Welcome to today's University Business web seminar

Swimming with sharks: Understanding and countering cyber threats in higher education

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

Thank you for joining us! The web seminar will start promptly at 2:00 ET.

UB University Business

FIREEYE™

Welcome to today's University Business web seminar

Swimming with sharks: Understanding and countering cyber threats in higher education

Thank you for joining us! The web seminar will start shortly at 2:00 ET.

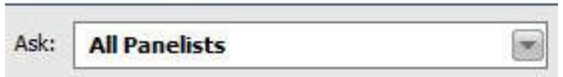
For technical support:
Use the Chat panel at the right of your screen. Select the name of our event producer, Jason York, and type your message.

"Chat" for tech support

No computer speakers? Prefer to listen privately?
Dial the phone number and access code posted in the Chat window.

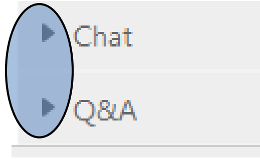
To submit a question to our panel:
Use the Q&A panel at the right of your screen. Send your question to All Panelists, the default option.

"Q&A" for panelist questions



Ask: All Panelists

Don't see a panel?
Click the "expand panel" triangle in front of the panel name.



Need to access the presentation at a later time?
Everyone will receive an email with links to the slides and the archive recording.

Swimming with sharks: Understanding and countering cyber threats in higher education

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

This web seminar is sponsored by:

FIREEYE™

Housekeeping

Swimming with sharks: Understanding and countering cyber threats in higher education

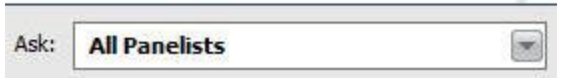
For technical support:
Use the Chat panel at the right of your screen. Select the name of our event producer, Jason York, and type your message.

“Chat” for tech support

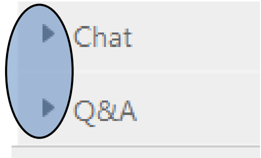
No computer speakers? Prefer to listen privately?
Dial the phone number and access code posted in the Chat window.

To submit a question to our panel:
Use the Q&A panel at the right of your screen. Send your question to All Panelists, the default option.

“Q&A” for panelist questions


Ask: **All Panelists**

Don’t see a panel?
Click the “expand panel” triangle in front of the panel name.



Need to access the presentation at a later time?
Everyone will receive an email with links to the slides and the archive recording.

Swimming with Sharks

Understanding and Countering Cyber Threats

Christian Schreiber, CISM, PMP

Cybersecurity Platform Strategist – FireEye

REVISION 004 – 22 June 2020

Introductions

Personal Background

20+ years IT and security experience

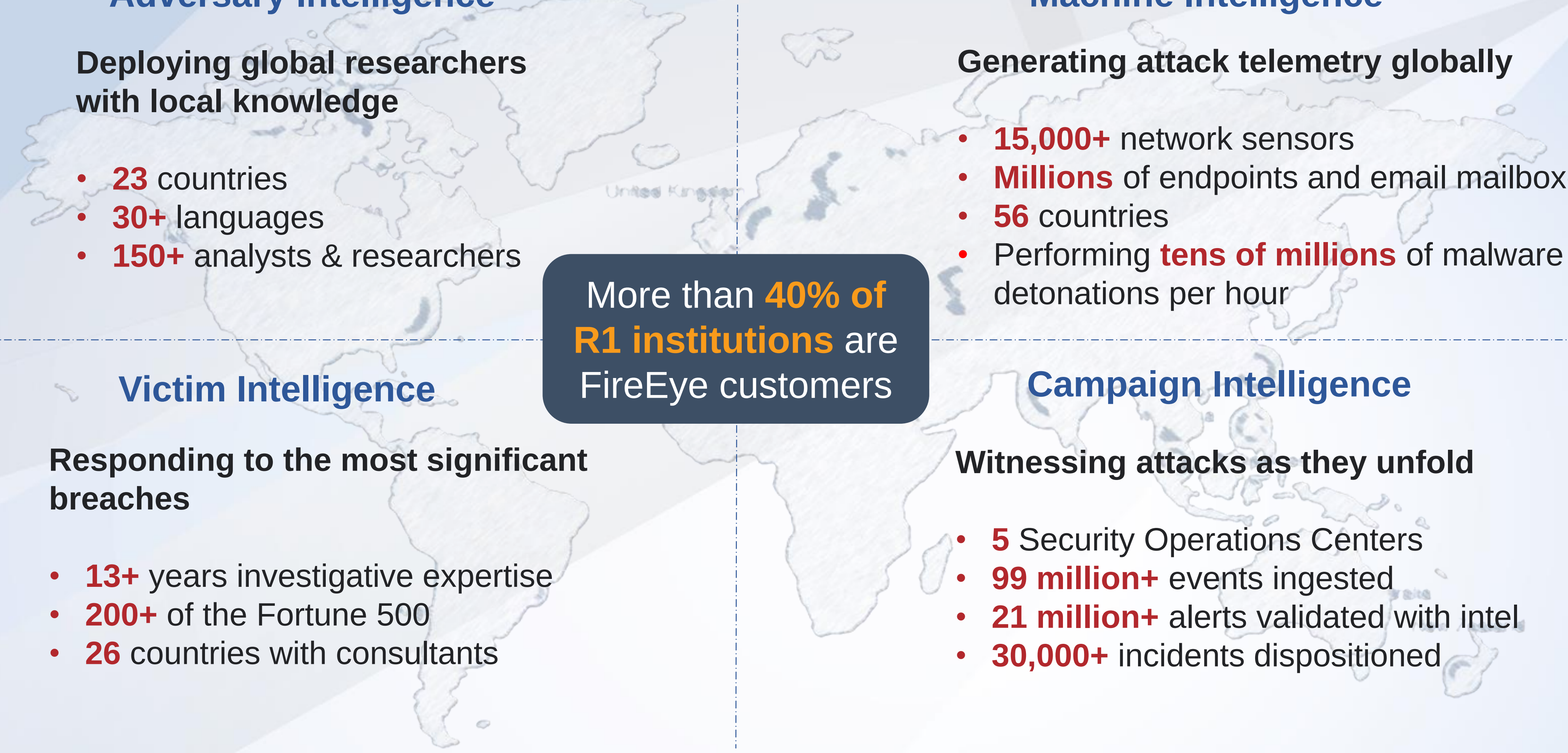
- Security leadership: The University of Arizona, University of Wisconsin – Whitewater, SunGard Data Systems / Ellucian
- IT leadership positions: University of Wisconsin – Madison, Central Michigan University

