Article Information

Authors: Michael Bacina, Steven Pettigrove, Jake Huang
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Security Alliance launches ISAC to combat cyber threats in Web3

The Security Alliance and nearly two dozen leading blockchain organisations have launched an Information Sharing and Analysis Center to enhance real time sharing of threat intelligence, and combat cyber hacks and financial crime in Web3.

Following a request for comment on a *Whitehat Safe Harbor Agreement* – a new security approach to assist in reducing blockchain hacks in February, Web3 security research group Security Alliance (**SEAL**) has launched an Information Sharing and Analysis Centre (**ISAC**) to enhance real time sharing of threat intelligence, and combat cyber hacks and financial crime in Web3.

ISAC is modelled on the ISAC framework first pioneered by the Financial Services ISAC (**FS-ISAC**) in 1999. ISACs are non-profit, member-driven organisations focused on information sharing in "critical infrastructure" sectors – including technology, communication and financial services. The function of an ISAC is to collect, analyse, and distribute cyber and related threat information, which would otherwise remain siloed, responsibly and via secure networks. This is the first ISAC purpose built for Web3.

The SEAL ISAC is designed to:

1. Enhance information sharing in threat intelligence through an Open Cyber Threat Intelligence Platform (**OpenCTI**), so members can easily and safely share context, external references, observables (such as cryptocurrency wallet addresses), entities, and relationships.
2. Provide timely threat analysis and alerts to members to help them anticipate, identify, and mitigate potential attacks.
3. Disseminate best practices and guidelines for cybersecurity to help members implement effective security measures and policies, including playbooks for incident response.
4. Coordinate response mechanisms for major security incidents, such as exchange hacks or network attacks, facilitated through the SEAL 911 Emergency Hotline.
5. Offer educational resources and training programs tailored to various stakeholders to raise awareness about security best practices and the latest threats.

SEAL ISAC is:

- Membership based and free to access
- Purpose-built for crypto on open source solutions
- Supportive for both centralized and decentralized entities
- Global from day 1
- Integrated with SEAL 911 and other SEAL initiatives

Early participants in SEAL ISAC include security teams from nearly two dozen organizations including Chainalysis, Ethereum Foundation, Filecoin Foundation, MetaMask, Polygon, Scroll, and Uniswap Labs. Additional participants are listed on SEAL ISAC's website. SEAL ISAC is also built with support from leaders in Ethereum, Polkadot, Solana, Filecoin, and other ecosystems.

The Security Alliance is the coalition behind several other security initiatives, including the Whitehat Safe Harbor, SEAL Wargames, which allows developer teams to simulate security incident scenarios, and the SEAL 911 Emergency Hotline, which enables users, developers and security researches who need access to urgent security advice, help with disclosing a

critical vulnerability, or to connect with a team of carefully vetted expert volunteers. Over the past 6 months, SEAL 911 has helped disrupt, intercept, and remediate several hacks, recovering over USD 50 million in crypto-assets.

Web3 security teams can apply to join SEAL ISAC here.

Piper Alderman is an advisor to the Security Alliance and was pleased to collaborate with SEAL on the Whitehat Safe Harbor Agreement alongside leading blockchain and cyber security lawyers including Gabriel Shapiro, the Lexpunk coalition, Debevoise & Plimpton LPP, and the policy teams at Paradigm and A16Z Crypto, among many others.