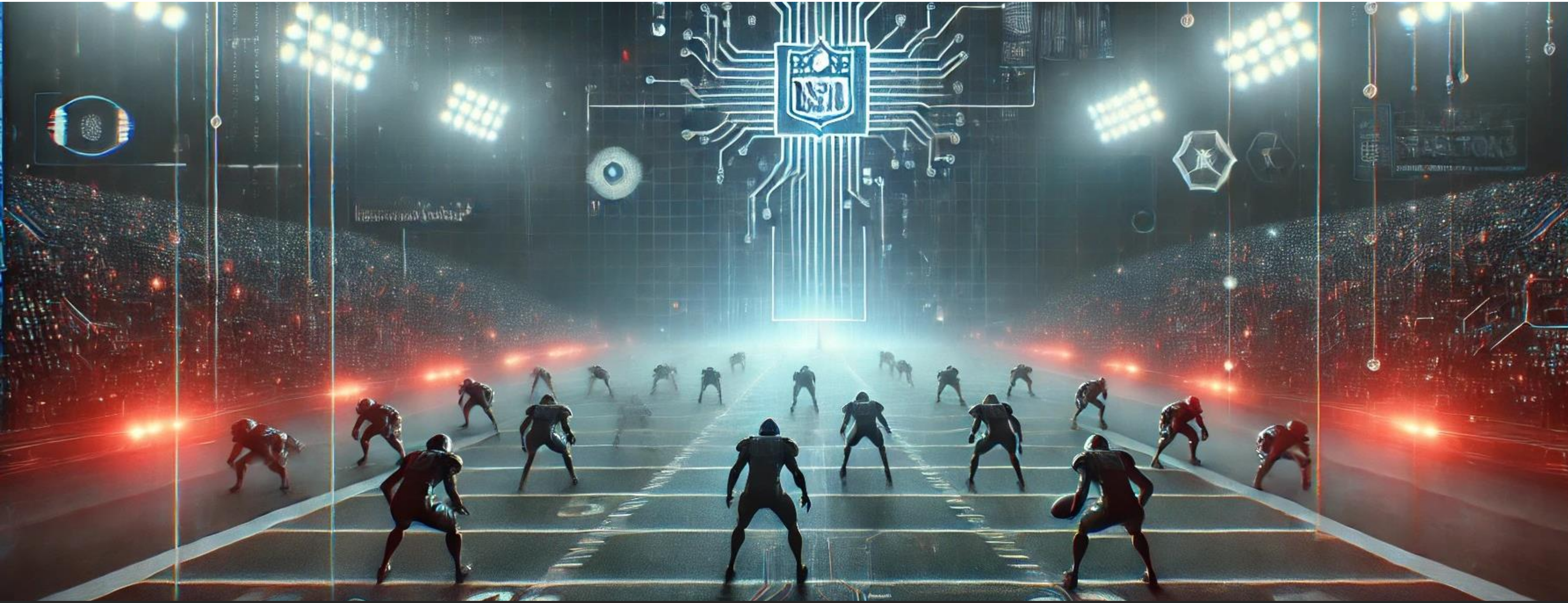
Operating in the Red Zone: Financial Investigations in Hostile Digital Territory



REPLICA™

POWERED BY GREY MARKET LABS

Frank Gentile

- Director of Customer Success for Grey Market Labs for the past 4 years
- 15+ years in CS at Cyber product companies – IBM, Carbon Black, Replica Cyber
- I work closely with our customers on their mission sets – what works, what doesn't, what capabilities are critical. Data mobility, policy restrictions, collaboration, automations.

REPLICA™

The Current Landscape: By the Numbers

$3.1 billion

Losses from 1,921 fraud cases analyzed by ACFE in 2024

1 in 3

People who reported fraud lost money (up from 1 in 4 last year)

70%

Fraud victims reported losses via social media - $1.9B total

$4.88 million

Average cost of a data breach (up from $4.45 million in 2023)

