TECH TALK

MAGNET FORENSICS®

Getting the Most Benefit from AXIOM Cyber for Remote Acquisition

PRESENTED BY Rhys Tooby

Rhys Tooby

Manager, Solution Consultants

✉ Rhys.tooby@magnetforensics.com

in rhystooby

Career

South Wales Police

- Digital Forensics Investigator – 7 years
- Manager Digital Forensics & Cyber Crime Unit – 5 years

Magnet Forensics

- Manager of Solution Consultants EMEA – 2 ½ years

Qualifications

- BSc in Information Technology
- AXIOM, Encase, Cellebrite, XRY, Oxygen, Vehicle Telematics Berla iVE and many more

Cybercrime Trends

Cyber-attacks are the fastest growing crime. They’re increasing in frequency, size, complexity, and cost to the victim organization.

1 in 5 organizations lose more $1 million a year to fraud

70%

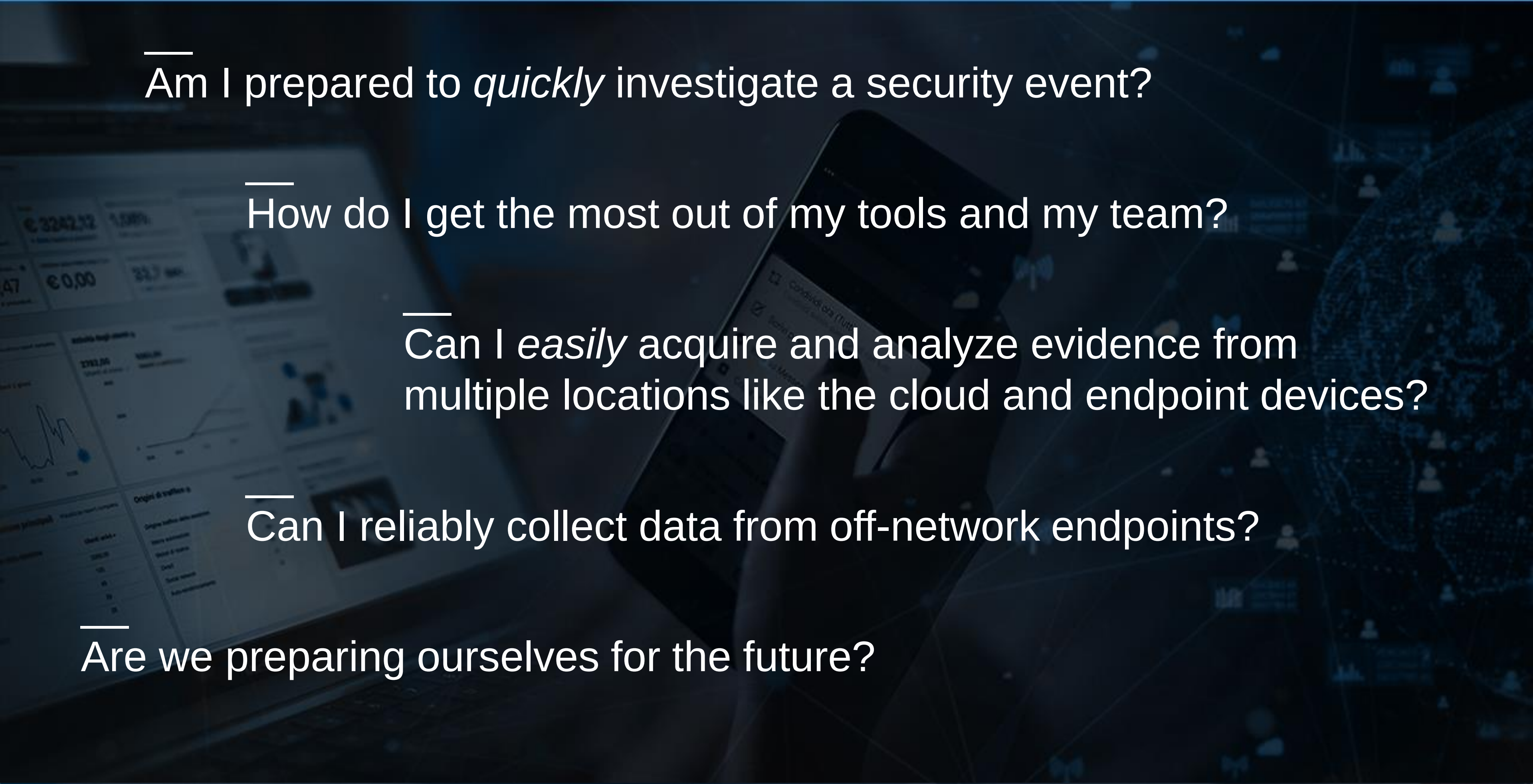
People who are bullied end up leaving their employer. Costs include retraining, and potential Wrongful Termination lawsuits

