مراکز سیستمهای هشدار سایبری : Alerts, Advisory, Bulletins

1.	https://cyber.gc.ca › alerts-advisories	Alerts and advisories - Canadian Centre for Cyber Security
2.	https://www.cisa.gov › uscert › ncas › alerts	Alerts | CISA
3.	https://www.cyber.gov.au › acsc › view-all-content › al	Cyber.gov.au
4.	https://www.cisecurity.org › cybersecurity-threats › aler	Center for Internet Security
5.	https://www.cisecurity.org › cybersecurity-threats	Center for Internet Security
6.	https://www.ncsc.gov.uk	National Cyber Security Centre - NCSC.GOV.UK
7.	https://digital.nhs.uk › cyber-alerts	Cyber alerts - NHS Digital
8.	https://www.cybersecurity.hk	Cyber Security Information Portal - Hong Kong
9.	https://www.ncsc.gov.ie	National Cyber Security Centre: NCSC
10.	https://www.nsa.gov › Press Room	NSA Cybersecurity Advisories & Guidance
11.	https://us-cert.cisa.gov	Homepage | CISA
12.	https://us-cert.cisa.gov › ncas › current-activity	Current Activity | CISA - US-CERT
13.	https://connect.hello.global.ntt › Cybersecurity-Advisory	Cybersecurity Advisory Services - Global NTT
14.	https://www.cyberthreatsensor.io/cybersecurity/solution	Cybersecurity Threat Solutions - Threat Detection And Response
15.	https://www.isaca.org	ISACA's CISA Certification - Information Systems Auditor
16.	https://www.cisa.gov › uscert › ncas › bulletins	Bulletins | CISA
17.	https://www.cyberthon.lt	CTF Competition - Solve Cybersecurity Challenges
18.	https://tools.cisco.com	Cisco Security Advisories
19.	https://support.microsoft.com/	Security updates for Microsoft Windows Store applications
20.	http://www02.abb.com › GAD › GAD01626.NSF › Op...	ABB Cyber Security Advisories
21.	https://new.abb.com › advanced-digital-services › cyber...	ABB Cyber Security Advisories
22.	https://new.siemens.com › ... › Services › CERT Services	CERT Services | Services | Siemens Global

23.	Schneider	
24.	Mitsubishi	
25.	Honeywell	
26.	پتسا	
27.	پیشرون بهینه نوآوران	
28.	موکز	
29.	راهکارهای هوشمند برنا	
30.	KYORITSU	
31.	OMRON	
32.	…..	

Global associations and teams

Logo	Organization	Description	Size	Member of FIRST
	FIRST[1]	The Forum of Incident Response and Security Teams is the global association of CSIRTs.	605 member organizations.	n/a
	Packet Clearing House[2]	"CERT of last resort" with global coverage, serving countries and constituencies which are not yet served by their own dedicated CERT. Founded in 1994.	18 staff, presence in 106 countries, budget USD 251m/yr.	Yes

National or economic region teams

Country	Team/s	Description	Size	Member of FIRST
Australia	AusCERT[3]	Cyber Emergency Response Team (CERT) in Australia and the Asia/Pacific region		Yes
Australia	Australian Cyber Security Centre (ACSC)[4]	In 2010 the Australian Federal Government started CERT Australia. In 2018 CERT Australia became part of the Australian Cyber Security Centre (ACSC) which then in turn became part of the Australian Signals Directorate (ASD).		Yes
Austria	CERT.at	The national Computer Emergency Response Team for Austria as part of the Austrian domain registry NIC.at for .at.[5]	9 employees[6]	Yes
Austria	govCERT Austria	A public-private partnership of CERT.at and the Austrian Chancellery.[7]		Yes
Austria	Austrian Energy CERT (AEC)	A cooperation between CERT.at and the Austrian energy sector for energy and gas sector.[8]		Yes
Austria	ACOnet-CERT	The Computer Emergency Response Team of ACOnet.[9]		Yes
Bangladesh	BGD e-Gov CIRT	Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National CIRT of Bangladesh (N-CIRT) currently with responsibilities including receiving, reviewing, and responding to computer security incidents and activities.		Yes
Belgium	CERT.be	Centre for Cyber Security Belgium		Yes
Bolivia	CGII.gob.bo	Centro de Gestión de Incidentes Informáticos	8 employees	
Brazil	CERT.br	Brazilian National Computer Emergency Response Team		Yes
Canada	Canadian Centre for Cyber Security	Assumed national CERT role with the transfer of the Canadian Cyber Incident Response Centre (CCIRC) from Public Safety Canada in October 2018.[10]		Yes
China	CNCERT/CC[11]	Founded in September 2002	40 employees[12]	Yes
Colombia	colCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT		
Croatia	CARNet CERT			Yes
Czech Republic	CSIRT.CZ			Yes
Denmark	DKCERT	Danish Computer Security Incident Response Team		Yes
Denmark	CFCS-DK	Centre for Cyber Security		Yes

