

Get to Know K12 SIX

K12 SECURITY INFORMATION EXCHANGE (K12 SIX)

AUGUST 29, 2023



K12 SIX Annual Sponsors



Today's Speaker





Doug Levin, Co-Founder and Director

- 30+ years working at intersection of education, technology, public policy, and research
- Formerly: EdTech Strategies, LLC (President), SETDA (Executive Director), NASBE (Deputy Director/COO), NCTA (Senior Director, Education Policy), AIR (Principal Research Analyst)
- Creator of *K-12 Cyber Incident Map*; frequent speaker and commentator
- Appointed CISA Cybersecurity Advisory
 Committee

Today's Agenda

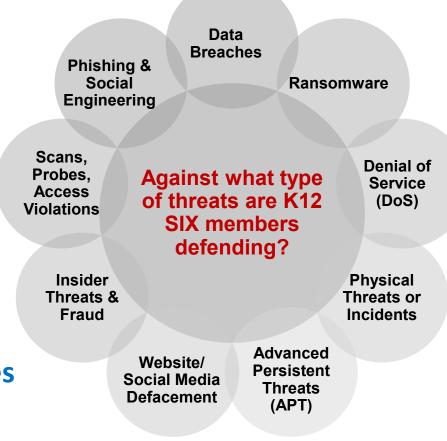


- About K12 SIX and GRF
- Membership Benefits
- Impact
- How to Join
- Free Resources/Upcoming Events

- A Global Resilience Federation (GRF) member community, K12 SIX is a real-time cyber threat intelligence sharing hub *exclusively for schools*, to aid in preventing and mitigating cyber threats.
- This non-profit member community provides cost-effective collective defense by crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security team.

Collective defense | Best practices | Model policies Professional development | Advocacy

https://www.k12six.org/member-benefits





Who We Are

- Under the umbrella of the Global Resilience Federation, an information sharing and analysis center (ISAC) for the U.S. K-12 sector
- Non-profit, membership community focused on cybersecurity (i.e., IT/data confidentiality, integrity, availability) capacity building
- Trusted partner in protecting your school community from emerging cybersecurity threats
- Thought leader, advocate for the cybersecurity needs of the K-12 community
- Funded via school system memberships, supplemented by sponsorships

Who We Aren't

- Not a seller/endorser of cybersecurity solutions
- Not focused on K-12 physical security, nor on cybersecurity workforce development
- Not a general-purpose association for educational technology, not solely focused on issues of student data privacy



K12 SIX membership is open to U.S. K-12 organizations, including:

- School districts
- Charter schools/charter management organizations
- Private/independent schools
- Regional education agencies
- State education agencies

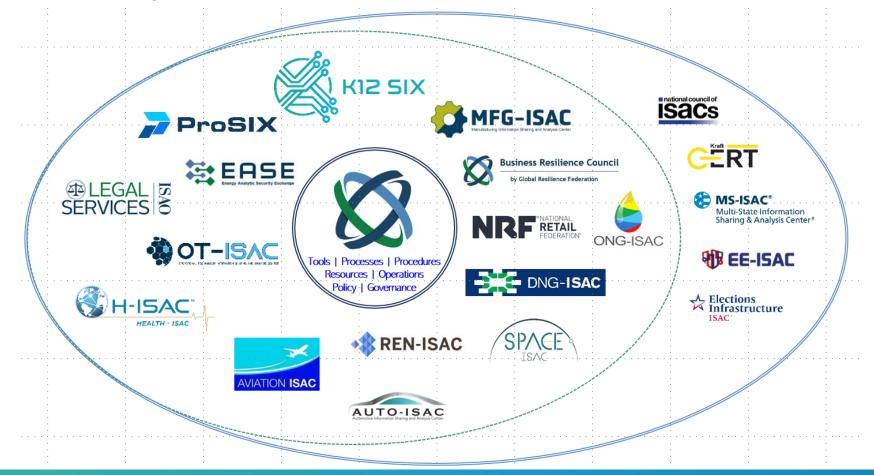
→ K12 SIX member school systems may designate MSP/outsourced K-12 IT staff as their K12 SIX representative.

 \rightarrow Exploring options to serve K-12 vendors/suppliers, non-U.S. school systems.

