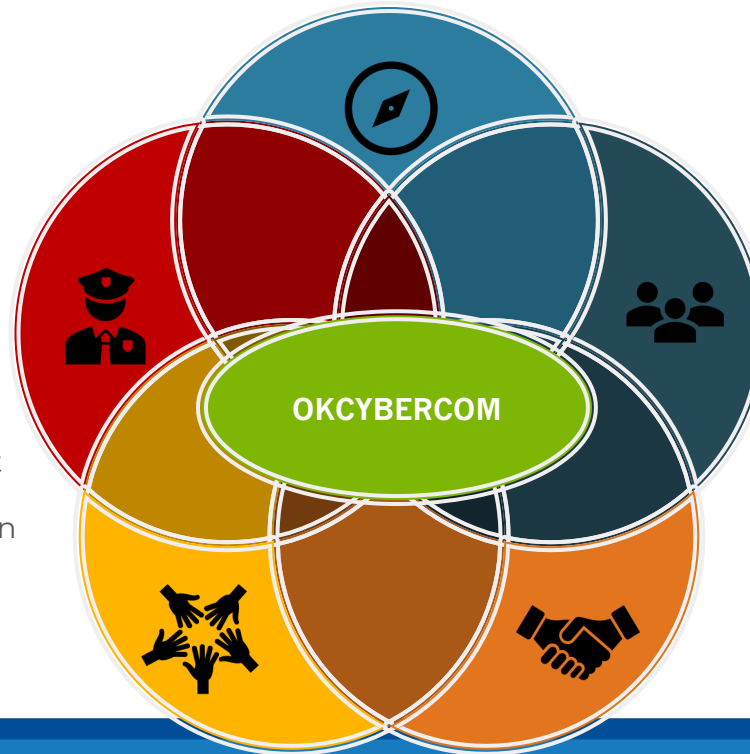
HOMELAND SECURITY

- US Department of Homeland Security
- Cybersecurity and Infrastructure Security Agency (CISA)
- Oklahoma Office of Homeland Security
- Oklahoma Information Fusion Center



STATE AGENCIES

- Unified agencies
- Non-unified agencies
- State Election Board
- Office of Emergency Management
- State Department of Education
- State Regents for Higher Education
- Risk Management
- Human Capital Management
- Oklahoma National Guard