Ecuador	ECUCERT	Centro de Respuesta a Incidentes Informáticos del Ecuador	Yes
Egypt	EG-CERT[13]	Work as trust center for Cyber Security Services across Egyptian cyber space.[14]	Yes
Estonia	CERT-EE[15]	The national and governmental Computer Emergency Response Team for Estonia.	Yes
Europe	CERT-EU[16]	Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies.[17]	Yes
Eurocontrol	EATM-CERT	European Air Traffic Management Computer Emergency Response Team	
Finland	NCSC-FI	National Cyber Security Centre of Finland	Yes
France	CERT-FR		Yes
Germany	CERT-Bund		Yes
Ghana	CERT-GH	National Cyber Security Centre of Ghana	
Ghana	NCA-CERT	National Communications Authority Computer Emergency Response Team	
Hong Kong	HKCERT		Yes
Iceland	CERT-IS	The national Computer Emergency Response Team for Iceland as part of the Post and Telecommunication Administration in Iceland	Yes
India	CERT-In	CERT-In	Yes
Indonesia	ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure coordination centre was founded in 2007.[18]	Yes
Iran	CERTCC MAHER	Maher Center of Iranian National Computer Emergency Response Team	
Israel	CERT-IL	The Israeli Cyber Emergency Response Team is part of Israel National Cyber Directorate	Yes
Italia	CSIRT Italia	Established at the National Cybersecurity Agency for the implementation of the NIS Directive in Italy absorbed previous CERT-PA and CERT-Nazionale.	
Japan	JPCERT/CC		Yes
Japan	IPA-CERT		Yes
Jersey	CERT-JE[19]	Jersey Cyber Emergency Response Team. Established 2021.[20]	
Kazakhstan	TSARKA	Computer Emergency Response Team in Kazakhstan was founded in 2015	Yes
Kyrgyzstan	CERT-KG		
Laos	LaoCERT	Lao Computer Emergency Response Team	
Latvia	CERT.LV	The Information Technology Security Incident Response Institution of the Republic of Latvia.	Yes
Luxembourg	CIRCL	CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.	Yes
Macau	MOCERT		
Malaysia	MyCERT	The Malaysia Computer Emergency Response Team was established in 1997. It is now part of CyberSecurity Malaysia[21]	Yes
Mexico	CERT-MX	The Centre of Expertise in Technological Response, is part of the Scientific Division of the Federal Police (Mexico)	Yes
Moldova	CERT-GOV-MD	Center for Response on Cybersecurity Incidents - CERT-GOV-MD	Yes