Education and Certifications

- Bachelor of Science in Business Administration from Central Michigan University
- Masters Certificate in Project Management from University of Wisconsin – Madison
- Certified Information Security Manager (CISM)
- Project Management Professional (PMP)

- **Joined FireEye in 2016**
  - Strategist helping customer executives achieve effective and resilient cybersecurity
  - Focus on education, healthcare, and public sector customers

FireEye: Unique visibility across attack lifecycle



Adversary Intelligence

Deploying global researchers with local knowledge

- **23** countries
- **30+** languages
- **150+** analysts & researchers

Machine Intelligence

Generating attack telemetry globally

- **15,000+** network sensors
- **Millions** of endpoints and email mailboxes
- **56** countries
- Performing **tens of millions** of malware detonations per hour

More than **40% of R1 institutions** are FireEye customers

Victim Intelligence

Responding to the most significant breaches

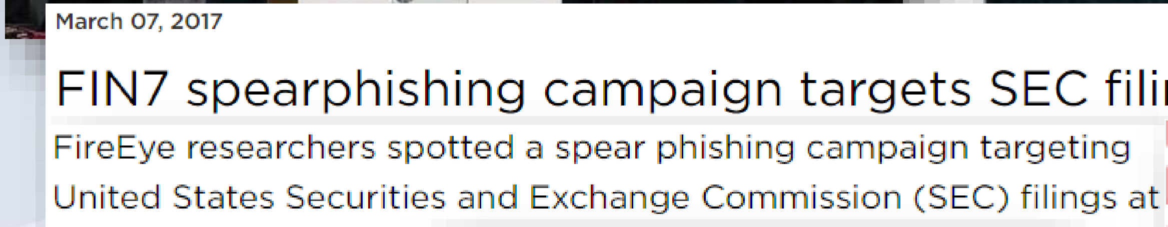
- **13+** years investigative expertise
- **200+** of the Fortune 500
- **26** countries with consultants

Campaign Intelligence

Witnessing attacks as they unfold

- **5** Security Operations Centers
- **99 million+** events ingested
- **21 million+** alerts validated with intel
- **30,000+** incidents dispositioned

Frequently consulted for cybersecurity insights


March 07, 2017

FIN7 spearphishing campaign targets SEC filings

FireEye researchers spotted a spear phishing campaign targeting United States Securities and Exchange Commission (SEC) filings at various organizations.

SC MEDIA

Cyber Espionage Seen Expanding to Grasp Trump Policy Changes

Bloomberg Politics

by Nafeesa Syeed
February 24, 2017, 2:26 PM EST

Washington
8:12 AM
DEVELOPING STORY
SOUTH KOREA SUSPECTS HACK CAME FROM CHINA
John Hultquist Director of Cyber Espionage Analysis, FireEye
LIVE
CNN