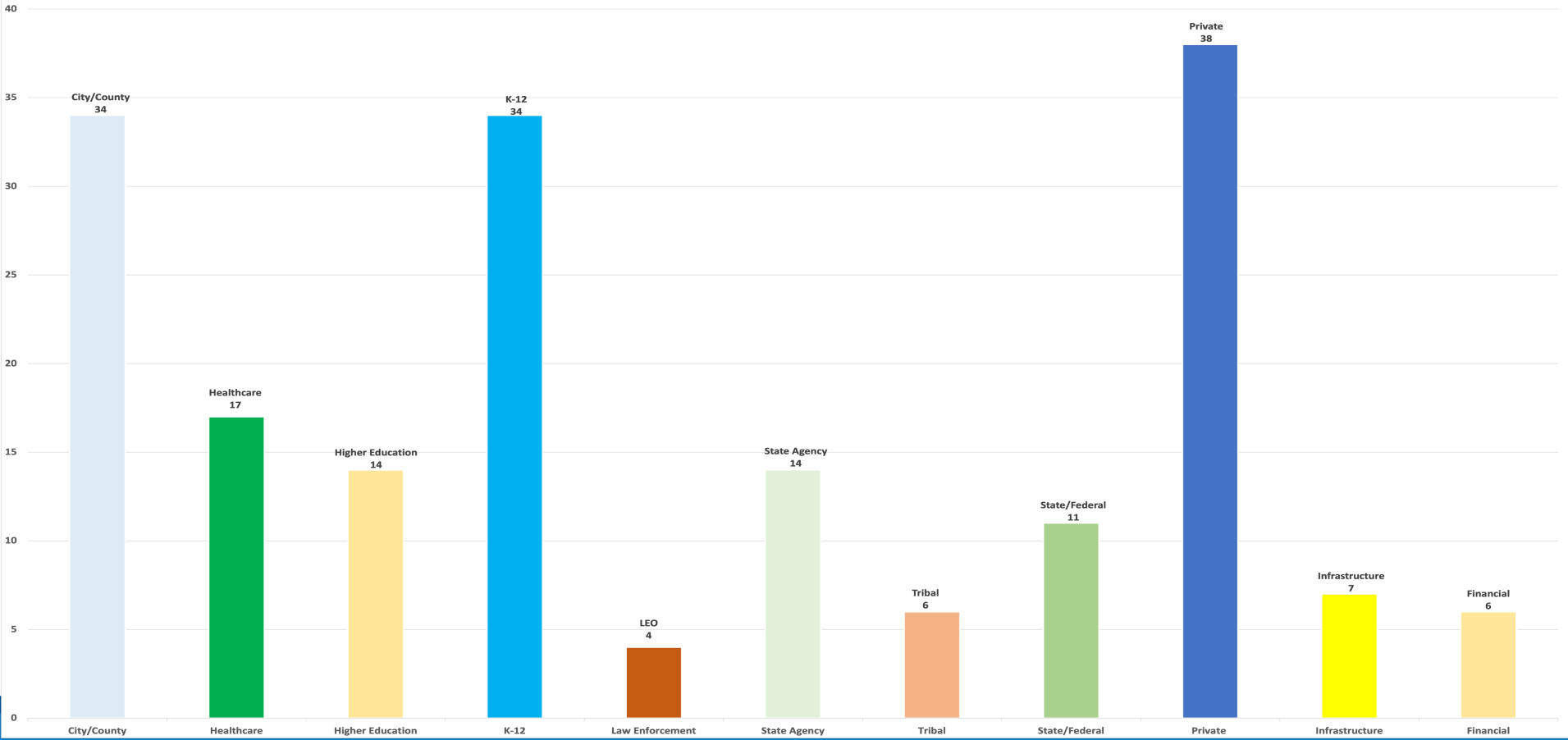


AFFILIATES

- Cities
- Counties
- Municipalities
- Universities
- Tribes
- K-12
- Private Sector
- InfraGard



Oklahoma Information Sharing and Analysis Center (OK-ISAC)



OK-ISAC Mission

- To reduce the risk of cyber threats to the State of Oklahoma.
- To reduce the overall cost of cybersecurity for all Oklahoma organizations by centralizing resources and providing a mechanism for leveraging large-scale purchases.
- To develop a cybersecurity ecosystem through public-private partnerships involving local entities, leading technology companies and other strategic private sector partners.