= +80%

IP can be +80% of a company’s total value and it’s at risk from outsiders and insiders alike

$3.92M

Average cost of a data breach in 2019
An average of +25k records are compromised at a cost of $150 each



Am I prepared to *quickly* investigate a security event?

How do I get the most out of my tools and my team?

Can I *easily* acquire and analyze evidence from multiple locations like the cloud and endpoint devices?

Can I reliably collect data from off-network endpoints?

Are we preparing ourselves for the future?

MAGNET AXIOM™ CYBER

Simplify digital forensics with AXIOM Cyber.

AXIOM Cyber is a robust digital forensics solution for businesses that simplify your investigations—so you can get to the truth quickly and prevent further damage.

Use AXIOM Cyber for All Your Investigations

FRAUD

- Steal or transfer money
- Payroll schemes
- Document modification
- Unrecorded or understated revenue
- Forgery

EMPLOYEE MISCONDUCT

- Cyber bullying
- Sexual harassment
- Workplace incivility
- IT policy violations
- Prohibited websites
- Potentially unwanted programs

INCIDENT RESPONSE

- Network intrusions
- Malware and Ransomware
- Phishing
- Advanced Persistent Threats
- Business Email Compromise

IP THEFT

- PII (customer or employee)
- Trade secrets
- Proprietary software or source code
- Highly sensitive documents and files

Covert Remote Collection

Remotely collect individual files, targeted locations, or the full disk, and memory

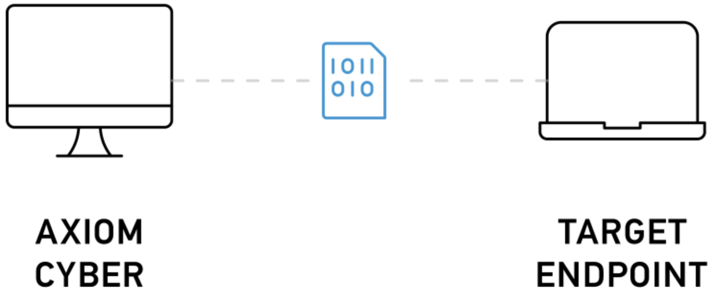
Reliably collect data from on- &off-network endpoints

Remotely collect files from Macs including those with T2 security chips and SIP enabled