258 days

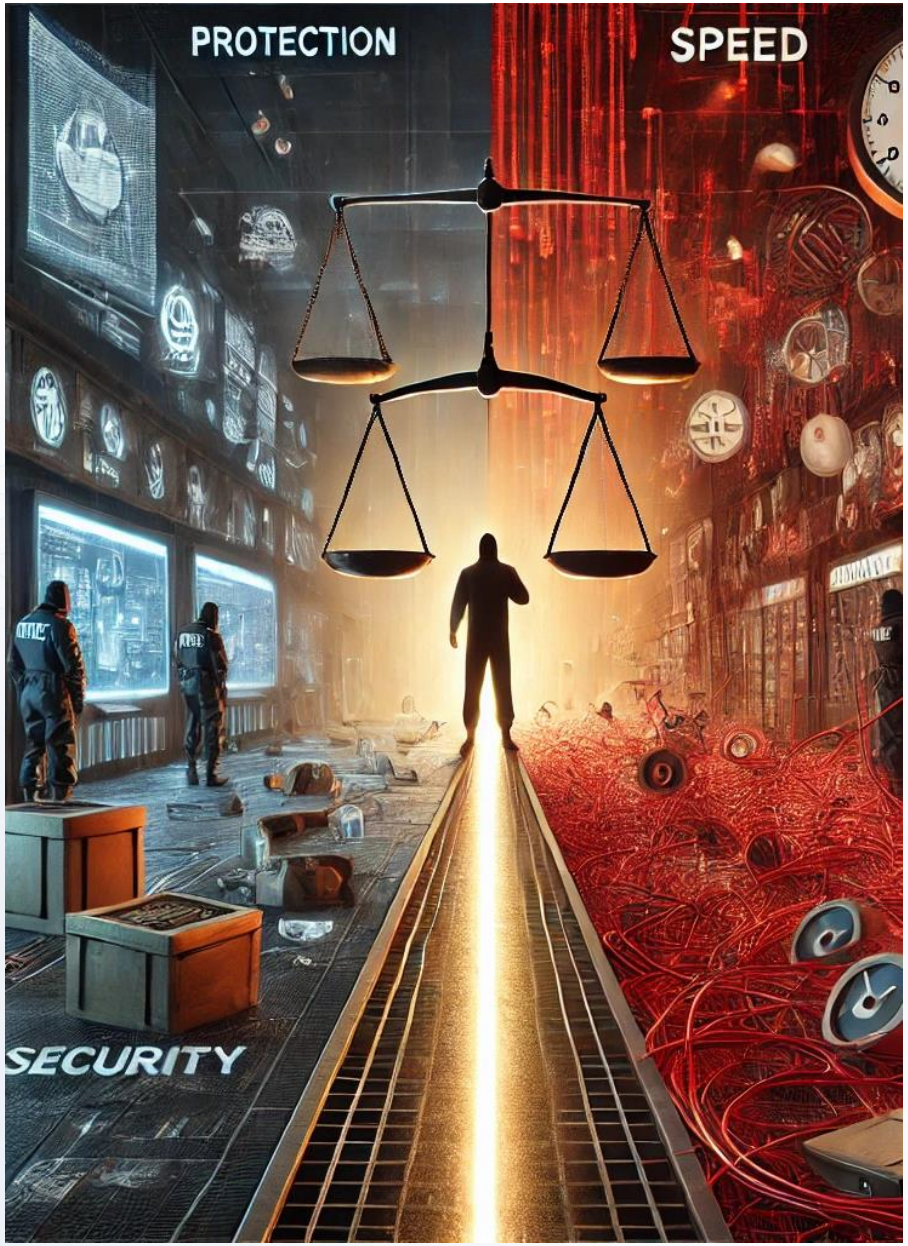
Mean time to identify and contain a breach

53%

Organizations facing critical security skills shortages

The Challenge: Security Without Compromise

Financial investigators face the constant challenge of balancing security and compliance with agility and efficiency. Finding equilibrium between protecting sensitive data and empowering investigative teams requires eliminating traditional security compromises.



Challenge #1: Data Access & Attribution

- Websites use attribution as its first line of defense

- Typical identifiable data points include (but aren't limited to):
  - IP range of requesting browser
  - Browser accept headers
  - Geo-location data
  - User agent strings
  - Other host "attributes" – e.g. language and font packs, clock time zones

- Hard target countries will often employ additional layers of validation before serving up information

Current Approaches to Attribution

Browser Incognito Mode

- Still trackable
- No real anonymity vulnerable to malware
- No identity control

Browser Extensions

- Only surface-level spoofing
- Still finger-printable
- May trigger suspicion
- Limited effectiveness

VPNs

- Shared/flagged IPs
- No protection against malware
- No identity control
- VPN providers may log activity

