CISA Automated Indicator Sharing (AIS)

PLATFORM FEATURE UPDATE

Adlumin's Threat Intelligence Scanner now includes threat intel feed data from the Cybersecurity and Infrastructure Security Agency (CISA).

CISA, which operates under the authority of the Department of Homeland Security, builds the national capacity to defend against cyberattacks. They also work with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

Adlumin is now a participating member in CISA's Automated Indicator Sharing (AIS) program. AIS enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks. The AIS community includes private sector entities; federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs).

By incorporating AIS feed data, Adlumin further strengthens its leading-edge threat intelligence technology, ensuring that our customers are able to detect and respond to threats in real-time.

9	Settings	Learning Center	Reports -	Tools -	Modules -	Tenants -	Support 🖉 😋 Ellen Loughlin 🕫
5							
	🕣 Thr	eat Intelligen	ce Portal				
(i):	Q, IP Search	Q, File Hash Search	< Information	Sharing			
	Enter an	IP Address			Search		
<u>.</u>							I Threat Intelligence News Feed
ų.							
ń	 across multiple threat data sources. Additionally, incoming device data from firewalls, VPN servers, and network security applicates is scamed using indicators of compromises from CIS/AUF. Automated Indicator Sharing (AB), a Oybersecurity and Infrastructure Security Agency (CIGA), capability, mathes the machine actuations of threat indicators of demonstration defension measures to help protect participants of the AB community and ultimately induce the prevalence of cyberstrates. The AIS community includes primes exoch refiles; electratic departments and analysis centers (ISACs) and information starting and analysis granizations (ISACs); and foreign partners and October 7, 2021 						Vulnerability scanners are not enough, according to an expert who champions an ali-encompassing holistic approach to vulnerability management as a means to eliminate surprises.
EQ.							ExtraHop adds new threat hunting and network advisory services to Reveal(x) October 7, 2021 The additor of Revealtic Advisor serves to the Revealtic 360 network selection and resonate too holes organizations proaddeth manage oversecure
	Adiumin users will receive notifications in the form of a detection if any incoming event contains an IP eddress that OTX has deemed potentially malicious.					ent contains an IP	The abatish of Reveals), Advisor services to the reveal(x) southework detection and response tools helps organizations protectively manage cybersecurity hygiene and accelerate incident negocies.
		S :	HXERID		TOTAL		Threat Source newsletter (Oct. 7, 2021) October 7, 2021
							Newsletter compiled by Jon Munshaw.Good afternoon, Talos readers. Every day, we see mountains and mountains of data. So how do we comb through all of it to trind out what's important to customers and users? Well, there are many ways, but we wante
							FIN12 hits healthcare with quick and focused ransomware attacks October 7, 2021

You can access this new feature under *Threat Intel* on the left sidebar menu.