The Federation Advantage

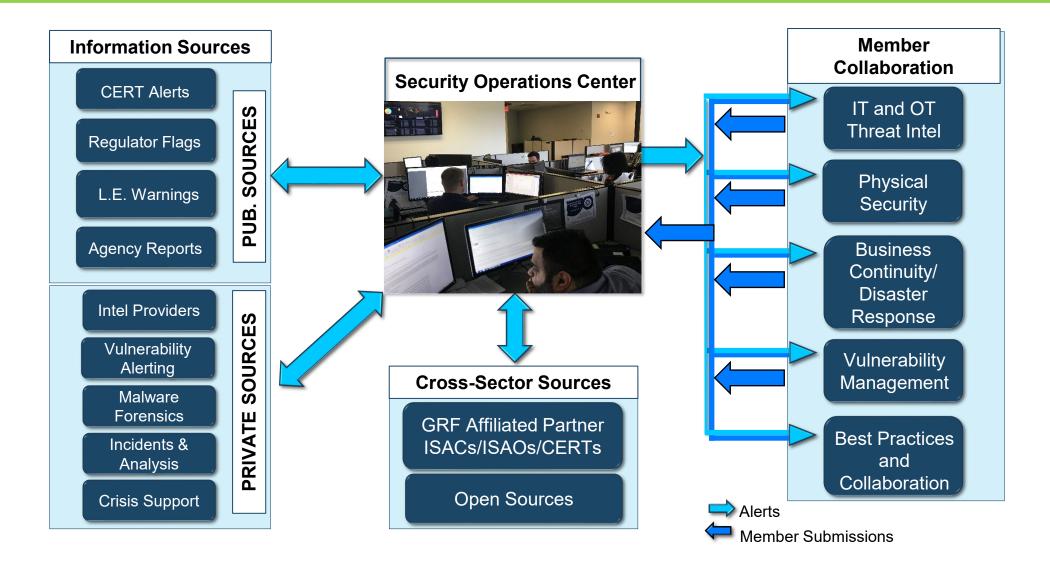


K12 SIX is a Global Resilience Federation (GRF) member community. GRF acts as an information hub: aggregating and analysing security information, disseminating actionable intelligence, and streamlining cross-sector collaboration.



Global Resilience Federation Sharing Pathways





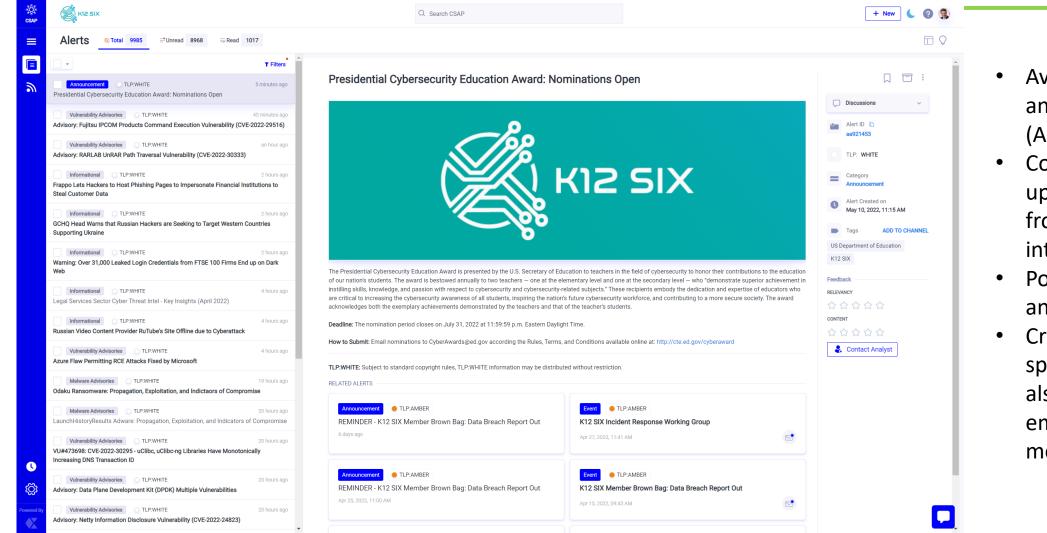
© 2023 K12 SIX



- K-12 focused cyber threat news, information, and analysis (continuously updated): news, events, incidents, threats, vulnerabilities, etc.
- Access to a secure, collaborative cyberthreat information sharing online portal and mobile app
- Summary weekly newsletters/reports, providing situational awareness on vulnerabilities, ransomware activity, and K-12 specific news
- Bi-weekly analyst-led threat briefings
- Weekly peer-to-peer 'water cooler'
- Anonymized/secure peer-to-peer threat sharing/request for information facilitation
- Opportunities to contribute: technical working group, meeting participation, public speaking, etc.
- Priority access to National K-12 Cybersecurity Leadership Conference

