|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  **FREE SERVICES** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Just Beginning

|  |
| --- |
| MS-ISAC AND CENTER FOR INTERNET SECURITY SERVICES |
|

 |  | Incident Response, Forensics and Remediation Planning. Call MS-ISAC (1-866-787-4722) for cyber incident response support. |  | Training Sessions & Webinars Participate in regular calls with MS-ISAC and peers to increase cyber awareness and education |  | [NCSR](https://www.cisecurity.org/ms-isac/services/ncsr/) Annually complete the Nationwide Cyber Security Review (NCSR) to determine your organizations current maturity against a standard framework and peers.(Level of effort 1-4 hours) |  | [MS-ISAC MCAP](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=2ahUKEwiTu6LL6OnlAhXPHzQIHYvtAbIQFjAEegQIAxAC&url=https%3A%2F%2Fwww.cisecurity.org%2Fwp-content%2Fuploads%2F2018%2F02%2FMS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf&usg=AOvVaw1kGibvWI_LWc8_xXKjhPgI) The Malicious Code Analysis Platform (MCAP) enables members to submit suspicious files. To register email mcap@msisac.org  |  | [CIS RAM](https://learn.cisecurity.org/cis-ram) This self-assessment is an information security risk assessment method that assesses security posture against the CIS Top 20 Controls. |  | [CIS-ESP](https://github.com/CIS-CERT/CIS-ESP) Use this tool to baseline systems and perform incident response ex. find Emotet files.Email MS-ISAC to get more information. |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | [Join MS-ISAC](https://learn.cisecurity.org/ms-isac-registration) to access State, Local, Tribal, Territorial government and Election specific cyber security information and services.(Level of effort <1 hour) |  | Compromised System Information Email MS-ISAC your external domain names and IP addresses and they will continuously scan and provide information if breaches are found.(Level of effort <1 hour) |  | Malware IPs Reduce risk by receiving a weekly list of known-bad sites. Email MS-ISAC for help automating the use of this information to prevent access to malicious websites. (Level of effort 4-8 hours) |  | [CIS-SecureSuite](https://www.cisecurity.org/blog/cis-securesuite-membership-free-for-u-s-sltts-what-you-need-to-know/) A set of tools that will help evaluate and apply secure configuration settings to laptops, servers, network devices, and more. |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | [FedVTE Training](https://fedvte.usalearning.gov/) the Federal Virtual Training Environment provides free online cybersecurity training to federal, state, local, tribal and territorial government employees and veterans (>1 hour) |  | Vulnerability Management Program Email MS-ISAC to receive monthly notifications of out-of-date software is found on external facing web servers.(Level of effort <1 hour) |  | Mentor Workgroup Participate as a mentor or mentee with other MS-ISAC members. |  | [CIS CSAT](https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/?utm_campaign=Controls&utm_medium=email&_hsenc=p2ANqtz-_CGf6dMWg_M4bsCQL7h9qLE1cKM9u5ucFWDQot_0wldeJXM3CIWsafD0bok7D37DUQ8XCCeY_xVD4lqEc04va-WNJXtw&_hsmi=69348469&utm_content=69348469&utm_source=hs_email&hsCtaTracking=aab6dc0b-432b-4e2f-883f-1effcab0d437%7Cc7ae2509-7108-48b8-8f82-9848cb4c8e25) A set of tools that will help track and prioritize implementation of the CIS Controls. |  | [Workgroups](https://www.cisecurity.org/ms-isac/services/workgroups/) Participate in a working group to address a specific cybersecurity challenge: Business Resiliency Education and Awareness Metrics Intelligence and Analysis Application Security |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|   |   |   |   |   |   |   |   |  Maturing |   |   |   |   |   |   |   |   |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| DHS AND OTHER SERVICES |  | [Join CTIS](https://www.anomali.com/learn/ctis) to share and access Colorado specific cyber information being distributed by your government peers.(Level of effort <1 hour) |  | [DHS Risk Vulnerability Assessment](https://www.us-cert.gov/resources/ncats)  Sign up to be put on a wait list (1yr or more) for a free penetration test and phishing test. Email DHS for more details.(Level of effort <1 hour) |  | [GCA DNS](https://www.globalcyberalliance.org/quad9/) Quad9 Reduce risk by preventing access to known-bad internet sites. (Level of effort < 1 hour) |  | [HSIN](https://www.dhs.gov/homeland-security-information-network-hsin) Access alert maps, policies, reports, guides, recorded webcasts and sector specific discussion groups. HSIN access is granted as a part of joining MS-ISAC. |  |  |  |  |  | [DHS CSET](https://cset.inl.gov/SitePages/Home.aspx) The Cyber Security Evaluation Tool guides asset owners through an evaluation of that asset. |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | [End User Training](https://cofense.com/cbfree-computer-based-training/) Cofense has 21 free modules for end user training on cyber security.(Level of effort <1 hour if you have a Learning Management Solution) |  | [External Scanning](https://www.us-cert.gov/resources/ncats) Reduce risk by providing DHS your external IP addresses. DHS will continuously scan providing weekly reports on your organization's vulnerabilities. Email DHS for more information.(Level of effort <1 hour) |  | [DMARC](https://dmarc.globalcyberalliance.org/dmarc-bootcamp/) Reduce the chance users will click on malicious email by preventing phony emails from ever being delivered. This link is to videos that will walk you through the configuration.(Level of effort 8-20 hours) |  | [Training](https://fedvte.usalearning.gov/) Federal Virtual Training Environment (FedVTE) is DHS' online, on-demand training center. It includes hands on labs and training courses. |  | DHS AIS  Bidirectional sharing of cyber threat indicators with NCCIC. Receive DHS-developed indicators and share back (supported: FlareClient, Soltra, Splunk – contact DHS for others) |  | [DHS CRR](https://www.us-cert.gov/ccubedvp/assessments) The Cyber Resilience Review is an interview-based assessment to evaluate operational resilience and cybersecurity practices. |  | [DHS C-IST](https://www.isao.org/resource-library/government-programs/dhs-cyber-infrastructure-survey-tool-c-ist/) The Cyber Infrastructure Survey provides an assessment of cybersecurity practices for one critical service. |  | [DHS VADR](https://www.us-cert.gov/resources/ncats)  The Validated Architecture Design Review provides a sophisticated analysis of the network. |