Mongolia	MNCERT/CC	Mongolian Cyber Emergency Response Team / Coordination Center. Founded in 2014.	Yes
Morocco	maCERT		Yes
Netherlands	NCSC-NL		
Netherlands	SURFcert	Computer Emergence Response Team for the Dutch research and education network.	Yes
New Zealand	CERTNZ[22]		Yes
Nigeria	ngCERT[23]		Yes
Norway	NorCERT[24]	Cyber Security Center and national CERT of Norway. Part of the National Security Authority (NSM).	Yes
Pakistan	PakCERT		
Papua New Guinea	PNGCERT		
Philippines	CSP-CERT	CyberSecurity Philippines - CERT, established in 2016 the very first Non-profit CSIRT/CERT organization in the Philippines.	
Poland	CERT Polska		Yes
Portugal	CERT.PT	Part of the National Cyber Security Center (CNCS) of Portugal	Yes
Qatar	Q-CERT		Yes
Republic of Ireland	CSIRT-IE		
Romania	CERT-RO	Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO	
Russia	GOV-CERT		
Russia	RU-CERT		Yes
Russia	CERT-GIB		
Russia	BI.ZONE-CERT		
Russia	Financial CERT	Financial Sector Computer Emergency Response Team (special division of the Bank of Russia)	Yes
Russia	KASPERSKY ICS CERT		
Russia	NCIRCC		
Saudi Arabia	Saudi-CERT	Saudi CERT has three main functions: increasing the level of knowledge and awareness regarding cybersecurity, disseminate information about vulnerabilities, and campaigns and cooperating with other response teams. Saudi CERT serves different stakeholder in the country including individuals business and government agencies. And proactive and reactive services.	Yes
Serbia	SRB-CERT	National CERT of the Republic of Serbia	Yes
Serbia	MUP CERT	Centar za reagovanje na napade na informacioni sistem	Yes
Singapore	SingCERT		Yes
Slovakia	SK-CERT	Národná jednotka SK-CERT | National unit SK-CERT	Yes
Slovenia	SI-CERT	Slovenian Computer Emergency Response Team, part of ARNES	Yes
Slovenia	SIGOV-CERT	Specifically formed for information security in the government sector of Slovenia	

South Africa	CSHUB-CSIRT	CyberSecurity Hub CSIRT established by the Department of Telecommunications and Postal Services[25]	
South Korea	KrCERT/CC		Yes
Spain	CCN-CERT	Centro Criptológico Nacional	Yes
Sri Lanka	SL CERT | CC[26]	Computer Emergency Readiness Team | Co-ordination Center	Yes
Sweden	CERT-SE[27]		Yes
Switzerland	GovCERT.ch[28]	The parent organisation of GovCERT.ch is the Swiss Reporting and Analysis Centre for Information Assurance (MELANI)[29]	Yes
Taiwan	TWCERT/CC[30]		Yes
Thailand	ThaiCERT [31]		Yes
Tonga	CERT Tonga		
Turkey	TR-CERT (USOM)		Yes
Ukraine	FS Group	FS Group - CERT	Yes
Ukraine	CERT-UA	Computer Emergency Response Team of Ukraine	Yes
United Arab Emirates	aeCERT	The United Arab Emirates - Computer Emergency Response Team	Yes
Uganda	CERT.UG	Uganda National Computer Emergency Response Team /CC (Absorbed UG-CERT [1])	Yes
United Kingdom	National Cyber Security Centre	Absorbed CERT-UK	Yes
United States	US-CERT	Part of the National Cyber Security Division of the United States Department of Homeland Security.[32]	Yes
United States	CERT/CC	Created by the Defense Advanced Research Projects Agency (DARPA) and run by the Software Engineering Institute (SEI) at the Carnegie Mellon University	Yes
Uzbekistan	UzCERT	Computer Emergency Response Team of Uzbekistan	
Vietnam	VNCERT	Vietnam CERT	Yes

Information Sharing and Analysis Center

Canada

- Global Mining and Metals Information Sharing & Analysis Centre (MM-ISAC)[3]

Europe

European Energy - Information Sharing & Analysis Centre (EE-ISAC)[4] is a network of private utilities, solution providers and (semi) public institutions such as academia, governmental and non-profit organizations which share valuable information on cyber resilience to strengthen the cyber security of the European Power Grid.

India

In India, the Information Sharing and Analysis Center (ISAC) operates as an independent non-profit organization that works closely as Public-Private-Partner (PPP) with apex nodal agency for cyber security, National Critical Information Infrastructure Protection Center (NCIIPC), designated under the IT Act Law 2000.

