M³AAWG is a Trusted Environment

M³AAWG ENGAGEMENT SERIES

What happens in M³AAWG stays in M³AAWG

- What occurs here cannot be shared outside the membership without the written permission of the Executive Director, unless we state the specific session is open to the press and social media.
- See the M³AAWG Meeting Policy at www.m3aawg.org/MeetingPolicy

Treat Everyone with Respect

- Treat all attendees respectfully in and out of sessions. No less will be tolerated.
- See the M³AAWG Conduct Policy at https://www.m3aawg.org/conduct-policy

You agreed to these policies when you registered for the meeting.
For questions, please contact Amy Cadagin at amy@m3aawg.org

Contribute to a Productive Meeting

- Mute your Zoom session; be courteous to those listening to the presentations

This slide is for Moderators' slide deck template only – not presenters.

Presenters remove this before using this slide

Reminders for Our Worldwide Friends

All meeting content is confidential: No photos, no video, no recording.
Reach out to room monitor staff with questions.

M3 AAWG ENGAGEMENT SERIES

L’ensemble du contenu de la réunion est confidentiel : les photos, vidéos et enregistrements sont interdits. Pour toute question, demandez conseil au personnel.

Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.

Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.

会議の内容はすべて機密扱いです。 写真やビデオの撮影、録音は禁止されています。質問がある方は、スタッフまでご連絡ください。

所有会议内容均为保密信息：禁止拍照、录像、录音。如有疑问，请咨询职员。

회의에서 다루는 모든 내용은 기밀입니다. 사진 및 동영상 촬영과 녹음은 금지됩니다. 질문이 있으시면 직원에게 문의해 주십시오.

Все содержимое собрания является конфиденциальным: нет фотографий, нет видео, нет записи.Смотрите сотрудников с вопросами.

This slide is for Moderato
– not presenters.
***Presenters remove th**

M3AAWG ENGAGEMENT SERIES

Eric George

Manager, Solution Engineering PhishLabs

Eric George is the Manager of Solution Engineering for PhishLabs. He has been at PhishLabs seven years, where he initially started as a SOC analyst and advanced to a manager role, where he built considerable security knowledge. Currently, Eric serves as the Manager of Solution Engineering, where he supports sales and business development efforts. In addition to his work at PhishLabs he is also a CISSP and serves as a technical Mobile Chair for M3AAWG.

M3AAWG
ENGAGEMENT SERIES

Digital Risk Protection

Evolving Your Cyber Threat Intel Program Into Action

INTRODUCTION TO PHISHLABS

M3AAWG ENGAGEMENT SERIES

DIGITAL RISK PROTECTION

- Domain Monitoring
- Social Media Protection
- Data Leakage Detection
- Account Takeover Prevention
- Brand Protection
- Executive Protection

2008
PhishLabs Founded

5
of the World's Largest Companies

10
of the Most Valuable Global Brands

10
of the 13 Largest Financials in North America

DIGITAL RISK PROTECTION (DRP)

M3AAWG ENGAGEMENT SERIES

"Due to the large amount of diverse use cases, DRPS would be beneficial to any organization in any industry around the world that prioritizes business resiliency as a primary approach to reducing impact to their digital assets."

Gartner Hype Cycle for Security Operations, 2020
June 2020, Pete Shoard

Gartner Hype Cycle for Security Operations, 2020

June 2020, Pete Shoard

Gartner Emerging Technologies Report: Critical Insights into Digital Risk Protection Services

July 2020, Ruggero Contu and Elizabeth Kim

Forrester New Wave: Digital Risk Protection, Q3 2018

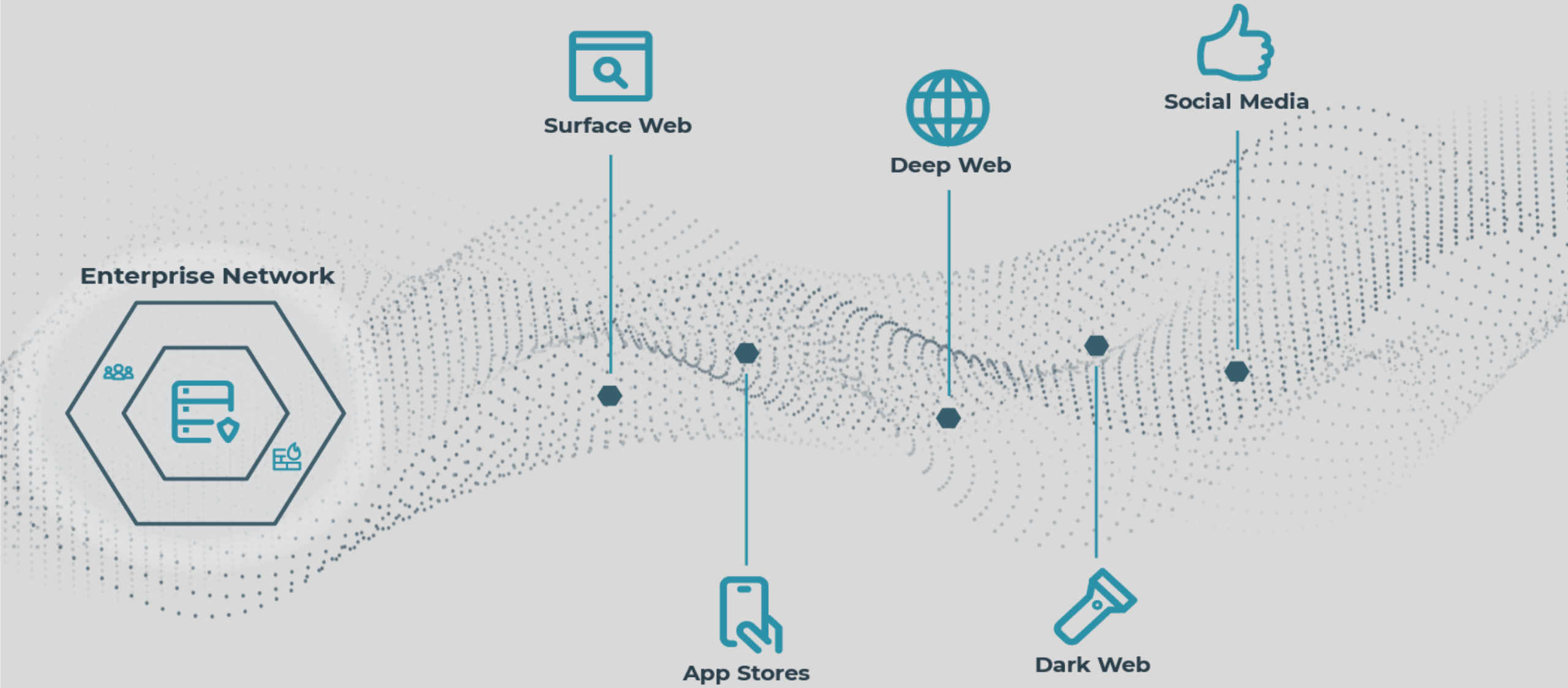
WHAT IS DIGITAL RISK PROTECTION (DRP)?