K12 SIX Cyware Situational Awareness Platform (CSAP): Primary Threat Intelligence Feed





- Available online and via mobile app (Android and iOS)
- Continuously updated, drawing from multiple intelligence sources
- Powerful search and filter functions
- Critical, K-12 specific alerts are also delivered via email to K12 SIX members

K12 SIX Cyware Situational Awareness Platform (CSAP): RSS Feed Manager



KIZ SIX	Q Search CSA	P + New 🤇 😨 🕵
Feeds All Feeds Dookmarked Trichived		Add or Manage
From all feed sources	CISA Alerts	Following
All-time Feeds	APR 27, 2022	
Malware	AA22-117A: 2021 Top Routinely Exploited Vulnerabilities	AA22-117A: 2021 Top Routinely Exploited Vulnerabilities
9	APR 20, 2022	
Webroot Blog	AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure	Original release date: April 27, 2022 Summary
Malwarebytes	APR 18, 2022	This joint Cybersecurity Advisory (CSA) was coauthored by cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom: the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Cyber Security Centre (ACSC),
Security News	AA22-108A: TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies	Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), and United Kingdoms National Cyber Security Centre (NCSC-UK). This advisory provides details on the top 15 Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors in 2021, as well as other CVEs frequently exploited.
Mark Reading	APR 13, 2022	exponer. U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities assess, in 2021, malicious cyber actors aggressively targeted newly disclosed critical software vulnerabilities against broad target sets, including public and private sector organizations worldwide. To a lesser extent, malicious cyber actors continued to exploit publicly
Bleeping Computer	AA22-103A: APT Cyber Tools Targeting ICS/SCADA Devices	known, dated software vulnerabilities across a broad spectrum of targets. The cybersecurity authorities encourage organizations to apply the recommendations in the Mitigations section of this CSA. These mitigations include applying timely patches
	AA22-083A: Tactics, Techniques, and Procedures of Indicted State-	to systems and implementing a centralized patch management system to reduce the risk of compromise by malicious cyber actors. Click here for a PDF version of this report.
ZUNE	Sponsored Russian Cyber Actors Targeting the Energy Sector	Technical Details
CISO News	AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers	Key Findings Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed
Tripwire - State of Security	MAR 15, 2022	vulnerabilities. For most of the top exploited vulnerabilities, researchers or other actors released proof of concept (POC) code within two weeks of the vulnerabilitys disclosure, likely facilitating exploitation by a broader range of malicious actors.
pprox Security on TechRepublic	AA22-074A: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and PrintNightmare Vulnerability	To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilitiessome of which were also routinely exploited in 2020 or earlier. The exploitation of older vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.
Vulnerabilities	FEB 26, 2022	Top 15 Routinely Exploited Vulnerabilities
	AA22-057A: Destructive Malware Targeting Organizations in Ukraine	Table 1 shows the top 15 vulnerabilities U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities observed malicious actors routinely exploiting in 2021, which include:
MITRE ATT&CK	FEB 24, 2022	• CVE-2021-44228. This vulnerability, known as Log4Shell, affects Apaches Log4j library, an open-source logging framework. An actor can exploit this vulnerability by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows a cyber actor to take full control over
Threatpost - Vulnerabilities	AA22-055A : Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks	the system. The actor can then steal information, launch ransomware, or conduct other malicious activity.[1] Log4] is incorporated into thousands of products worldwide. This vulnerability was disclosed in December 2021; the rapid widespread exploitation of this vulnerability demonstrates the ability of malicious actors to quickly weaponics known vulnerabilities and target organizations before they patch.
Threat Advisories	FEB 23, 2022 AA22-054A: New Sandworm Malware Cyclops Blink Replaces	• CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065. These vulnerabilities, known as ProxyLogon, affect Microsoft Exchange email servers. Successful exploitation of these vulnerabilities in combination (i.e., vulnerability chaining) allows an unauthenticated cyber actor to execute arbitrary code on vulnerable
(CISA Alerts	VPNFilter	 Exchange Servers, which, in turn, enables the actor to gain persistent access to files and mailboxes on the servers, as well as to credentials stored on the servers. Successful exploitation may additionally enable the cyber actor to compromise trust and identity in a vulnerable network. CVE-2021-34273, CVE-2021-34273, CVE-2021-31207. These vulnerabilities, known as ProxyShell, also affect Microsoft Exchange email servers. Successful exploitation
-	FEB 16, 2022	of these vulnerabilities in combination enables a remote actor to execute arbitrary code. These vulnerabilities reside within the Microsoft Client Access Service (CAS)
Personal Blogs	AA22-047A: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology	which typically runs on port 443 in Microsoft Internet Information Services (IIS) (e.g., Microsofts web server). CAS is commonly exposed to the internet to enable use to access their email via mobile devices and web browsers.