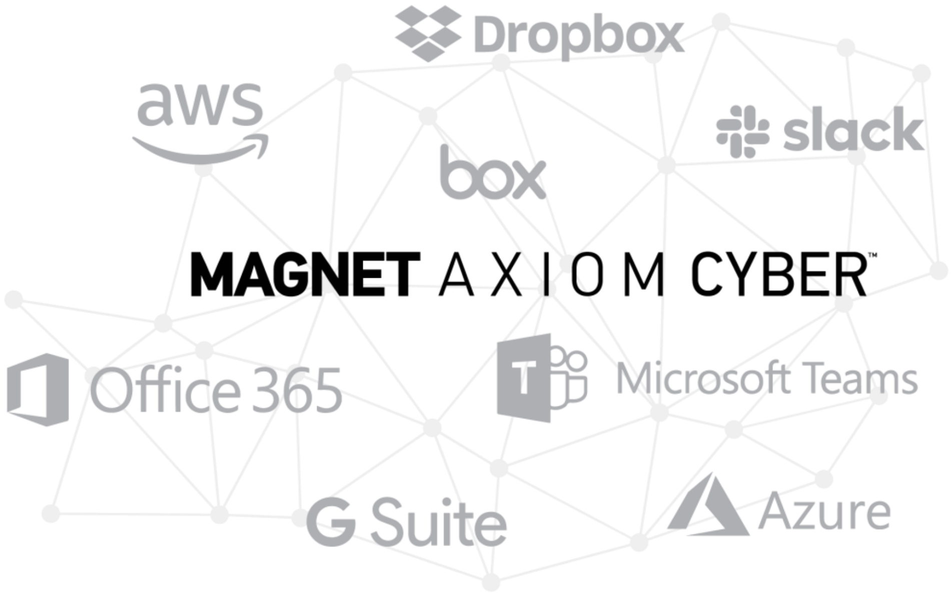
Logical acquisitions are written to forensically sound, open source format: AFF4-L

Automatically reconnect to target endpoint if it goes offline and resume collections from where it left off

Configurable, on-demand agent



Support for the Corporate Cloud



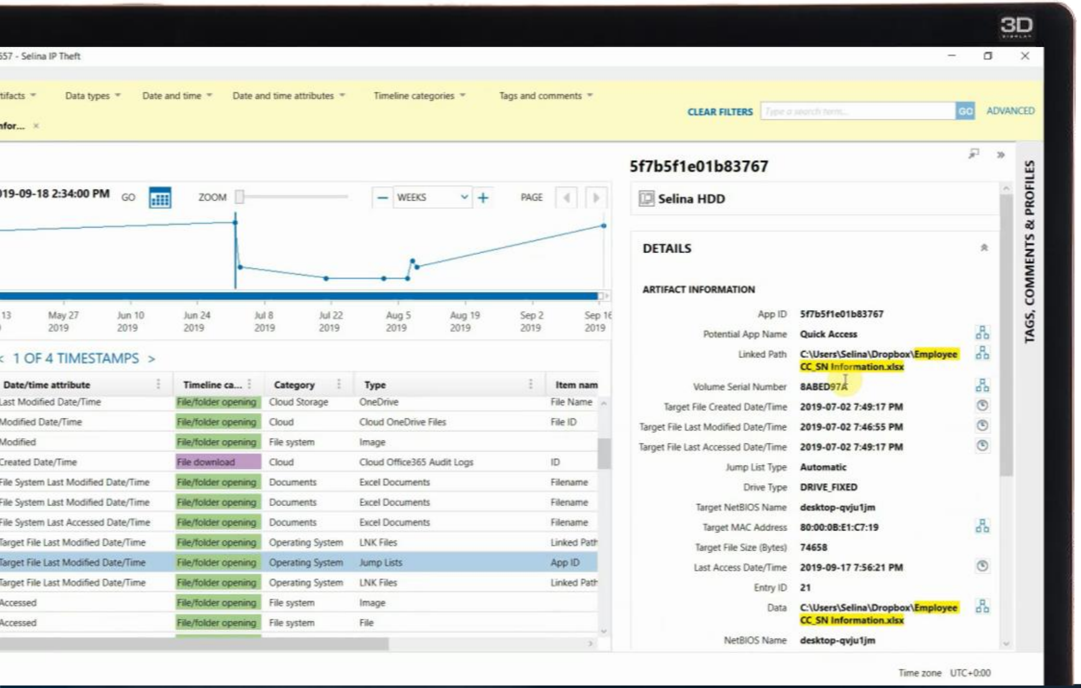
Admin credentials to acquire from Office 365, G Suite, and Box.com