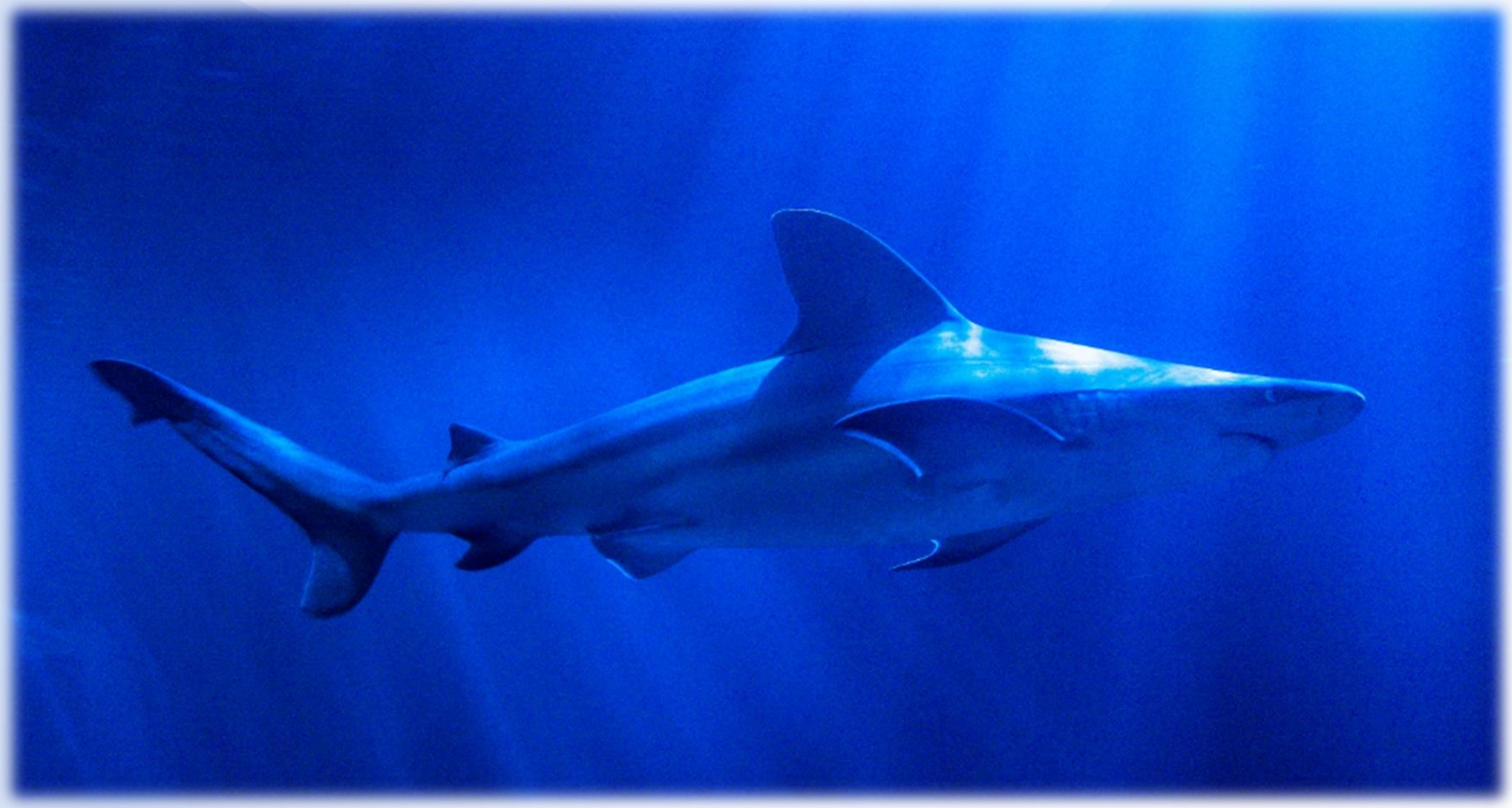
"This stuff is cool, and I'm sure most would rather plug the holes, but don't fool yourself, its a setback for counterterrorism," commented John Hultquist, threat intelligence manager for the cybersecurity firm FireEye (FEYE, +0.53%).

FORTUNE | WikiLeaks Dumps Thousands of Files on Alleged CIA Hacking Tools

Why are we talking about sharks?

No, not another phishing talk…

Some threats capture the imagination



Others are easily overlooked

Why swim with sharks?

- **People have many different goals:**
  - Adventure
  - Photography
  - Science research

Why run technology infrastructure?

- **You have many different goals:**
  - – Back office / ERP
  - – Student learning
  - – Research
  - – Etc.

Another underlying shared goal…

Stay Safe!