REPLICA™

Challenge #2: Mobility & Device Access

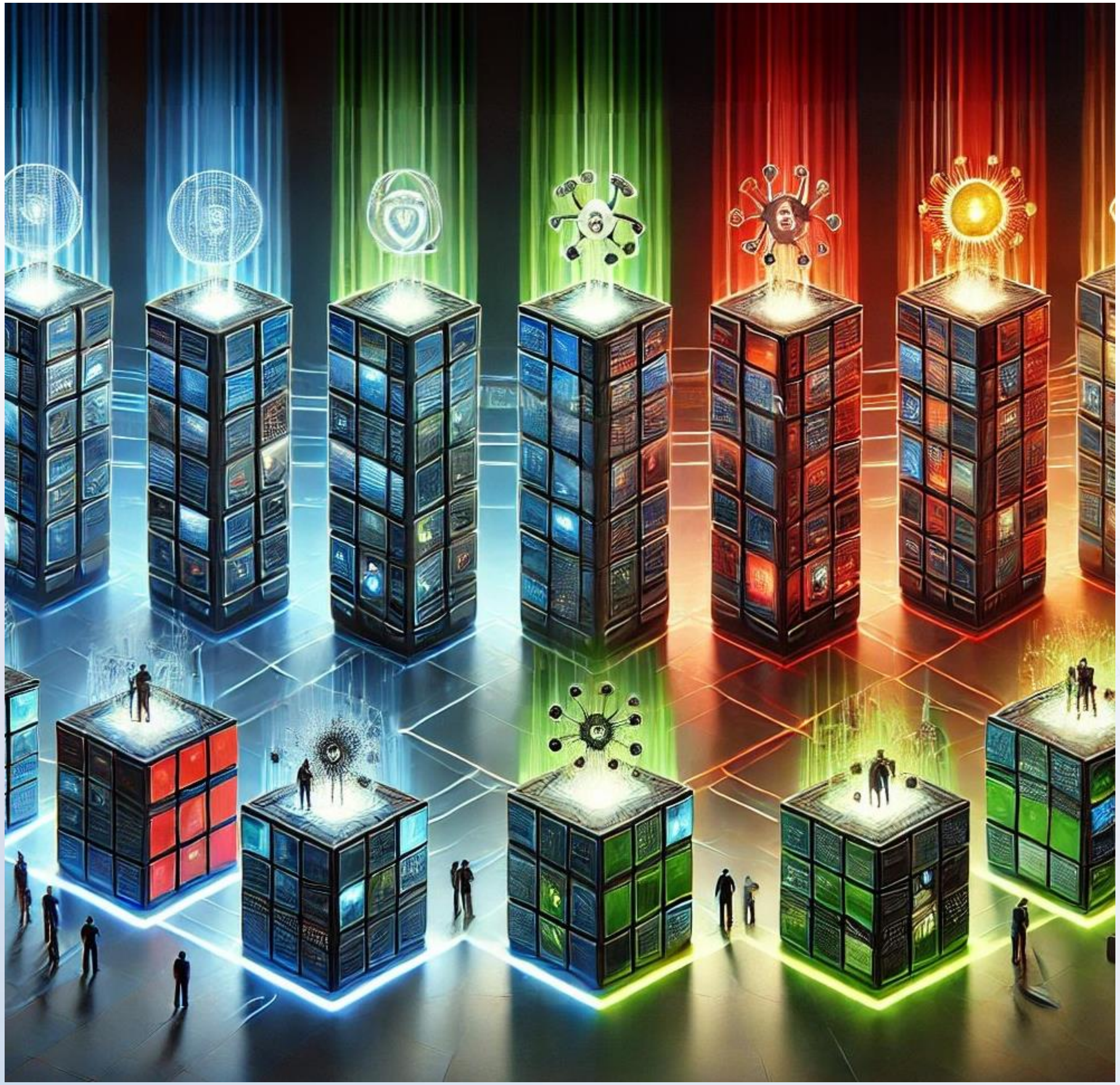
- Why are security teams looking to mobile?
  - Multi factor authentication
  - “Mobile Only” applications
  - Increase in threat vectors – Phishing kits, for example – that target only mobile browsers
  - Mobile as an egress route
  - Persona Maintenance
- What are the barriers?
  - Sourcing and maintaining a fleet of mobile devices is HARD
  - In some cases, phones are simply not permitted

Personal Device Risks

Using personal devices for investigations exposes investigators to significant risks:

- Including direct identity exposure
- Lack of isolation from personal/professional account
- Device fingerprinting
- Operational security failures
- Legal exposure, and enterprise-wide risk.

Personal devices lack the necessary controls and isolation to safely conduct high-stakes financial investigations without compromising sensitive information and activities.