United States

The National Council of ISACs (NCI Directorate) members include:

- Automotive (Auto-ISAC)
- Aviation (A-ISAC)
- Communications ISAC (NCC)
- Defense Industrial Base (DIB-ISAC)
- Emergency Services (EMR-ISAC)
- Electricity (E-ISAC)
- Energy Analytic Security Exchange (EASE)
- Elections Infrastructure ISAC (EI-ISAC)[5]
- Financial Services (FS-ISAC)
- Healthcare Ready
- Health (H-ISAC)
- Information Technology (IT-ISAC)
- Maritime Security ISAC
- Media and Entertainment Sharing Analysis Center (ME-ISAC)
- Nuclear (NEI)
- Oil and Gas (ONG-ISAC)
- Public Transit (PT-ISAC)
- Real Estate (RE-ISAC)

- Research & Education Network (REN-ISAC)
- Retail & Hospitality ISAC (RH-ISAC) Formerly R-CISC
- Space ISAC (S-ISAC)
- Supply Chain (SC-ISAC)
- Surface Transportation (ST-ISAC)
- Water ISAC (Water-ISAC)

Open Source Threat Intelligence Feeds

1. FBI: InfraGard Portal. ...
2. DHS CISA Automated Indicator Sharing
3. Abuse.ch
4. COVID-19 Cyber Threat Coalition Feeds
5. BlockList.de
6. Phishtank Verified Online Url Feeds
7. Proofpoint Emerging Threats Rules
8. The CINS Score
9. SANS Internet Storm Center
10. VirusTotal
11. Cisco Talos Intelligence
12. The Spamhaus Project
13. VirusShare Malware Repository
14. Google Safe Browsing
15. Emerging Threats
16. FBI InfraGard
17. Dan.me.uk
18. hpHosts
19. AlienVault OTX
20. Abuse.ch Feodo Tracker
21. Abuse.ch URLhaus
22. Department of Homeland Security: Automated Indicator Sharing. ...
23. 3. @ ...
24. SANS: Internet Storm Center. ...
25. VirusTotal: VirusTotal. ...
26. Cisco: Talos Intelligence. ...
27. VirusShare: VirusShare Malware Repository. ...

Threat Intelligence Feeds Products

1. **Recorded Future Intelligence Services**
2. **WildFire**
3. **Kaspersky Threat Intelligence Services**
4. **IntSights External Threat Protection Suite**
5. **CTM360**
6. **PhishLabs Digital Risk Protection**
7. **DeCYFIR**
8. **SOCRadar Digital Risk Protection Platform**
9. **XVigil**
10. **Flashpoint**
11. **CybelAngel**
12. **Blueliv Threat Intelligence Services**
13. **Digital Shadows SearchLight**
14. **Anomali**
15. **Secureworks Threat Intelligence Services**
16. **BloxOne Threat Defense**
17. **ZeroFOX Platform**
18. **Mandiant Threat Intelligence**
19. **HanSight Threat Intelligence**
20. **Silo for Research**
21. **BlueCat DNS Edge**

https://www.opencti.io › ...	OpenCTI - Open platform for cyber threat intelligence	OpenCTI is an **open source** platform allowing organizations to store, organize, visualize and share their knowledge on **cyber threats**.
OpenCTI is **an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables**. It has been created in order to structure, store, organize and visualize technical and non-technical information about cyber threats.		
https://www.misp-project.org	MISP Open Source Threat Intelligence Platform &amp; Open ...	The MISP is an **open source** software solution for collecting, storing, distributing and sharing **cyber** security indicators and **threats** about **cyber** security
Features of MISP, the open source threat sharing platform A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.		