 For more information on DHS Services, the DHS Cyber Security Advisor is also available.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FEE-BASED SERVICES** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| MS-ISAC AND CENTER FOR INTERNET SECURITY SERVICES |  |  |  | [Albert](https://www.cisecurity.org/services/albert/) is an intrusion detection sensor (IDS). Albert is a MS-ISAC fully managed monitoring service - after you install the hardware locally, MS-ISAC manages the hardware/software and sends vetted alerts to staff. |  | [Managed Security Services](https://www.cisecurity.org/ms-isac/services/) MS-ISAC can perform the following managed services: Firewall monitoring Host-based IDS IDS/IPS Monitoring Proxy Monitoring |  | [Phishing Assessment](https://www.cisecurity.org/ms-isac/services/) MS-ISAC customized assessment to evaluate organizations risk to phishing attacks.Email MS-ISAC for more information. |  | [Penetration Tests](https://www.cisecurity.org/ms-isac/services/) MS-ISAC performs network and web application penetration test that simulates real-world attacks.Email MS-ISAC for more information. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|

|  |
| --- |
|  |

 |  |  | [CIS CyberMarket](https://www.cisecurity.org/services/cis-cybermarket/) is a collaborative purchasing group for state, local, tribal, and territorial (SLTT) governments***SANS*** – employee security awareness training and online technical training***(ISC)2*** – certification programs and training***New York University Tandon School of Engineering*** – online graduate school program***Belarc*** – IT asset and security configuration management***McAfee Skyhigh Security Cloud*** – cloud access security broker***Kroll*** – cyber risk management and assessment solutions***Akamai*** – cloud-based targeted threat protection solution and secure internet gateway***Everest Insurance & Gallagher*** – cyber risk insurance |  | [Vulnerability Assessments](https://www.cisecurity.org/ms-isac/services/) MS-ISAC assessment to identify, prioritize and report critical vulnerabilities within your network and web applications. Assessments: Network Vulnerability  Web Applications Payment Card Industry Email MS-ISAC for more information. |  | MaturingJust Beginning |  | Security Assessment MS-ISAC will perform an assessment to identify pre-existing compromises in your organization.Email MS-ISAC for more information. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| DHS AND OTHER SERVICES |  |  |  |  |  | Qualys Vulnerability Scan purchase a vulnerability scanning system to identify unpatched and vulnerable systems in your organization. Email Qualys for more information and volume discount pricing. |  |  |  | CyberCorps -Scholarship for Service (SFS) |  |  |  |  |  |  |

Last Updated: December 3, 2019