- **Shark divers and tech leaders have different goals**
- **For IT leaders:**
  - – Confidentiality
  - – Integrity
  - – Availability

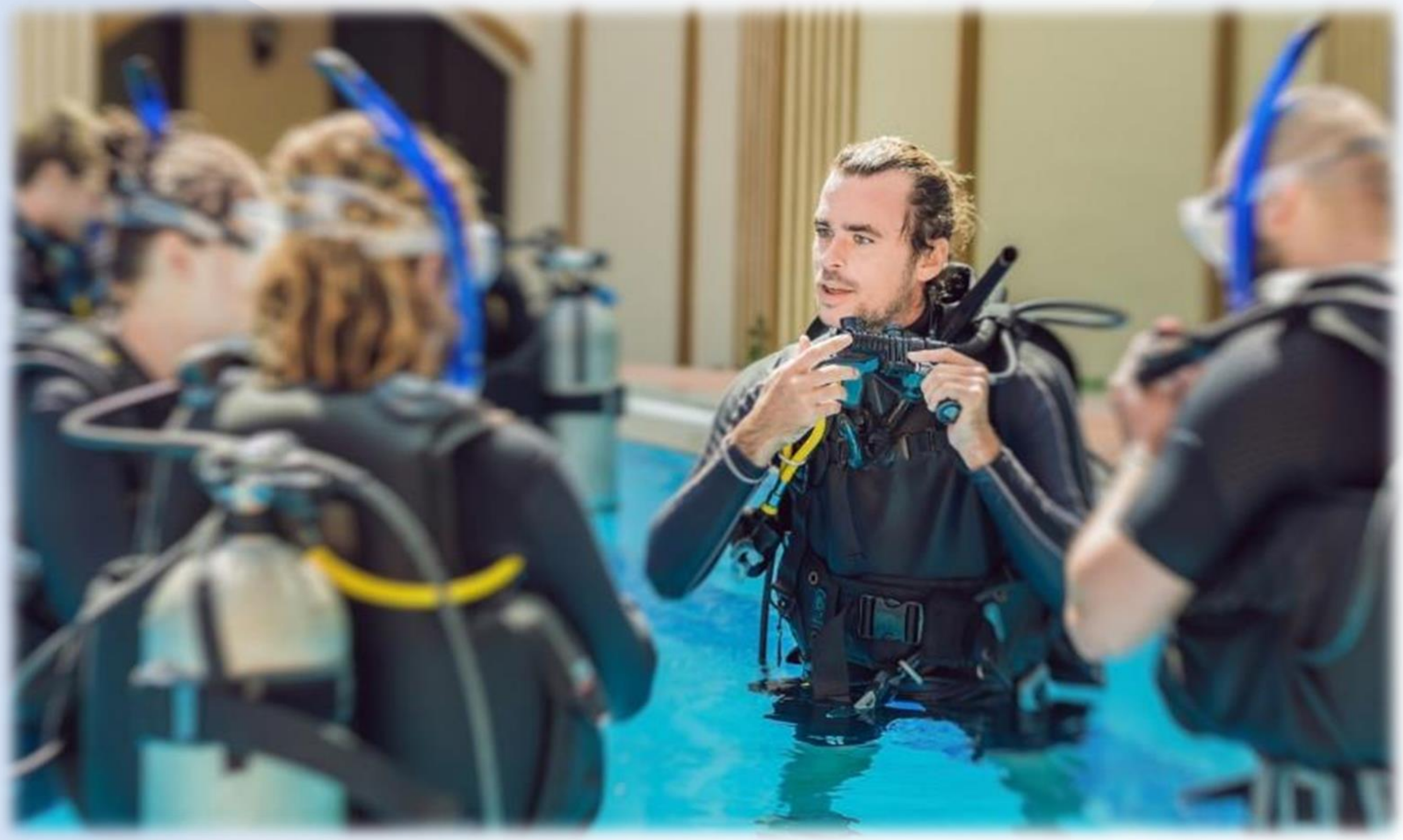
How do you stay safe?

Master technical skills

Understand threat landscape

Master technical skills

Learn the basics



STAY SAFE!

MASTER TECH SKILLS

– Make sure your IT and security personnel have access to training

Get the right gear

STAY SAFE!

MASTER TECH SKILLS

– Make sure your team has the tools, budget, and management support needed

Practice! Use and maintain your gear

Stay Safe!

MASTER TECH SKILLS

– Tabletop exercises, red team / purple team, capture the flag events

Plan appropriately

STAY SAFE!

MASTER TECH SKILLS

– Know your broader business goals, but also make sure safety is planned from the start

Continuously improve

Stay Safe!

MASTER TECH SKILLS

– Apply lessons learned from practice and real world scenarios

Understand threat landscape

Know what you’re up against

Operational threats

Stay Safe!

UNDERSTAND THREATS

– Equipment failure, personnel turnover, and other factors can impact safety performance

Environmental threats

Stay Safe!

