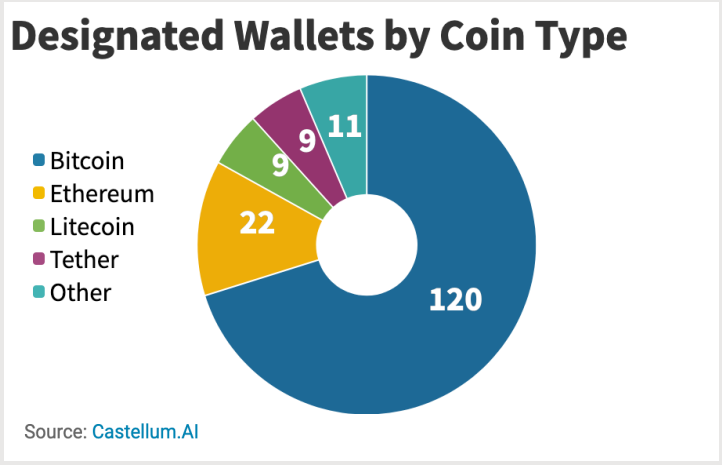
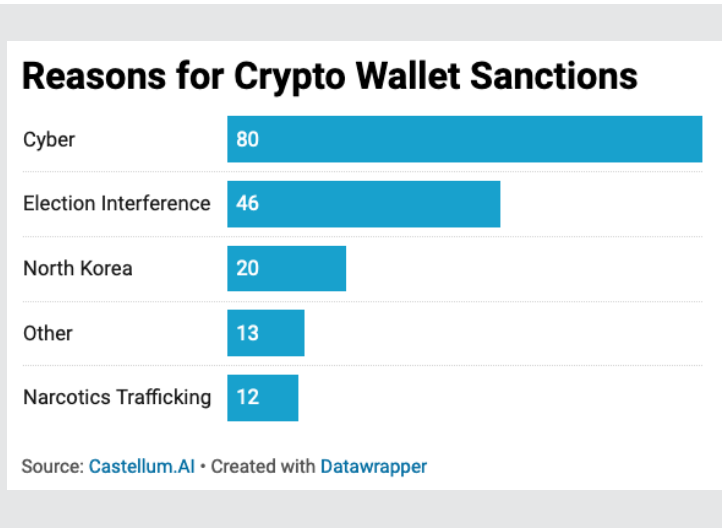
CASTELLUM.AI

INCIDENT RESPONSE & SANCTIONS COMPLIANCE

The US started sanctioning cryptocurrency addresses in 2018, growing the number to over 170 as of January 2022. In September 2021, Treasury updated an advisory forbidding ransomware payments to sanctioned parties and sanctioned jurisdictions (e.g. Iran). Castellum.AI helps clients quickly and cost-effectively comply with the law when navigating an already high-risk and time-sensitive situation.

- **CHALLENGE**: Incident response companies sending ransomware payments on behalf of clients must comply with sanctions regulations.
- **SOLUTION**: OFAC encourages incident response firms to screen payments, wallet addresses and more as part of a risk-based compliance program.
- **IMPLEMENTATION**: Screening identifying information, such as wallet addresses, against sanctions lists is a key component of a risk-based compliance program.





HOW WE HELP:

MEET OFAC REQUIREMENTS
Our Investigator Platform lets users easily screen crypto wallet addresses, individuals and locations to assess sanctions risk.

MEET INSURANCE REQUIREMENTS
Our one-click audit reports meet cyber insurance conditions for claim resolution and payout.

MOVING FORWARD
The US and other governments have issued $2.5 bn in crypto-focused fines, and they're just getting started. In addition to wallets, OFAC designated two crypto exchanges.