Allows easy way to centralize tracking of public threat feeds and cybersecurity news

K12 SIX Cyware Situational Awareness Platform (CSAP): Crisis Notification System



	C	Search CSAP		+ New 🤇 🔋 📕	
Alert Categories > Toggle settings for alert categories.	Crisis Profile			Edit	
 Channels > Manage settings for channels. Crisis Profile > Manage emergency contact informati 	1. Select Business Hours Please enter your business hours, time zone, and voice preference. Start Time 08:00 Time Zone (GMT- 5:00) Eastern Time (US and Canada) Voice Preference Mary	2. Add Contact Numbers Please enter the emergency contacts Code* +1		Send SMS	 Allows for flexible 24/7 outreach to K12 SIX members (or their designees) in the event of a crisis
	3. Set Call Priority Order Please specify the order of call priority for your emergency contacts. Priority Weekday (Business Hour 1 5712671288	s) Weekday (5712671288	(After Business Hours) S712671288	Weekend	
V V V V V 3.0					

K12 SIX Cyware Situational Awareness Platform (CSAP): Document Library



KIZ SIX		Q Search CSAP	Q Search CSAP		+ New 🤇 🤇		
Doc Librar	ry						
All Files My	y Files & Folders	Shared with me Starred					
▼ Filters							
Starred	Туре 👙	Name 🗇	Size 🇅	TLP	Owner	Last Modified 🍦	Actions
	19	Attachments from Member Submission	-		A Staci Elliott	Jan 21, 2022, 03:04 PM	e (i)
	13	Cybersecurity Best Practices	-		A Jinny Kang	Oct 14, 2020, 12:30 PM	e) (j
	3	GRF Business Reslience Council - Geopolitical Reports	-		A Staci Elliott	Apr 07, 2022, 10:22 AM	c> (j
☆	141	GRF COVID-19 Reports	-		A Jinny Kang	Sep 30, 2020, 11:20 AM	c)
☆	0	GRF Monthly Newsletter	-		A Staci Elliott	Apr 04, 2022, 12:23 PM	(i)
☆		K12 SIX Essential Protections Series	-		A Doug Levin	Sep 03, 2021, 12:16 PM	cə (j)
	•	Member Resources	-		A Jinny Kang	Sep 17, 2020, 11:26 AM	(i)
	33	Monthly Member Meeting Archives	-		A Jinny Kang	Sep 23, 2021, 11:26 AM	(i)
	74	MS-ISAC Alerts	-		A Arshad Somani	Feb 22, 2021, 04:52 PM	c) (j
	•	Public Partner Alerts	_		A Arshad Somani	May 03, 2021, 10:38 AM	ed (j

Central repository for all important reference documents, including archives of member meetings and events