UNDERSTAND THREATS

– Geopolitical and regulator factors can impact your risk

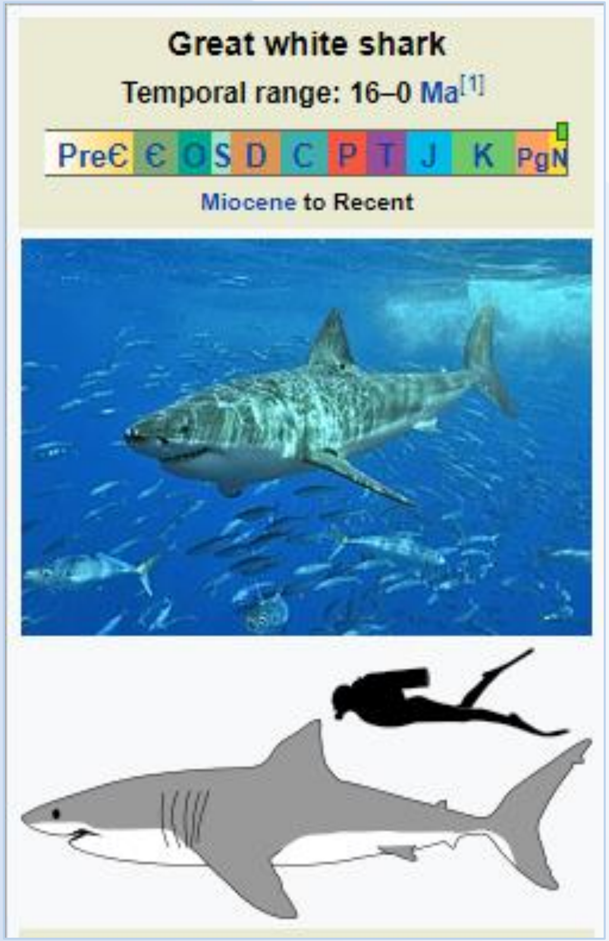
Active threats

STAY SAFE!

UNDERSTAND THREATS

- External (or internal) attacks require additional precautions

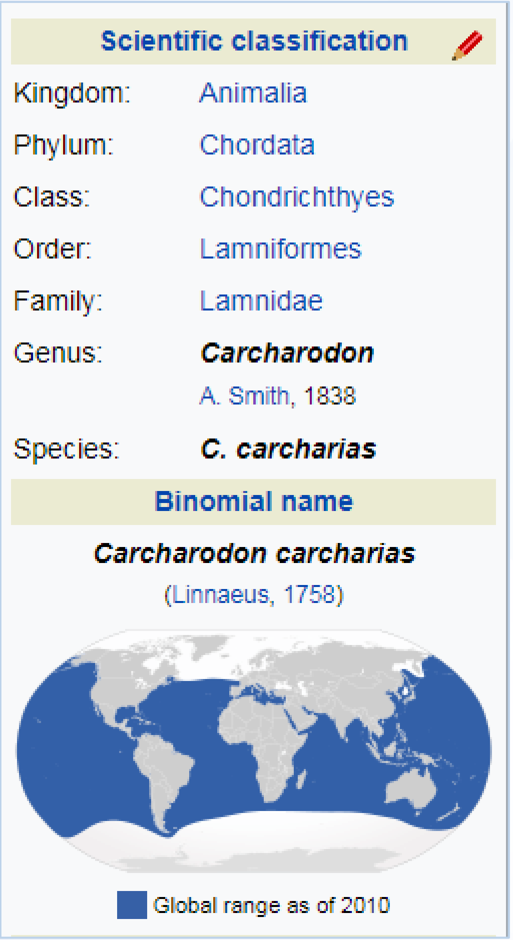
Threat intelligence provides context



Great white shark

Temporal range: 16–0 Ma[1]

Miocene to Recent



Scientific classification

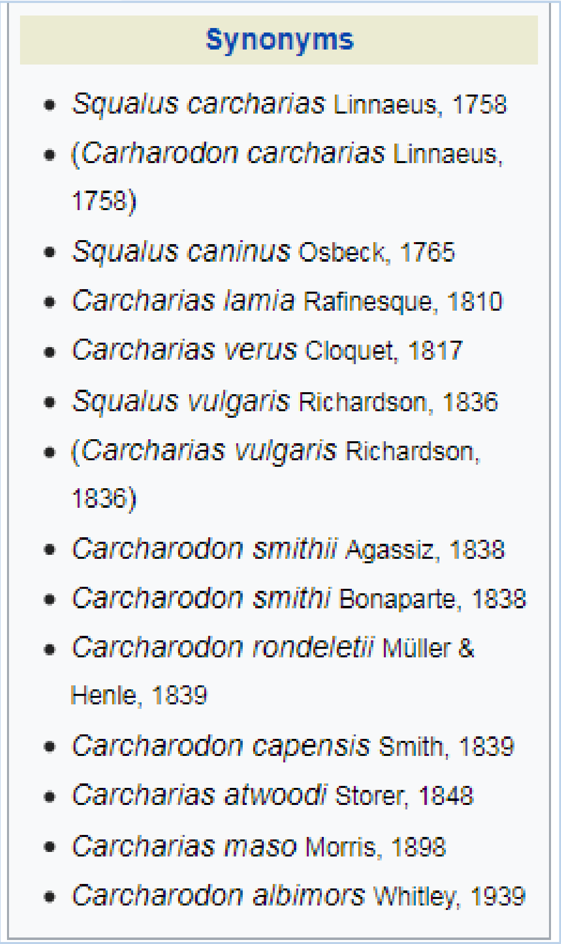
Kingdom:	Animalia
Phylum:	Chordata
Class:	Chondrichthyes
Order:	Lamniformes
Family:	Lamnidae
Genus:	***Carcharodon*** A. Smith, 1838
Species:	***C. carcharias***