Open-Source Intelligence Tools

BuiltWith	With BuiltWith, it’s possible to uncover the different tech stacks and platforms that power certain websites. It also generates a list of JavaScript/CSS libraries, plugins and other utilities used by the website in question. Personnel can then use that to perform vital functions, such as patching WordPress weaknesses and updating a plugin with a new version.
Creepy	An OSINT tool written in Python, Creepy collects geolocation data from social networking sites as well as image hosting services. It enables users to present that data on a map. Not only that, but users can also download those results in .CSV or .KML to show in Google Maps.
theHarvester	theHarvester is an OSINT tool through which users can gather emails, subdomains, IPs, URLs and other pieces of data using numerous public data sources. On the passive side, theHarvester is capable of using search engines such as DuckDuckGo and Google. But it also comes with active search capabilities such as conducting DNS brute forcing and taking screenshots of whatever subdomains it finds.
Maltego	A Java tool that runs on Windows-, Linux- and macOS-powered machines, Maltego is a graphical link analysis tool that helps users to gather and connect OSINT as part of an ongoing investigation. Maltego comes with 58 data integrations from over 35 data partners, and it allows users to choose four different layouts to recognize patterns in the data they’ve uncovered.
Metagoofil	The value of Metagoofil lies in its ability to extract metadata from public documents, including PDFs and Microsoft Office files. It does this by using a Google search to find and download the documents to a local disk. At that point, the tool uses Hachoir, PdfMiner and other libraries to lift the metadata from those documents.
Recon-ng	Recon-ng is a framework that stands apart from others due to its focus on web-based open source reconnaissance. It helps users to pursue their reconnaissance work by way of modules. Towards that end, Recon-ng comes with several built-in modules, such as those that help users to uncover further domains related to a target domain.
Shodan	With Shodan, users can search the web for internet-connected devices. Websites provide some insight into those assets, but Shodan takes its scans a step further by revealing assets like Internet of Things (IoT) products. Shodan helps achieve comprehensive visibility over all a group’s devices and to keep those assets up to date.
SpiderFoot	Those running Linux- and Windows-based machines can use SpiderFoot to automate their collection of OSINT. This open source reconnaissance tool comes with over 200 modules for data collection and analysis. This can help gain a broad view of their attack surfaces, including low-hanging fruit like unmanaged assets and exposed credentials.
Spyse	With more than 25 billion records stored about online assets, Spyse helps users to collect public data relating to websites, servers and devices connected on the web. Security teams can use that knowledge to check on risks and suspicious connections between those points in an effort to minimize their employer’s attack surface.
TinEye	Unlike the other OSINT tools discussed thus far, TinEye focuses on reverse image searches. It can help moderate content that’s posted on the web and to detect instances of fraud involving a brand. What’s more, teams can use TinEye to track where those images are appearing online.

Fusion Centers and Intelligence Sharing

- Arizona. ...
- Arkansas. ...
- California. ...
- Colorado. ...
- Connecticut. ...
- Delaware.

There are **78 recognized fusion** centers listed on the Department of Homeland Security (DHS) website.

Global Justice XML (Archive)

The Global Justice Extensible Markup Language (XML) Data Model (Global JXDM) is an XML standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner.

The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes.

The Global JXDM is an object-oriented data model for organizing the content of a data dictionary, the Global Justice XML Data Dictionary (Global JXDD), in a database. From this database, an XML schema specification can be generated that consistently represents the semantics and structure of common data elements and types required for information exchange within the justice and public safety communities.

There are three primary parts to the Global JXDM: the Data Dictionary (identifying content and meaning), the Data Model (defining structure and organization), and the Component Reuse Repository (a database).

The work accomplished to date, based on participation by practitioners from the justice and public safety communities, has resulted in the creation of a data model that can be used to generate data schema which will facilitate information sharing among the various jurisdictions of those communities. This was done in a manner that reduced the cost of developing the technical solutions required, simplified the process and associated products, and enhanced the interoperability quotient of the end product. The approach combines successful practices in data modeling with recent technology standards for XML schema. Ultimately, XML and the Global Justice XML Data Model can help to make criminal justice information sharing easier, quicker, and less expensive for agencies by offering standard tools, techniques, and data structures.

With the help of XML and the Global Justice XML Data Model, the opportunity for proactive justice information sharing is enhanced, arming everyone across the justice and public safety communities with the most accurate and up-to-date data to make the very best decisions possible-increasing law enforcement and criminal justice agency efficiency, public safety, and national security.