M3AAWG ENGAGEMENT SERIES

DRP is an operational process that combines intelligence, detection, and response to mitigate attacks across the external digital risk landscape.

WHAT IS DIGITAL RISK PROTECTION

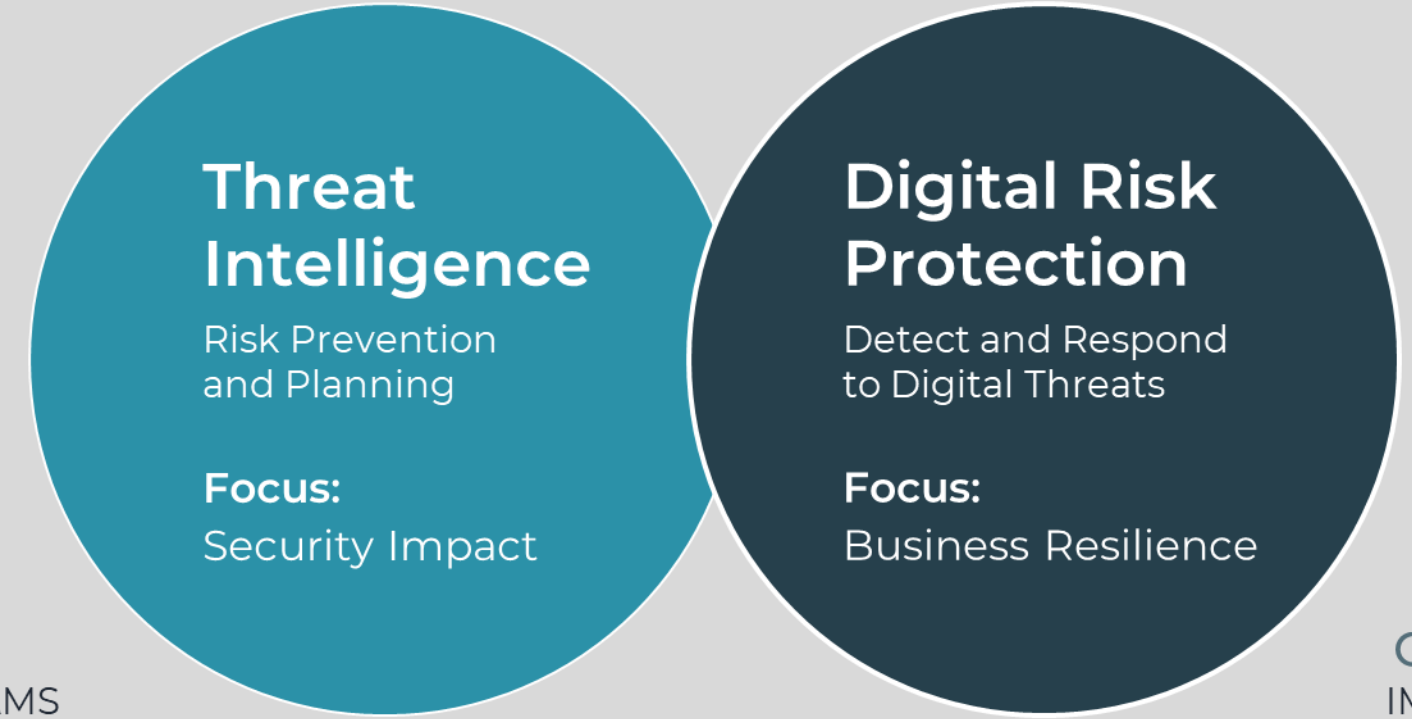
M3AAWG
ENGAGEMENT SERIES



TRADITIONAL THREAT INTELLIGENCE AND DRP

M3AAWG ENGAGEMENT SERIES

Incident Response
Security Rating/Scorecard
Threat Hunting
Prioritization
Attack Surface Reduction



Domain Monitoring
Account Takeover Prevention
Brand Protection
Social Media Protection
Data Leak Detection
Executive Protection

STRATEGIC
INFORMS PROGRAMS

OPERATIONAL
IMMEDIATE IMPACT

DRP USE CASES

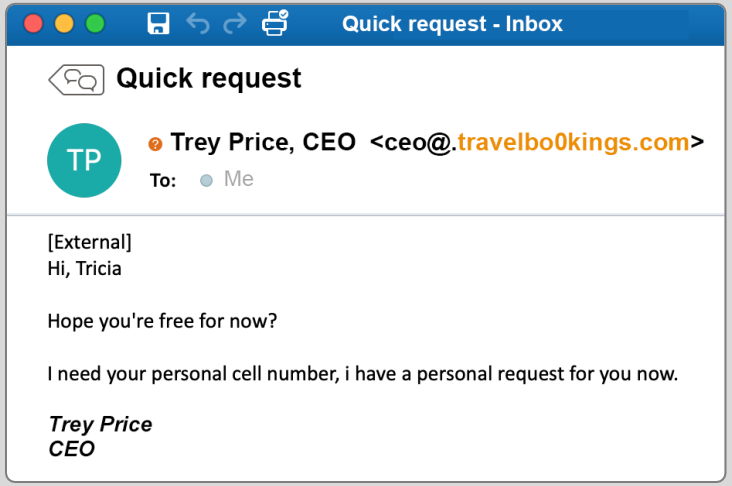
M3AAWG ENGAGEMENT SERIES

DOMAIN MONITORING

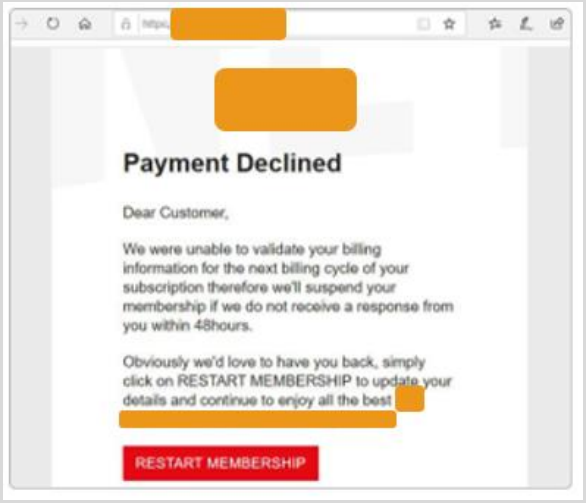
M3AAWG ENGAGEMENT SERIES

Threat examples:

- Business Email Compromise (BEC)
- Credential theft phishing sites
- Domain Redirects
- Claims of false association
- Traffic diversion



Business Email Compromise (BEC)



PHISHING SITE: https://verification-[brand].com

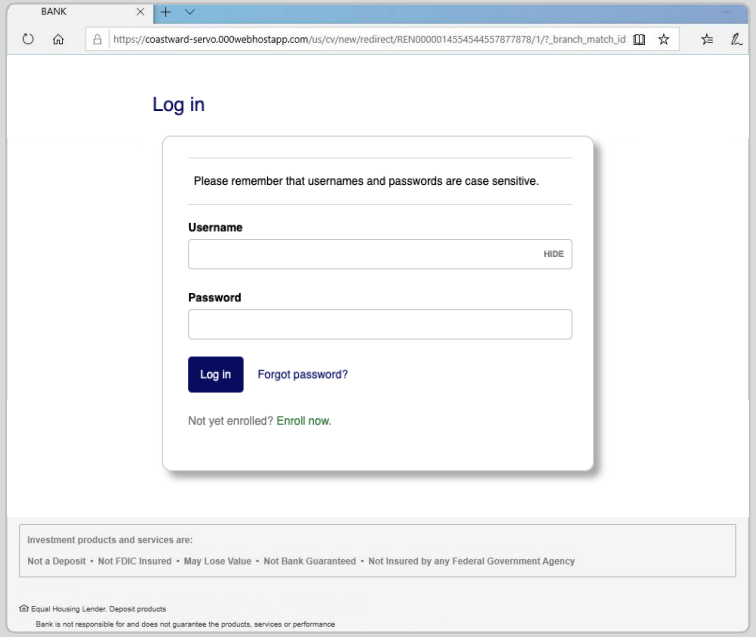
MONETIZED LINKS: http://[brand]inc.com

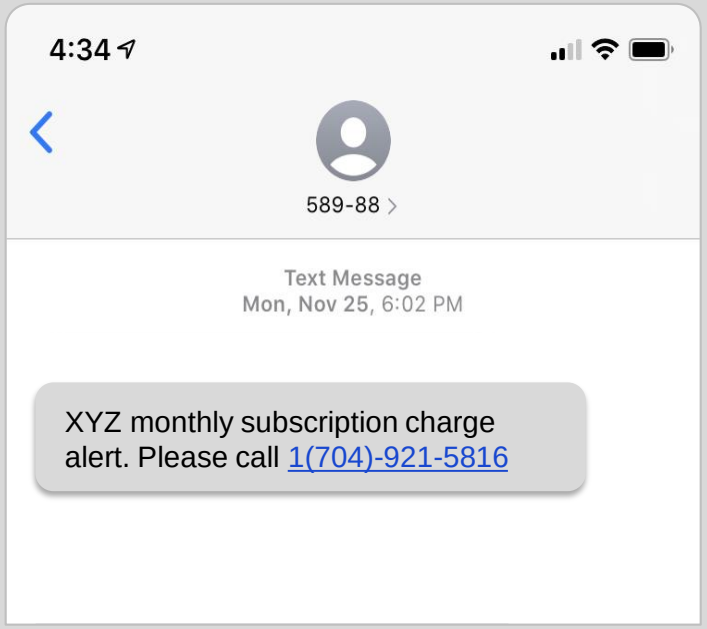
ACCOUNT TAKEOVER PREVENTION

M3AAWG ENGAGEMENT SERIES

Threat examples:

- Credential theft phishing sites
- Vishing/SMiShing
- Crimeware



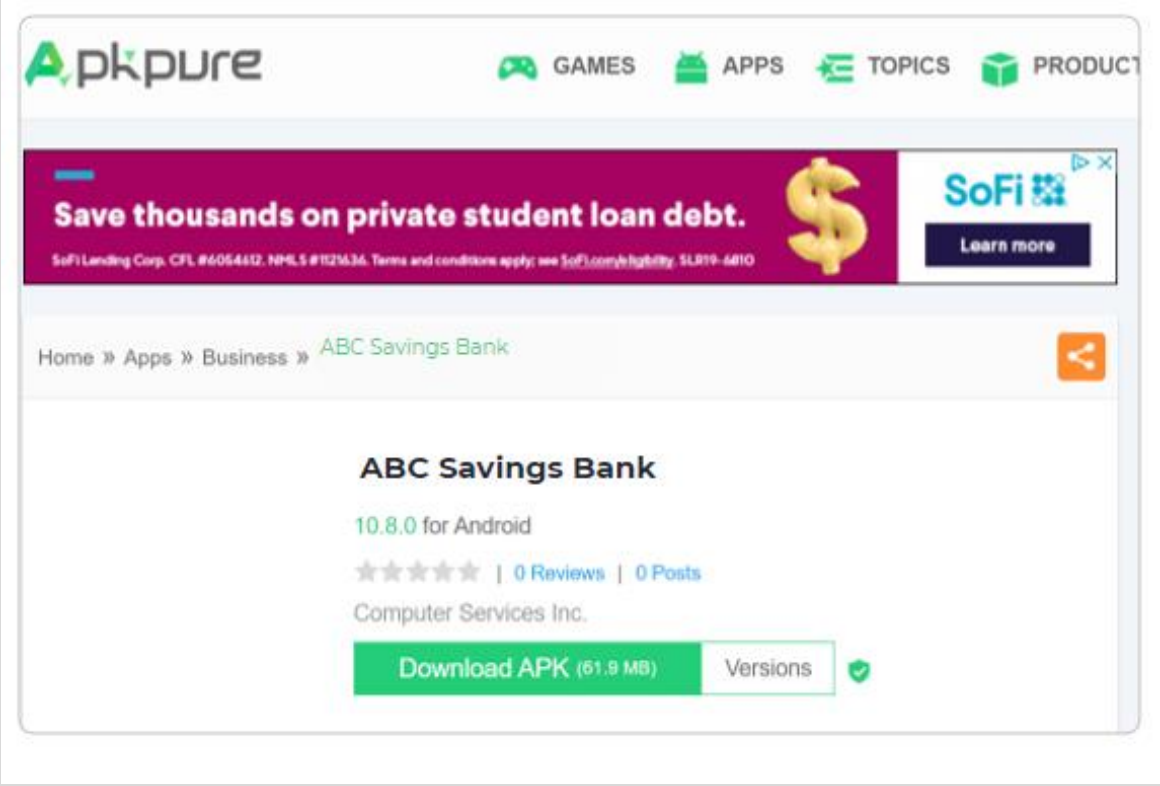


BRAND PROTECTION

M3AAWG ENGAGEMENT SERIES

Threat examples:

- Brand impersonation
- Rogue mobile apps
- Trademark infringement
- Traffic redirection schemes

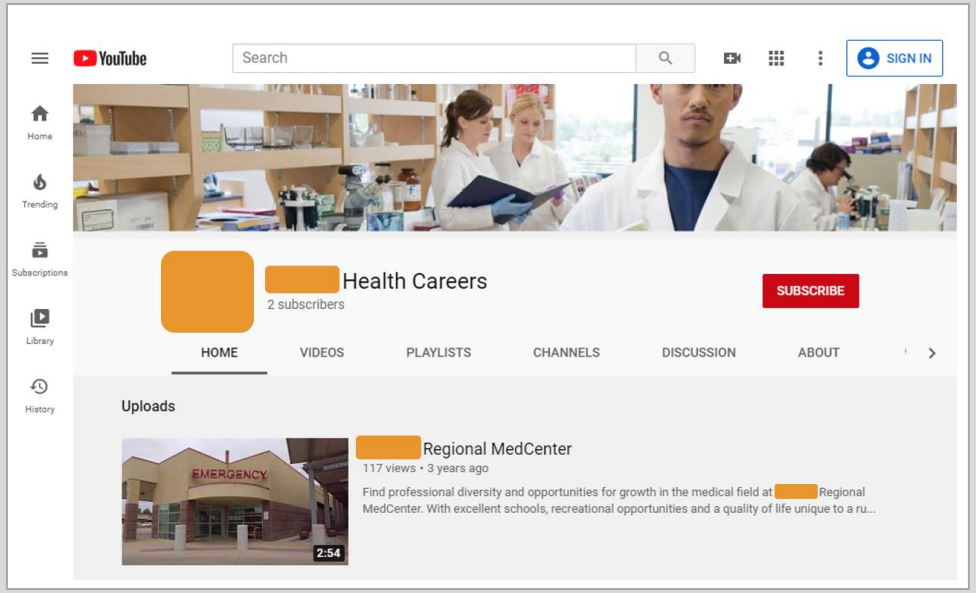


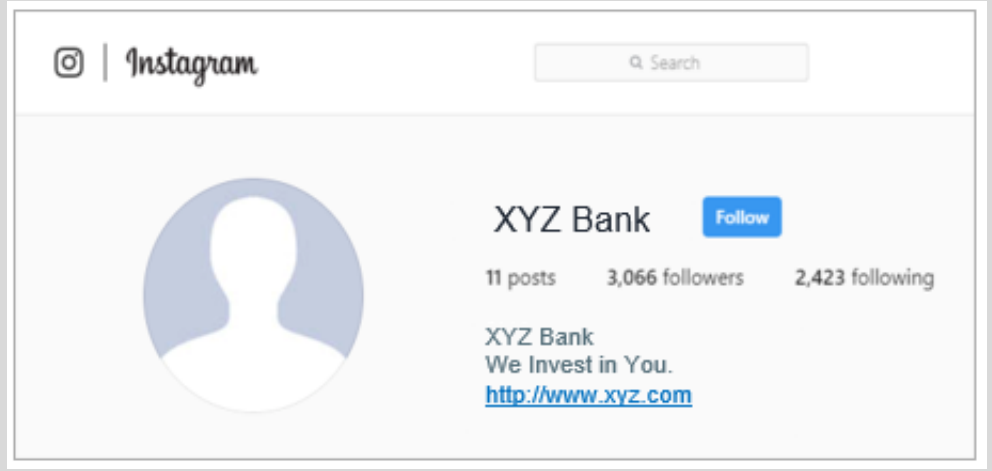
SOCIAL MEDIA PROTECTION

M3AAWG ENGAGEMENT SERIES

Threat Examples:

- Targeted Cyber threats (Malware, Phishing)
- PII leaks used to scam or for harm
- Brand and VIP Impersonation
- Physical threats (location/event)
- Unauthorized associations (Partners/Sponsors)
- Employment scams





DATA LEAK DETECTION

M3AAWG ENGAGEMENT SERIES

Common types of leaked data:

- PII, PHI (Regulated data)
- Employee credentials
- Credit card numbers
- Intellectual Property (IP)
  - Source code
  - Business plans

Business Continuity Management / Disaster Recovery , Fraud Management & Cybercrime , Fraud Risk Management

More Ransomware Gangs Threaten Victims With Data Leaking

22% of Ransomware Incidents Now Involve Data Exfiltration, Investigators Find

Mathew J. Schwartz (euroinfosec) • August 25, 2020

ars TECHNICA SUBSCRIBE SIGN IN

INSIDE [redacted]

More than 20GB of [redacted] source code and proprietary data dumped online

[redacted] leak includes docs [redacted] provided under NDA as recently as May.

DAN GOODIN AND JIM SALTER - 8/6/2020, 7:59 PM

CYBER SECURITY NEWS · 2 MIN READ

[redacted] [redacted] and Other Major Companies Affected by Massive Source Code Leak

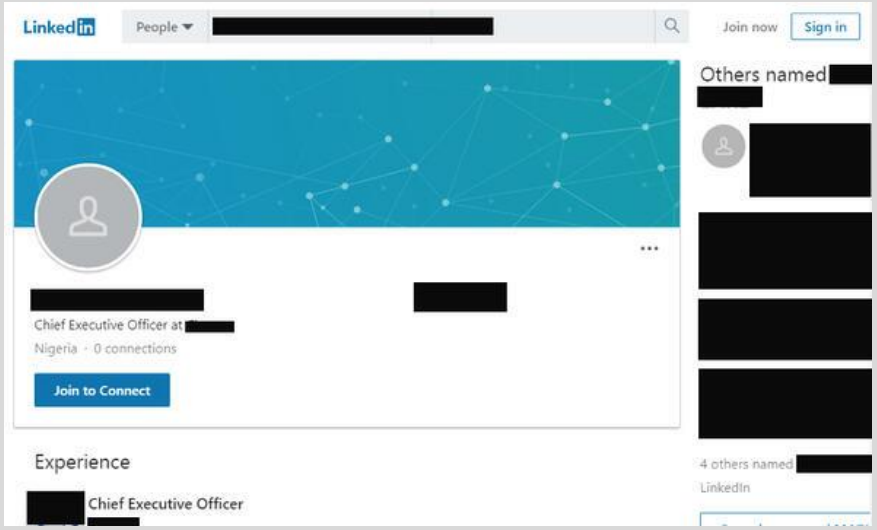
ALICIA HOPE · AUGUST 6, 2020

EXECUTIVE PROTECTION

M3AAWG ENGAGEMENT SERIES

Threat Examples:

- VIP Impersonation
- Physical Threats
- Whaling



WHERE DO I GO FROM HERE?