Binomial name

Carcharodon carcharias

(Linnaeus, 1758)

■ Global range as of 2010

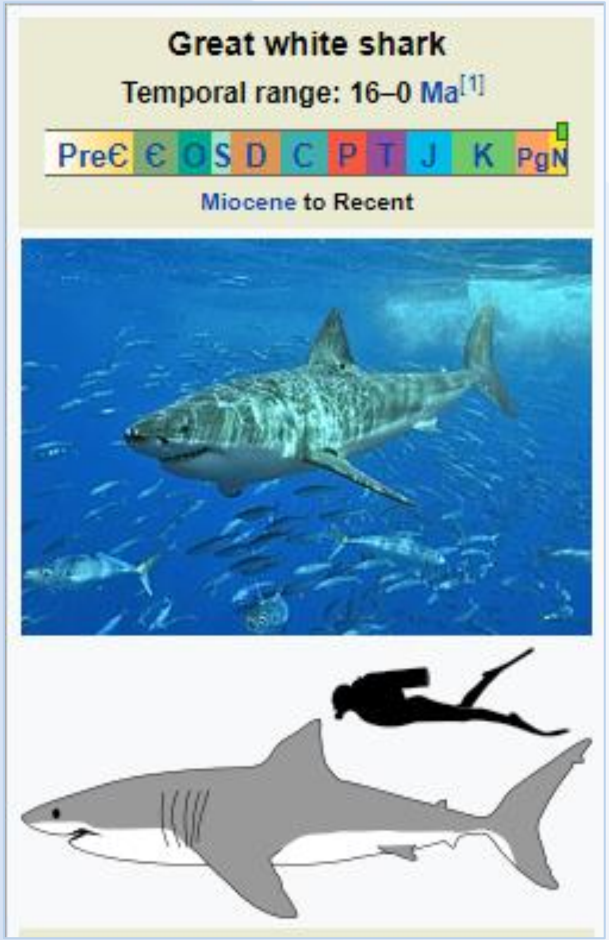


Synonyms

- *Squalus carcharias* Linnaeus, 1758
- (*Carharodon carcharias* Linnaeus, 1758)
- *Squalus caninus* Osbeck, 1765
- *Carcharias lamia* Rafinesque, 1810
- *Carcharias verus* Cloquet, 1817
- *Squalus vulgaris* Richardson, 1836
- (*Carcharias vulgaris* Richardson, 1836)
- *Carcharodon smithii* Agassiz, 1838
- *Carcharodon smithi* Bonaparte, 1838
- *Carcharodon rondeletii* Müller & Henle, 1839
- *Carcharodon capensis* Smith, 1839
- *Carcharias atwoodi* Storer, 1848
- *Carcharias maso* Morris, 1898
- *Carcharodon albimors* Whitley, 1939

* Wikipedia. “Great white shark.” Available online at https://en.wikipedia.org/wiki/Great_white_shark

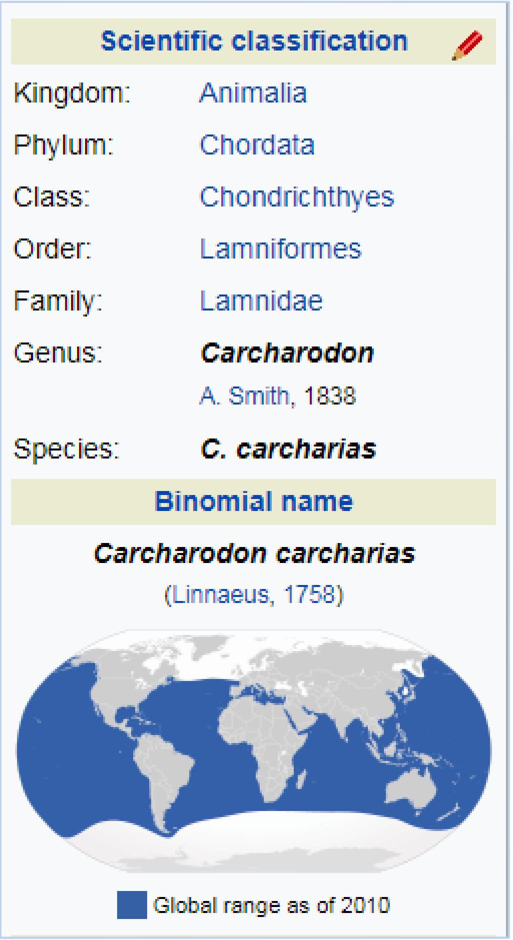
Threat intelligence provides context



Great white shark

Temporal range: 16–0 Ma[1]