Collect data from corporate cloud storage platforms: AWS (S3 and EC2) and Azure VM Images

Corporate communication tools: MS Teams, Slack, Zoom, and more

Acquire from social media and other cloud services with user credentials

Reduce Complexity



< 1 OF 4 TIMESTAMPS >

Date/time attribute	Timeline ca...	Category	Type	Item nam
Last Modified Date/Time	File/folder opening	Cloud Storage	OneDrive	File Name
Modified Date/Time	File/folder opening	Cloud	Cloud OneDrive Files	File ID
Modified	File/folder opening	File system	Image	
Created Date/Time	File download	Cloud	Cloud Office365 Audit Logs	ID
File System Last Modified Date/Time	File/folder opening	Documents	Excel Documents	Filename
File System Last Modified Date/Time	File/folder opening	Documents	Excel Documents	Filename
File System Last Accessed Date/Time	File/folder opening	Documents	Excel Documents	Filename
Target File Last Modified Date/Time	File/folder opening	Operating System	LNK Files	Linked Path
Target File Last Modified Date/Time	File/folder opening	Operating System	Jump Lists	App ID
Target File Last Modified Date/Time	File/folder opening	Operating System	LNK Files	Linked Path
Accessed	File/folder opening	File system	Image	
Accessed	File/folder opening	File system	File	

5f7b5f1e01b83767

Selina HDD

DETAILS

ARTIFACT INFORMATION

App ID	5f7b5f1e01b83767
Potential App Name	Quick Access
Linked Path	C:\Users\Selina\Dropbox\Employee CC_SN Information.xlsx
Volume Serial Number	8ABED97A
Target File Created Date/Time	2019-07-02 7:49:17 PM
Target File Last Modified Date/Time	2019-07-02 7:46:55 PM
Target File Last Accessed Date/Time	2019-07-02 7:49:17 PM
Jump List Type	Automatic
Drive Type	DRIVE_FIXED
Target NetBIOS Name	desktop-qvju1jm
Target MAC Address	80:00:0B:E1:C7:19
Target File Size (Bytes)	74658
Last Access Date/Time	2019-09-17 7:56:21 PM
Entry ID	21
Data	C:\Users\Selina\Dropbox\Employee CC_SN Information.xlsx
NetBIOS Name	desktop-qvju1jm

Time zone UTC+0:00

Artifacts-first approach surfaces relevant evidence

Build timelines to pin-point security events

Visualize connections between evidence items

Leverage AI to find pictures and inappropriate chats

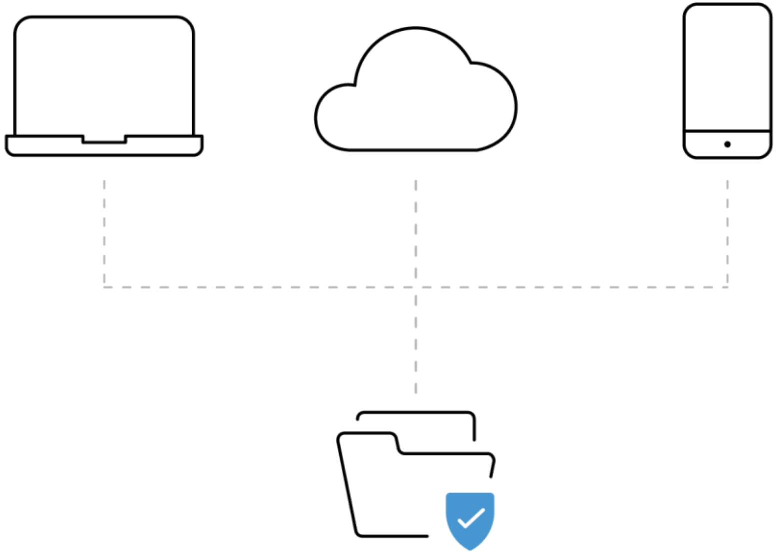
Easy-to-understand reports for non-technical stakeholders