M3AAWG ENGAGEMENT SERIES

Use Case			
Domain Monitoring			
Account Takeover			
Brand Protection			
Social Media Protection			
Data Leak Detection			
Executive Protection			

WHERE DO I GO FROM HERE?

M3AAWG ENGAGEMENT SERIES

Use Case	Priority Level
Domain Monitoring	High
Account Takeover	High
Brand Protection	High
Social Media Protection	High
Data Leak Detection	Medium
Executive Protection	Medium

WHERE DO I GO FROM HERE?

M3AAWG ENGAGEMENT SERIES

Use Case	Priority Level	Stakeholders
Domain Monitoring	High	Security, IT, HR
Account Takeover	High	Security, Legal, Marketing
Brand Protection	High	Security, Legal, Marketing/Brand
Social Media Protection	High	Security, HR, IT, Marketing, Risk
Data Leak Detection	Medium	Legal, IT, Security Risk & Compliance
Executive Protection	Medium	Security, IT, Legal, Marketing

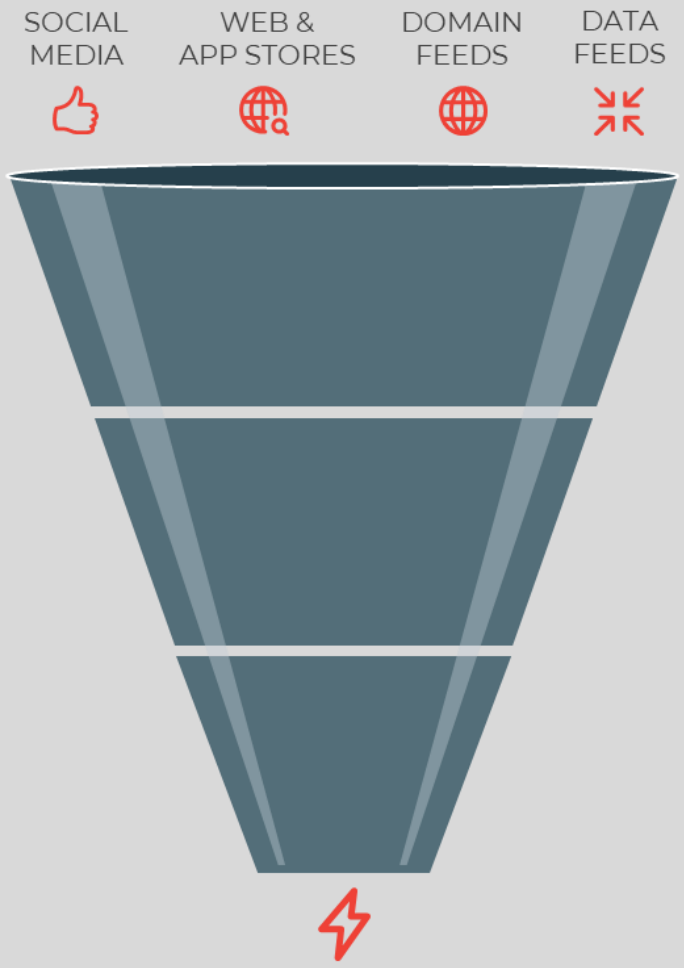
WHERE DO I GO FROM HERE?

M3AAWG ENGAGEMENT SERIES

Use Case	Priority Level	Stakeholders	Current State
Domain Monitoring	High	Security, IT, HR	Outsourced
Account Takeover	High	Security, Legal, Marketing	Monitoring
Brand Protection	High	Security, Legal, Marketing/Brand	No current capability
Social Media Protection	High	Security, HR, IT, Marketing, Risk	Outsourced
Data Leak Detection	Medium	Legal, IT, Security Risk & Compliance	Legal: Cease and Desist
Executive Protection	Medium	Security, IT, Legal, Marketing	No current capability