Miocene to Recent



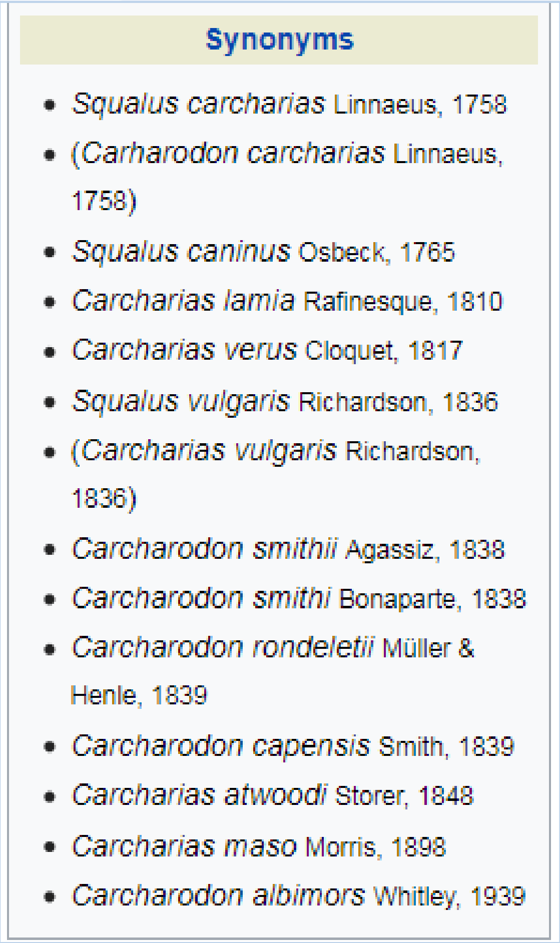
Scientific classification	
Kingdom:	Animalia
Phylum:	Chordata
Class:	Chondrichthyes
Order:	Lamniformes
Family:	Lamnidae
Genus:	***Carcharodon*** A. Smith, 1838
Species:	***C. carcharias***

Binomial name

Carcharodon carcharias

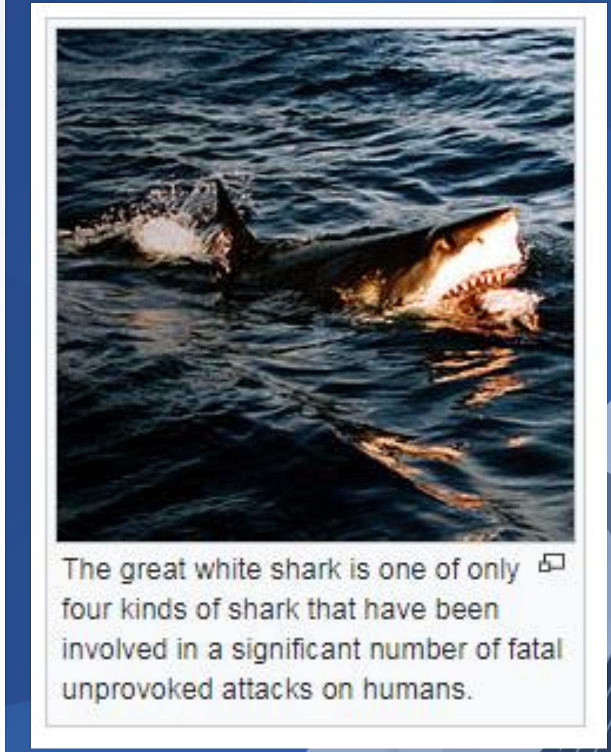
(Linnaeus, 1758)

■ Global range as of 2010



Synonyms

- *Squalus carcharias* Linnaeus, 1758
- (*Carharodon carcharias* Linnaeus, 1758)
- *Squalus caninus* Osbeck, 1765
- *Carcharias lamia* Rafinesque, 1810
- *Carcharias verus* Cloquet, 1817
- *Squalus vulgaris* Richardson, 1836
- (*Carcharias vulgaris* Richardson, 1836)
- *Carcharodon smithii* Agassiz, 1838
- *Carcharodon smithi* Bonaparte, 1838
- *Carcharodon rondeletii* Müller & Henle, 1839
- *Carcharodon capensis* Smith, 1839
- *Carcharias atwoodi* Storer, 1848
- *Carcharias maso* Morris, 1898
- *Carcharodon albimors* Whitley, 1939



The great white shark is one of only four kinds of shark that have been involved in a significant number of fatal unprovoked attacks on humans.