Mass surveillance

- **Daily documents**: Requirement for the use and tracking of state-issued identity documents and registration.
- **Border and travel control**: Inspections at borders, searching computers and cell phones, demanding decryption of data, and tracking travel within as well as to and from a country.
- **Financial tracking**: A state's ability to record and search financial transactions: checks, credit cards, wires, etc.
- **Gag orders**: Restrictions on and criminal penalties for the disclosure of the existence of state surveillance programs.
- **Anti-crypto laws**: Outlawing or restricting cryptography and/or privacy enhancing technologies.
- **Lack of constitutional protections**: A lack of constitutional privacy protections or the routine overriding of such protections.
- **Data storage**: The ability of the state to store the data gathered.
- **Data search**: The ability to organize and search the data gathered.
- **Data retention requirements**: Laws that require Internet and other service providers to save detailed records of their customers' Internet usage for a minimum period of time.
  - **Telephone data retention requirements**: Laws that require telephone companies to record and save records of their customers' telephone usage.
  - **Cell phone data retention requirements**: Laws that require cellular telephone companies to record and save records of their customers' usage and location.
- **Medical records**: Government access to the records of medical service providers.
- **Enforcement**: The state's ability to use force to seize anyone they want, whenever they want.
- **Lack of *habeas corpus***: Lack of a right for a person under arrest to be brought before a judge or into court in a timely fashion or the overriding of such rights.
- **Lack of a police-intel barrier**: The lack of a barrier between police organizations and intelligence organizations, or the overriding of such barriers.
- **Covert hacking**: State operatives collecting, removing, or adding digital evidence to/from private computers without permission or the knowledge of the computers' owners.
- **Loose or no warrants**: Arrests or searches made without warrants or without careful examination and review of police statements and justifications by a truly independent judge or other third-party.

Alert Level Information

What Do the Different Alert Level Colors Indicate?

- GREEN or LOW indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.
    - Examples:
        - Normal probing of the network
        - Low-risk viruses
    - Actions:
        - Continue routine preventive measures, including the application of vendor security patches and updates to anti-virus software signature files on a regular basis.
        - Continue routine security monitoring.
        - Ensure personnel receive proper training on cybersecurity policies.
    - Notification:
        - No notification is warranted if a state is currently at this level.
        - Notification via our website will be done concurrently with the Alert Level change.
- BLUE or GUARDED indicates a general risk of increased hacking, virus, or other malicious activity. The potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.
    - Examples:
        - A critical vulnerability is discovered but no exploits are reported.
        - A critical vulnerability is being exploited but there has been no significant impact.
        - A new virus is discovered with the potential to spread quickly.
        - There are credible warnings of increased probes or scans.
        - A compromise of non-critical system(s) did not result in loss of data.
    - Actions:
        - Continue recommended actions from previous level.
        - Identify vulnerable systems.
        - Implement appropriate countermeasures to protect vulnerable systems.
        - When available, test and implement patches, install anti-virus updates, etc., in the next regular cycle.
    - Notification:
        - Notification via our website will be done concurrently with the Alert Level change.
- YELLOW or ELEVATED indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service. At this level, there are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.
    - Examples:
        - An exploit for a critical vulnerability exists that has the potential for significant damage.
        - A critical vulnerability is being exploited and there has been a moderate impact.
        - There is a compromise of a secure or critical system(s) containing sensitive information.
        - There is a compromise of a critical system(s) containing non-sensitive information if appropriate.
        - A virus is spreading quickly throughout the Internet, causing excessive network traffic.
        - There is a distributed denial of service attack.

    - Actions:
        - Continue recommended actions from previous levels.
        - Identify vulnerable systems.
        - Increase monitoring of critical systems.
        - Immediately implement appropriate countermeasures to protect vulnerable critical systems.
        - When available, test and implement patches, install anti-virus updates, etc., as soon as possible.
    - Notification:
        - Notification to the Multi-State ISAC via secure portal email or telephone will be given when a state upgrades its Alert Level to Yellow or Elevated.
        - Notification via our website will be done concurrently with the Alert Level change.
        - Notification via secure portal email will be sent to the states when the any state or the national Alert Level is raised to Yellow or Elevated.
- ORANGE or HIGH indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.
    - Examples:
        - An exploit for a critical vulnerability exists that has the potential for severe damage.
        - A critical vulnerability is being exploited and there has been significant impact.
        - Attackers have gained administrative privileges on compromised systems.
        - There are multiple damaging or disruptive virus attacks.
        - There are multiple denial of service attacks against critical infrastructure services.
    - Actions:
        - Continue recommended actions from previous levels.
        - Closely monitor security mechanisms, including firewalls, web log files, anti-virus gateways, system log files, etc., for unusual activity.
        - Consider limiting or shutting down less critical connections to external networks such as the Internet.
        - Consider isolating less mission-critical internal networks to contain or limit the potential of an incident.
        - Consider the use of alternative methods of communication, such as phone, fax, or radio in lieu of email and other forms of electronic communication.
        - When available, test and implement patches, anti-virus updates, etc., immediately.
    - Notification:
        - Notification to the Multi-State ISAC via secure portal email or telephone will be given when a state upgrades its Alert Level to Orange or High.
        - Notification via the Multi-State ISAC's website will be done concurrently with the Alert Level change.
        - Notification via secure portal email will be sent to the states when any state or national Alert Level is raised to Orange or High.
- RED or SEVERE indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or widespread level of damage or disruption of Critical Infrastructure Assets.
    - Examples:
        - Complete network failures
        - Mission-critical application failures