HOW TO BUILD AN EFFECTIVE DRP PROGRAM

M3AAWG ENGAGEMENT SERIES



COLLECTION

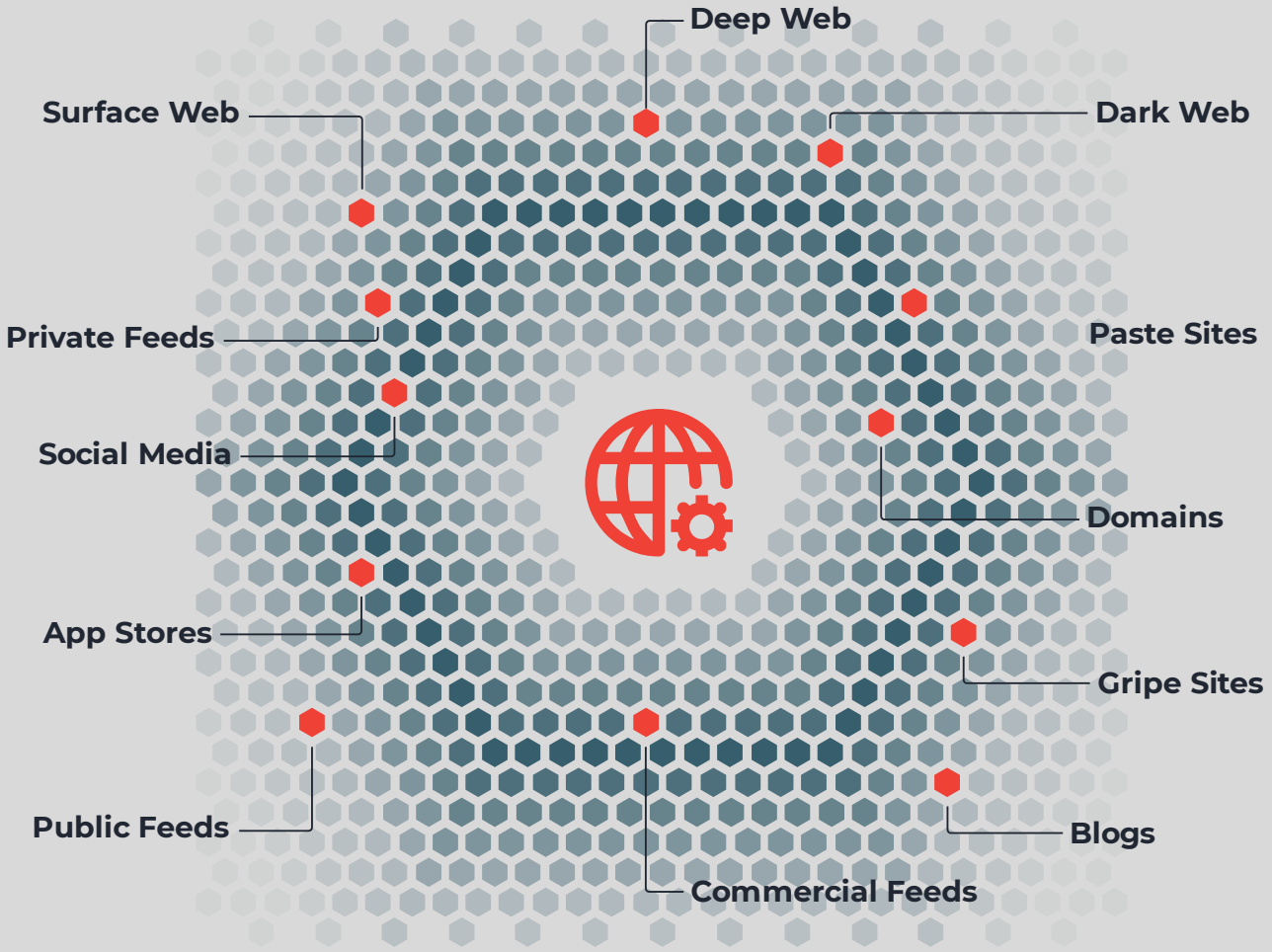
CURATION

MITIGATION

STEP 1: COLLECTION

M3AAWG ENGAGEMENT SERIES

- What do I need to collect for my use cases?
- How can I source the data? Where will I store it?
- Will I use both free and paid sources?
- Evaluating data quality: Are the sources broad enough? Timely enough?
- How will I measure value from sources?



COLLECTION CHALLENGES

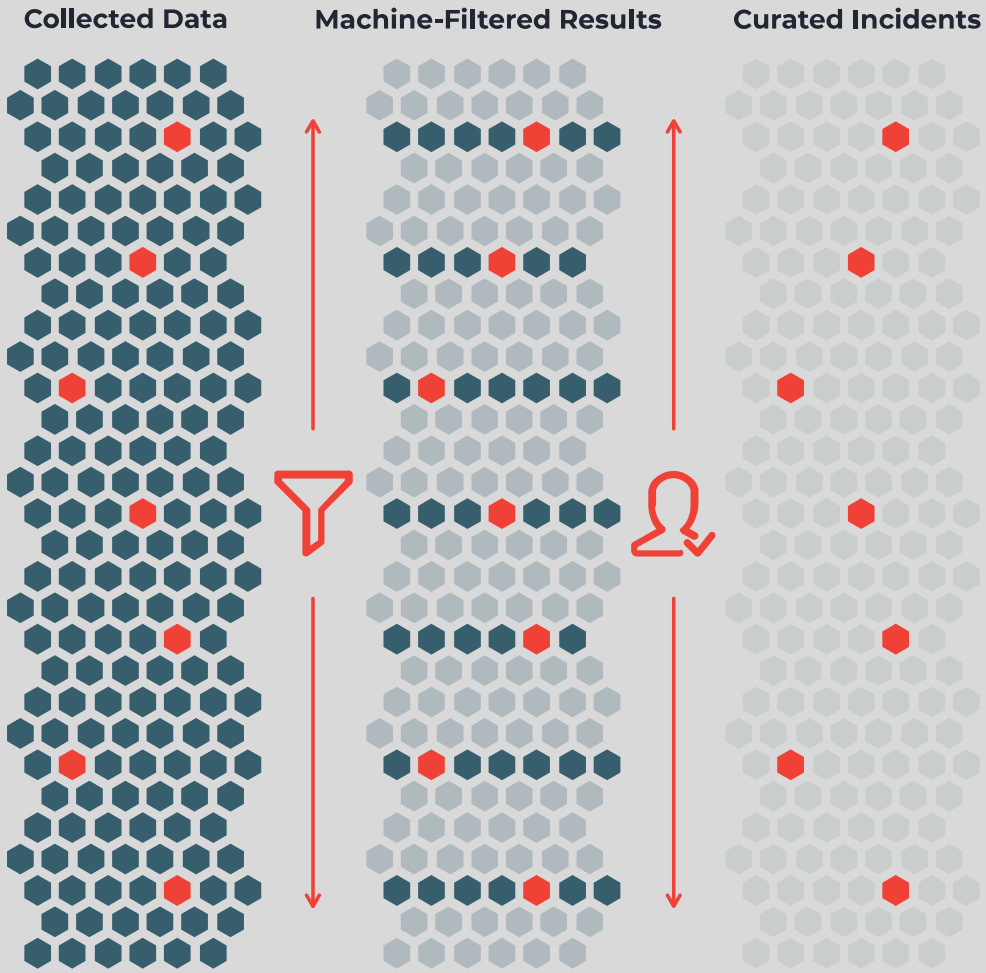
M3AAWG ENGAGEMENT SERIES

- Fidelity of data sources can vary dramatically
- Open source or commercial data feeds aren't available or sufficient for many uses (need direct collection)
- Hidden content, countering evasion techniques.
- Lack of consistent data structures needed to organize/analyze at scale
- High value data sources require relationships and investments (zone files for ccTLDs, SMS spam)