OK-ISAC Capabilities

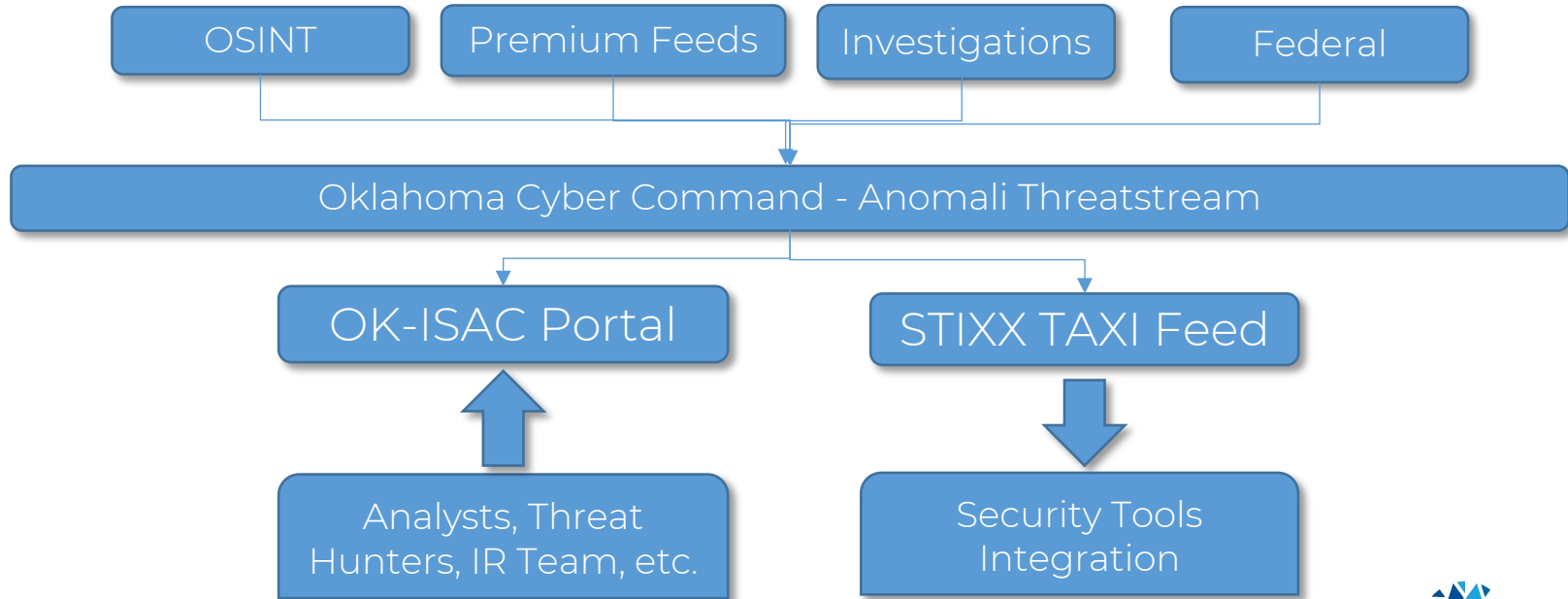
We are building a cybersecurity community in Oklahoma because cybersecurity is a community effort. The OK-ISAC is a dynamic initiative focused on helping to improve the security posture of all Oklahoma organizations.

- A secure online repository for sharing threat intelligence with members .
- Participation in conferences, workshops and tabletop exercises .
- Support efforts to develop cyber workforce by partnering with Higher Education .
- Develop and maintain relationships with industry partners.
- Supports members through implementing best practices and establishing a culture of cybersecurity and compliance.

OK-ISAC – Cyber Threat Intelligence



Sharing real-time threat intelligence through the Oklahoma Cyber Command instance of Anomali Threatstream:



TLP: GREEN

Collaboration in Cybersecurity

- Innovative solutions to support local efforts to achieve a stronger whole community approach to cybersecurity.
 - security-as-a-service,
 - wide-scale training,
 - risk-assessment instruments.
- Collaboration at all levels including federal, state, local and private to not only enhance cyber resiliency but establish a culture of cyber awareness across Oklahoma.

The logo for OMAG (Oklahoma Multi-Agency Group) consists of the letters "OMAG" in a bold, black, sans-serif font.



OKLAHOMA
OMES OK-ISAC

TLP: WHITE





OK-ISAC Membership

For any entity interested, the cost to join this program is free. You can request membership by visiting the link below:

<https://cybersecurity.ok.gov/content/request-access-ok-isac>

Your membership will also provide access to statewide cyber briefings, cybersecurity alerts, workshops and special presentations from our partners. Together we can make Oklahoma more secure!



Questions?

- Email.
cybercommand@omes.ok.gov
- Website.
cybersecurity.ok.gov
- OK-ISAC.
okisac@omes.ok.gov

Chance Grubb, Senior Staff
Officer/OK-ISAC Lead
chance.grubb@omes.ok.gov

Alex Parcell, OK-ISAC Threat Analyst
alexander.parcell@omes.ok.gov

Amber Mangham, Watch Officer
amber.mangham@omes.ok.gov