Get All The Evidence You Need

Bring together evidence from Macs, PCs, mobile devices, and cloud sources in a single case file

Acquire unencrypted collections of files from encrypted drives

Save time and see the whole picture with Analytics features (Timeline, Connections, Magnet.AI) that can be applied to data from all sources



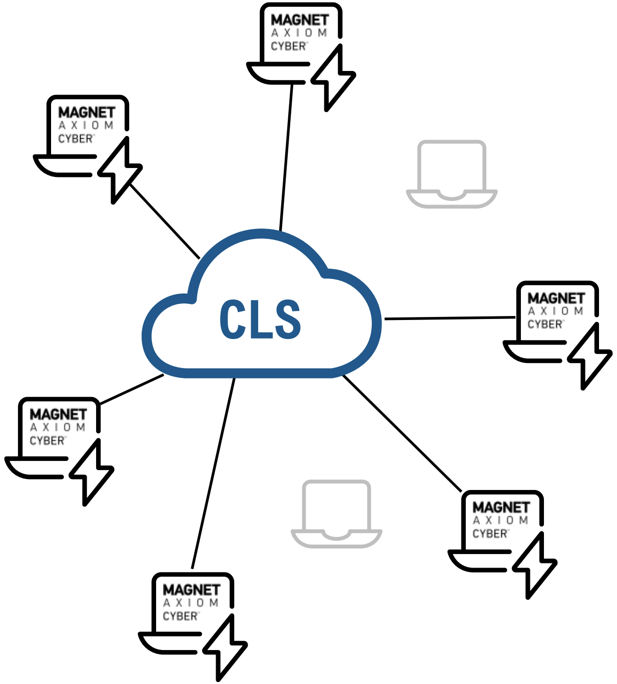
Cloud License Server (CLS)

Enables off-network collection and the simplified ability to run AXIOM Cyber in the Cloud (AWS EC2 or Microsoft Azure)

Flexibility! Especially now when many are working from home

Get the most value out of every license

Be online to check-in/out licenses, work offline if needed



Example of a 6 seat CLS license

DEMO

TECH TALK

MAGNET FORENSICS®

To Acquire, or Not to Acquire, That Is the Question

PRESENTED BY Rhys Tooby

RESPONSE TIME IS CRITICAL

Deep dive forensic analysis of endpoints takes time and resources

- Employees are more remote than ever before
- Sending data acquisition kits is time and cost prohibitive
- Remotely acquiring data from an endpoint takes hours

The average annual cost of insider threats is

$11.45 million

ObserveIT (2020). The Real Cost of Insider Threats in 2020.

Do you have the right tools to quickly triage?

MAGNET IGNITE™

Magnet IGNITE is a cloud-based triage tool that enables you to quickly understand your next steps with fast remote scans of endpoints.

FAST

Perform fast, remote triage of endpoints to know if a full forensic analysis is needed.

CLOUD BASED

Eliminate overhead costs with a cloud-based tool accessible from a web browser.

EFFICIENT

Reduce downtime by creating one agent to run on multiple endpoints at the same time.

Magnet IGNITE helps identify instances of

- Data exfiltration
- IP theft
- Misuse of corporate assets
- Incident Response from both internal and external bad actors

MAGNET IGNITE™

We welcome your feedback.