K12 SIX Cyware Situational Awareness Platform (CSAP): Event Calendar

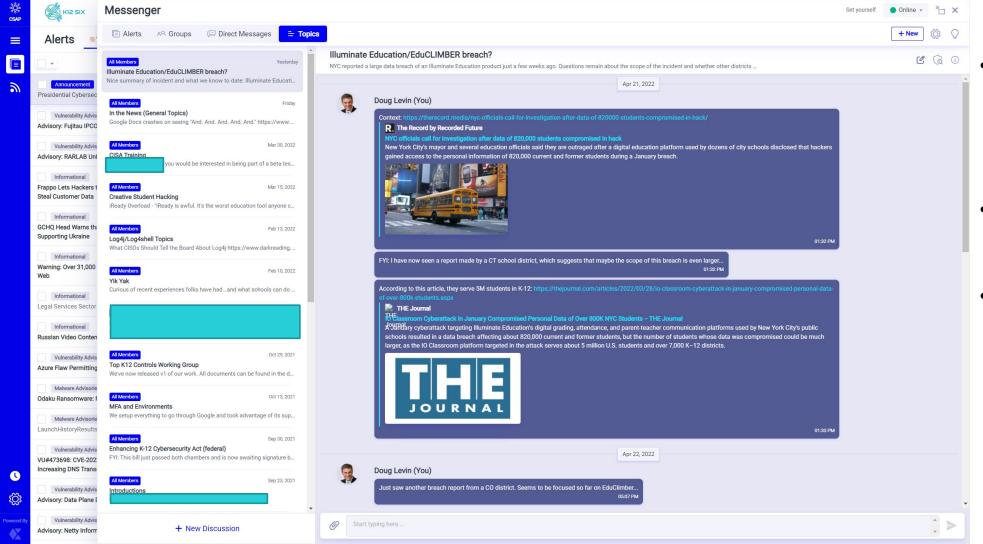


KIZ SIX		Q Search CSAP		Download as ICS file
Events				K12 SIX Member Brown Bag: Data Breach Report Out
Past Events 3	Upcoming Events 1			Starts Thu May 05, 2022 11:00 am Ends Thu May 05, 2022 12:00 pm
May V 2022 May Non Tue Wed Thu Fit	Sat Sun	Sun Mon	Tue Wed	Location Microsoft Teams No URL Provided
25 25 27 28 29 29 2 2 3 4 5 6 9 10 11 12 13	7 8	Open Office Hours Virtual Ask-a-CT		K12 SIX ✓ Attend ? Maybe X Not Attending
16 17 18 19 20 23 24 25 26 27 30 31 1 2 3	21 22 28 29 4 5	8 9	70 77	About Event ort out on a recent district data breach staff will share information on the attacker's TTPs, investigatory steps taken, resources used, cyber insurance engagement, and
Jpcoming Events GRF Monthly Cross-Sector Collaboration Call May 12, 2022 11:00 am - 12:00 pm		(Open Office Hours Virtual Ask-a-CI)		GRE Mo disclosure of the incident to the public and those directly impacted. The goal is to share knowledge gained and to also learn from others who may have had similar experiences. We will use Microsoft Teams for this meeting:
Single day event		15 16 Open Office Hours Virtual Ask-a-CI	17 1	K12 SIX Member Brown Bag: Data Breach Report Out Thursday, May 5, 11-12PM ET
				Microsoft Teams meeting Join on your computer or mobile app
		22 23 Open Office Hours Virtual Ask-a-CI)	24 ([TLP AMBER] K12 SIX Monthly Men	25 Click here to join the meeting TO call in (audio only) +1.540-491-4128,615566981# United States, Roanoke Phone Conference ID: 615 566 981# Eind a local number I. Reset PIN
		29 30	31	Learn More Meeting options

- Captures all • regularly scheduled and ad hoc member meetings and events
- Exportable to K12 SIX member calendars

K12 SIX Cyware Situational Awareness Platform (CSAP): Portal Messenger





- Real-time secure chat functionality, similar to Slack/Teams
- Available online and via mobile app
- Ability to submit threat intel and requests for information

K12 SIX Impact



- Definitive source for publicly-disclosed K-12 cybersecurity incidents (K12 Cyber Incident Map)
- Publisher of K-12 Essential Cybersecurity Protections suite
- RFIs: cyber insurance requirements, MFA implementation, K-12 cybersecurity policies, pros/cons of cybersecurity roadmap, SLCGP implementation, etc.
- Confidential aid to K-12 cyber incident victims (proactive/upon request, districts/vendors)
- Crowdsourced the Log4j vulnerability status of commonly used K-12 software (both in the classroom and for operations/administration)
- Partnerships with the federal government (ED, CISA) and national/state associations (SETDA, AASA, METAA, etc.)
- Keynotes, presentations; work widely cited by policymakers, media

How to Join K12 SIX



- Visit <u>www.k12six.org</u>
- Click 'Join' button in upper right corner of your screen
- Fill out online application, pay annual membership dues (based on student enrollment/organization type)
- Schedule orientation

K12 SIX Public Resources

- The K-12 Cyber Incident Map: https://www.k12six.org/map and "State of K-12 Cybersecurity: Year in Review" report series https://www.k12six.org/the-report
- K12 SIX 'Essentials' Series: <u>https://www.k12six.org/essentials-</u>
 <u>series</u>
 - Cybersecurity Frameworks: What K-12 Leaders Need to Know
 - K-12 Essential Cybersecurity Protections Series
 - K-12 Cyber Incident Response Runbook
 - 2024 K12 SIX Annual Conference (Savannah, Feb 13-14, 2024)





Webinar Series: https://www.k12six.org/webinars

- 9/5: Unifying your Cybersecurity Posture at the Identity: ٠ SIEM/SOAR/SOC for K-12
- 9/12: Leveraging AI to Defend Against Back to School Threats •

© 2023 K12 SIX

• 9/26: The Four Pillars of School Security





TLP:CLEAR



Questions?

Membership/partnership inquiries: <u>info@k12six.org</u> or <u>https://www.k12six.org/contact</u>