Challenge #3: Collaboration

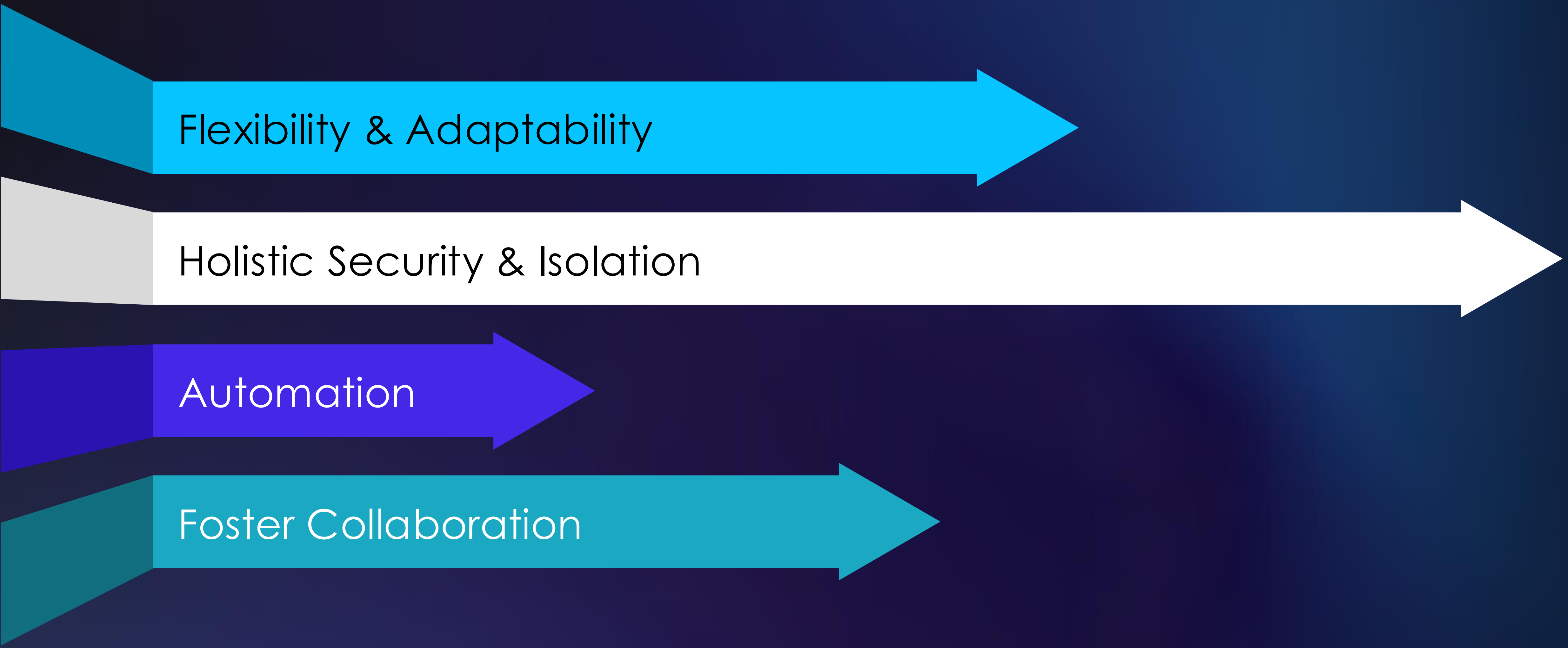
- Sharing is hard
  - TTPs
  - Technology
  - Experience

- Three different forms of collaboration
  - Intra-team
  - Team to team
  - Team to 3rd party

Challenge #4: Automation & Efficiency

- Many teams are seeking ways to automate common work streams for a variety of reasons
  - Frees up analysts to do more of what they want to do
  - Allows for broader coverage
- Some examples include:
  - Web scraping
  - “Listening posts”

The Path Forward



- Flexibility & Adaptability
- Holistic Security & Isolation
- Automation
- Foster Collaboration

REPLICA™

Navigating Security Challenges: A Comprehensive Approach

- Access to the right data at the right time

  Ensuring security teams can access the necessary data without technical limitations or external threats.

- Policy Restrictions

  Navigating organizational policies and regulations to enable necessary security operations.

- Mobility

  Securing and supporting remote and mobile work environments.

- Collaboration

  Facilitating seamless communication and knowledge sharing between teams to address issues in real-time.

- Flexibility and Adaptability

  The ability to access necessary data without being restricted by technical limitations or external threats.

- Security and Isolation

  Ensuring sensitive activities are isolated to protect the organization.

- Automation

  Simplifying workflows and reducing manual effort to improve efficiency.

REPLICA™

REPLICA™

POWERED BY GREY MARKET LABS

Contact Us Today!

info@replicacyber.com
www.replicacyber.com