Please contact us for demo or to share your feedback at:

ignite@magnetforensics.com

magnetforensics.com/products/magnet-ignite

DEMO

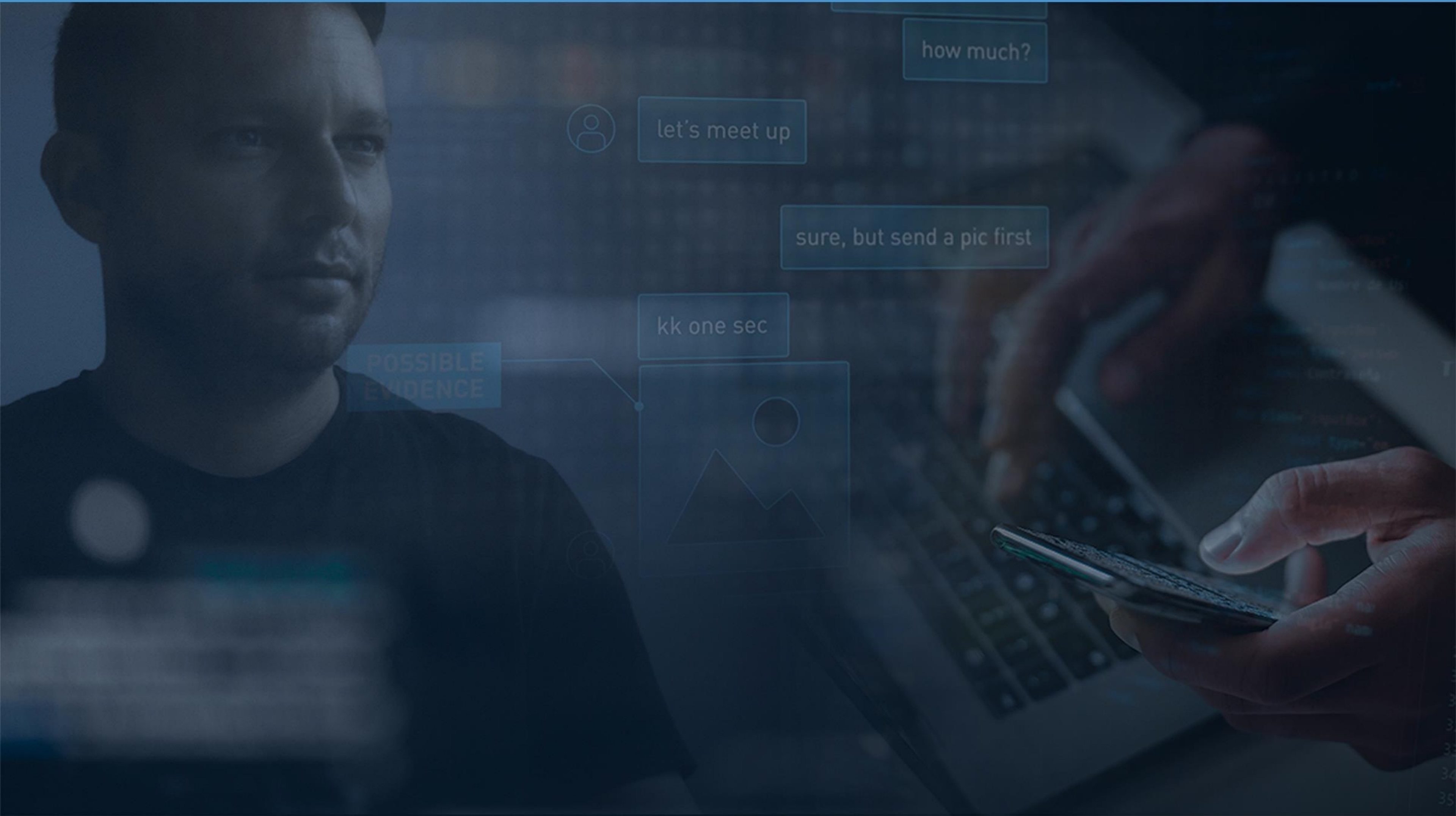
how much?

let's meet up

sure, but send a pic first

kk one sec

TECH **TALK**



how much?

let's meet up

sure, but send a pic first

kk one sec