STEP 2: CURATION

M3AAWG ENGAGEMENT SERIES

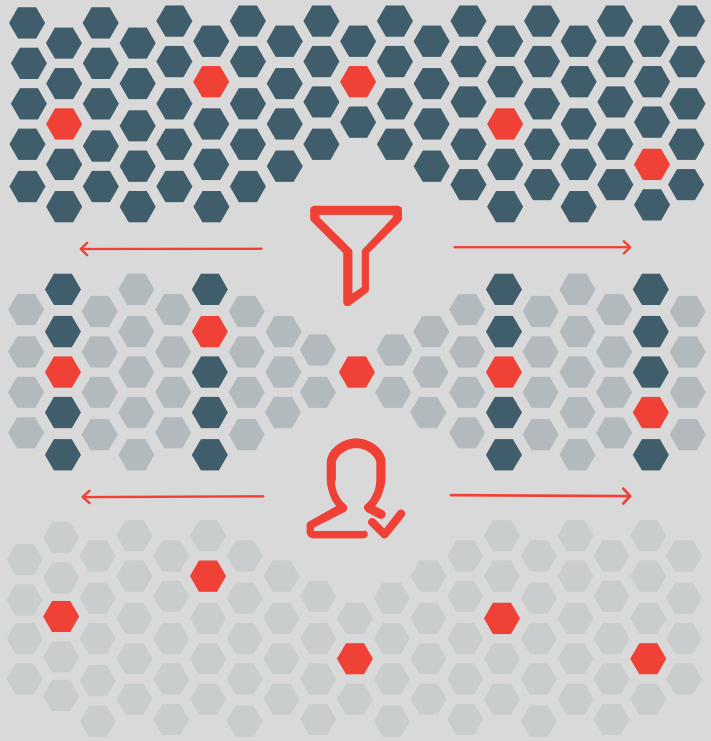
- How is intelligence disseminated, and how will I get access to it?
- Where does automation end and human analysis begin?
- Will my analysts need to review all threats for false positives?
- Determine appropriate coverage: 24 x 7 x 365 vs. business hours, ad hoc



CURATION CHALLENGES

M3 AAWG ENGAGEMENT SERIES

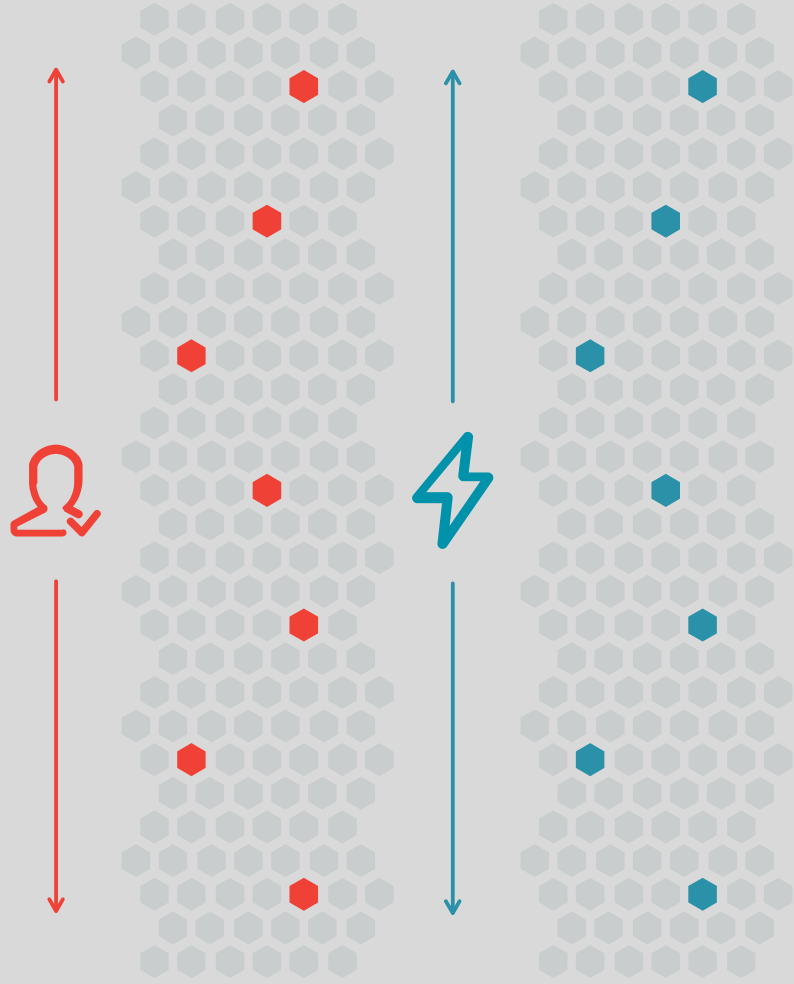
- Measuring your fidelity and adding a feedback loop to fine tune your process
- Managing false positives and false negatives
- Managing automated versus human processes
- Can’t review everything; determining the cut line using risk scoring



STEP 3: MITIGATION

M3AAWG ENGAGEMENT SERIES

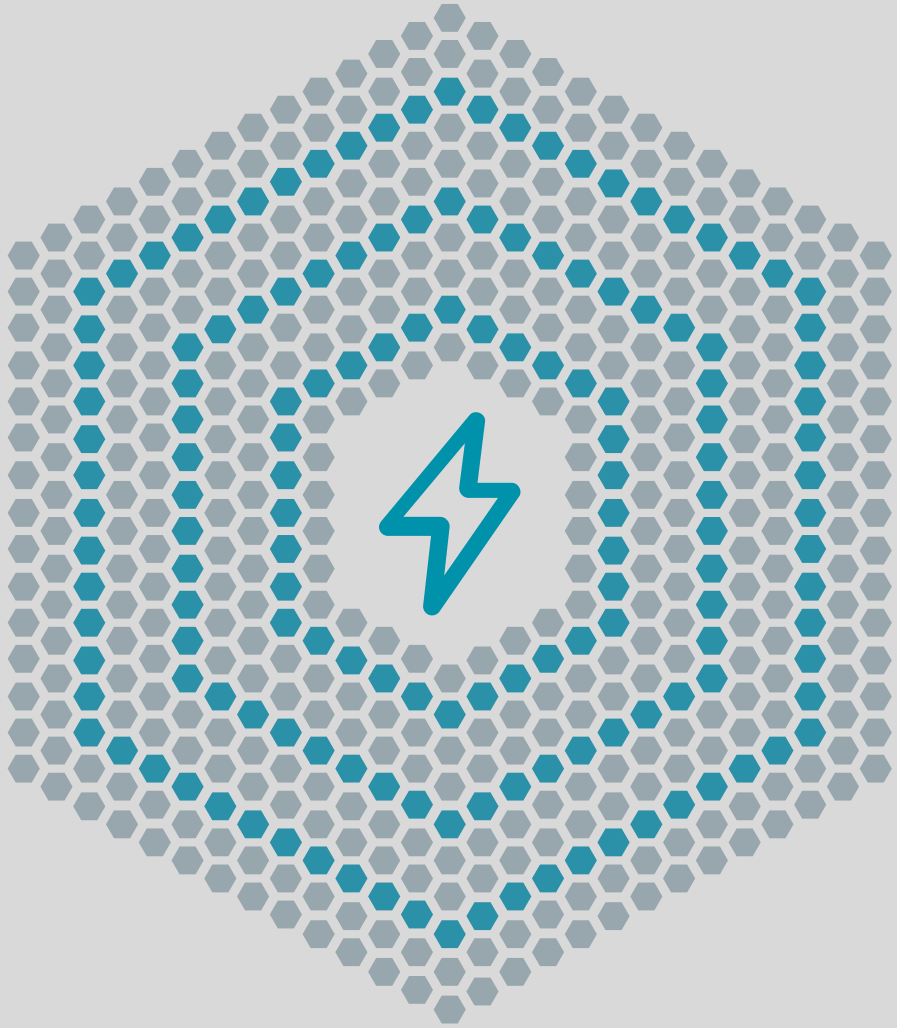
- How to block? How to take down?
- Will legal handle certain types of threats? Manage DMCA takedowns or send C&D letters?
- Do we need a take down team?
- 24 x 7 x 365 required?