        - Compromise or loss of administrative controls of critical system
        - Loss of critical supervisory control and data acquisition (SCADA) systems
        - Potential for or actual loss of lives or significant impact on the health or economic security of the state
    - Actions:
        - Continue recommended actions from previous levels.
        - Shut down connections to the Internet and external business partners until appropriate corrective actions are taken.
        - Isolate internal networks to contain or limit the damage or disruption.
        - Use alternative methods of communication, such as phone, fax, or radio as necessary in lieu of email and other forms of electronic communication.
    - Notification:
        - Notification via secure portal email, telephone, pager, or fax will be given when a state upgrades its Alert Level to Red or Severe.
        - Notification via our website will be done concurrently with the Alert Level change.
        - Notification to the states via secure portal email or telephone to set up a conference call when the Multi-State ISAC upgrades the national Alert Level to Red or Severe.

How Is the Alert Level Determined?

The Alert Level is determined using the following threat severity formula:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

- *Lethality: How likely is it that the attack will do damage?*
  (Value = Potential Damage)

    - 5: Exploit exists. Attacker could gain root or administrator privileges. Attacker could commit denial of service.
    - 4: Exploit exists. Attacker could gain user level access privileges. Attacker could commit denial of service.
    - 3: No known exploit exists. Attacker could gain root or administrator privileges. Attacker could commit degradation of service.
    - 2: No known exploit exists. Attacker could gain user level access privileges.
    - 1: No known exploit exists. Attacker could not gain access.

- *Criticality: What is the target of the attack?*
  (Value = Target)

    - 5: Core services such as critical routers, firewalls, VPNs, IDS systems, DNS servers, or authentication servers
    - 4: Email, web, database, and critical application servers
    - 3: Less critical application servers
    - 2: Business desktop systems
    - 1: Home users

- *System Countermeasures: What host-based preventive measures are in place?*
  (Value = Countermeasure)

    - 5: Current operating system with applicable patches applied. Server has been hardened and verified via vulnerability scan. Running host-based IDS or integrity checker. Anti-virus signature exists and has been applied to target systems.

- 4: Current operating system with applicable patches applied. Operating system has been hardened. Anti-virus signature exists and has been applied to target systems.
- 3: Current operating system with fairly up-to-date patches applied. Anti-virus signatures are current.
- 2: Current operating system but missing some applicable patches. Anti-virus signature either does not exist or has not been applied to target systems.
- 1: Older operating systems, including Windows NT 3.51, Solaris 2.6, Windows 95/98/ME. No anti-virus software protection.

- *Network Countermeasures: What network-based preventive measures are in place?*
  (Value = Countermeasure)

  - 5: Restrictive (i.e., “deny all except what is allowed”) firewall. Firewall rules have been validated by penetration testing. All external connections including VPNs go through (not around) the firewall. Network-based IDS is implemented. Email gateway filters attachments used by this virus.
  - 4: Restrictive firewall. External connections (VPNs, wireless, Internet, business partners, etc.) are protected by a firewall. Email gateway filters attachments used by this virus.
  - 3: Restrictive firewall. Email gateway filters common executable attachments.
  - 2: Permissive firewall (i.e., ”accept all but”) or allowed service (e.g., HTTP, SMTP). Email gateway does not filter all attachments used by this virus.
  - 1: No firewall implemented. Email gateway does not filter any attachments.

Using the result from the formula defined above, the Alert Level Indicator would generally reflect severity levels as follows:

- Alert Level Indicator – Severity
  - Green – Low : -8 to -5
  - Blue – Guarded : -4 to -2
  - Yellow – Elevated : -1 to +2
  - Orange – High : +3 to +5
  - Red – Severe : +6 to +8