MITIGATION CHALLENGES

M3AAWG ENGAGEMENT SERIES

- No plan in place ahead of threat detected
- Technical mitigation doesn't cover all scenarios
- Mitigating quickly enough to be effective
- Takedown requires building relationships, persistence, knowledge of laws & regulations; navigating language, and time zones
- No uniform global standard for takedowns. Every service provider requires a different process
- Providing evidence can be difficult



DRP BEST PRACTICES

M3AAWG ENGAGEMENT SERIES

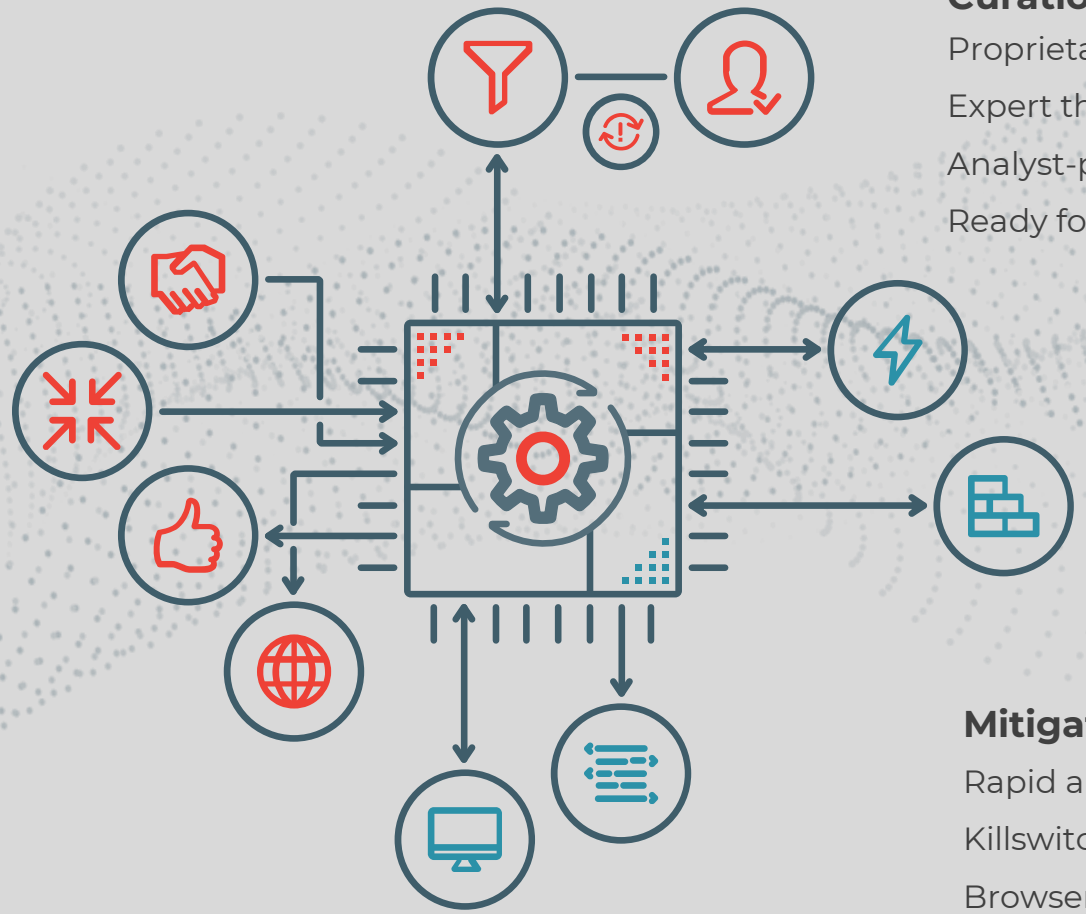
Collection

Advanced crawling, anti-evasion

Continuous monitoring

Open, deep, dark web, social

Public, private, client feeds



Curation

Proprietary algorithms

Expert threat assessment

Analyst-platform feedback loop

Ready for action

Mitigation

Rapid and complete

Killswitches, fastlanes, takedown network

Browser-blocking and API integrations

Intuitive web app and reporting APIs

DRP TAKEAWAYS

M3AAWG ENGAGEMENT SERIES

- DRP is an emerging security function.
- It has many use cases that deliver value.
- It has immediate, stop the bleeding impact.
- DRP program best practices:
  - Collect data from a broad set of reliable sources.
  - Detect threats using both automated and human data analysis.
  - Have a playbook and relationships in place to mitigate threats.

FREE RESOURCES AND LINKS

M3AAWG ENGAGEMENT SERIES

Gartner Digital Risk Protection Emerging Technologies Report

https://info.phishlabs.com/gartner-digital-risk-protection-emerging-technologies

FREE RESOURCES:

Phishing Data:

http://data.phishtank.com/data/online-valid.csv

https://openphish.com/feed.txt

Social Media Searches:

https://boardreader.com/

https://www.social-searcher.com/

Data Leaks / Compromised Creds:

https://igotphished.abuse.ch/

Look-alike Domain Name Detection:

https://dnstwist.it/

https://github.com/elceef/dnstwist

Dark Web Searches:

https://reconponydonugup.onion/

http://haystakvxad7wbk5.onion/

App Stores Lists:

https://www.businessofapps.com/guide/app-stores-list/

M3AAWG ENGAGEMENT SERIES

CONTACT ERIC

For additional questions, please email:

mobile-tech-chair@mailman.m3aawg.org