* Wikipedia. "Great white shark." Available online at https://en.wikipedia.org/wiki/Great_white_shark

Put advanced attacks in context

It’s a “who” not a “what”

- There is a human at the keyboard
- Performing highly tailored and customized attacks
- Targeted at YOU

Professional, organized, well funded

- Attackers escalate sophistication of their tactics as needed
- They remain relentlessly focused on their objective

If you kick them out, they WILL return

- They have specific objectives
- Their goal can be long-term or short-term
- They use persistence tools and tactics to ensure ongoing access

Put advanced attacks in context

It’s a “who” not a “what”

- There is a human at the keyboard
- Performing highly tailored and customized attacks
- Targeted at YOU

Professional, organized, well funded

- Attackers escalate sophistication of their tactics as needed
- They remain relentlessly focused on their objective

If you kick them out, they WILL return

- They have specific objectives
- Their goal can be long-term or short-term
- They use persistence tools and tactics to ensure ongoing access

64%

- IR customers who experienced a significant attack by the same or similarly motivated attack group within 19 months

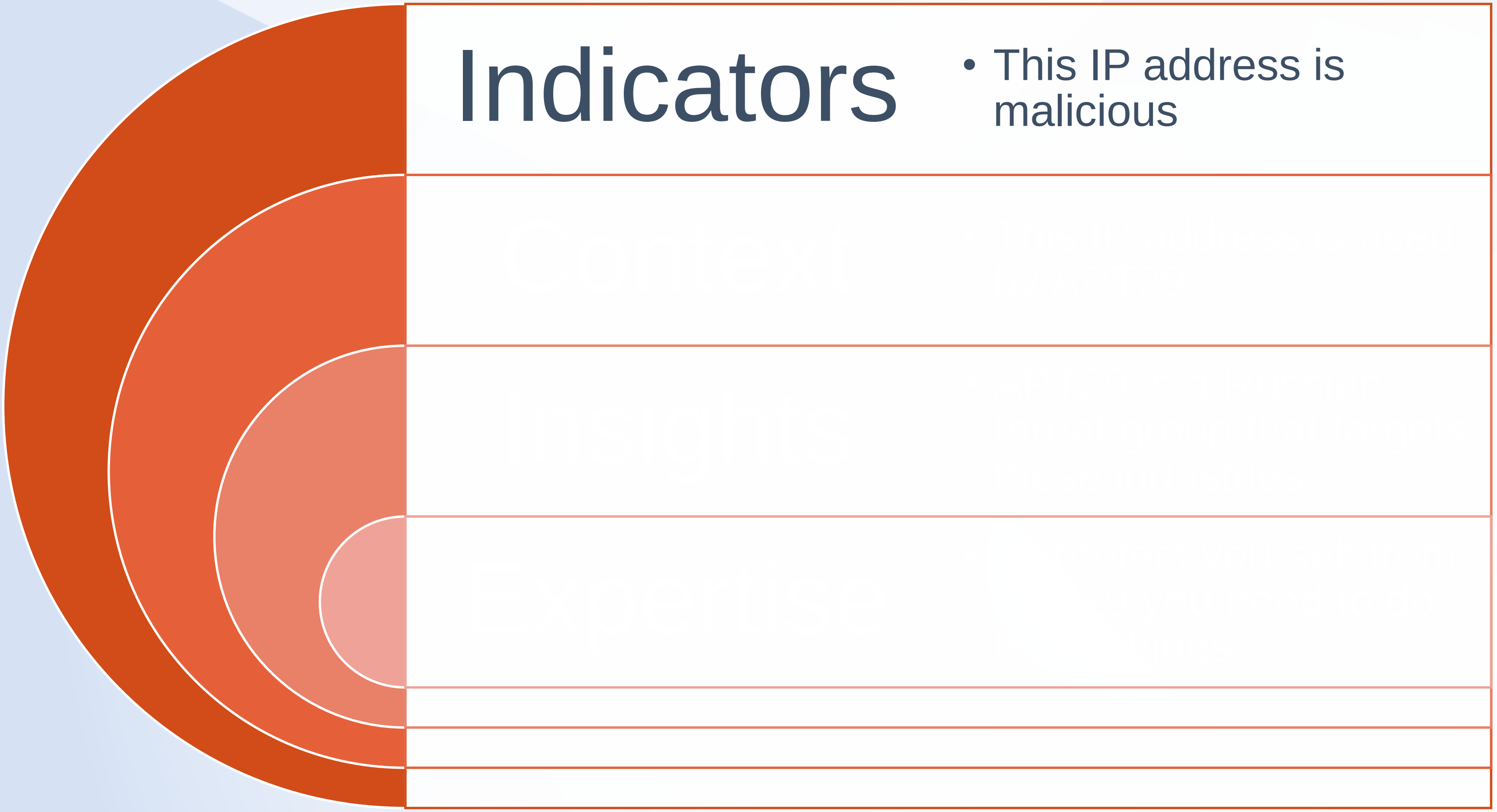
49%

- IR customers who had at least one significant attack who were successfully attacked again within one year

86%

- IR customers who had more than one significant attack who had more than one unique attacker in their environment

Not all threat intelligence is equal



Indicators

- This IP address is malicious

Context

- This IP address is used by APT28

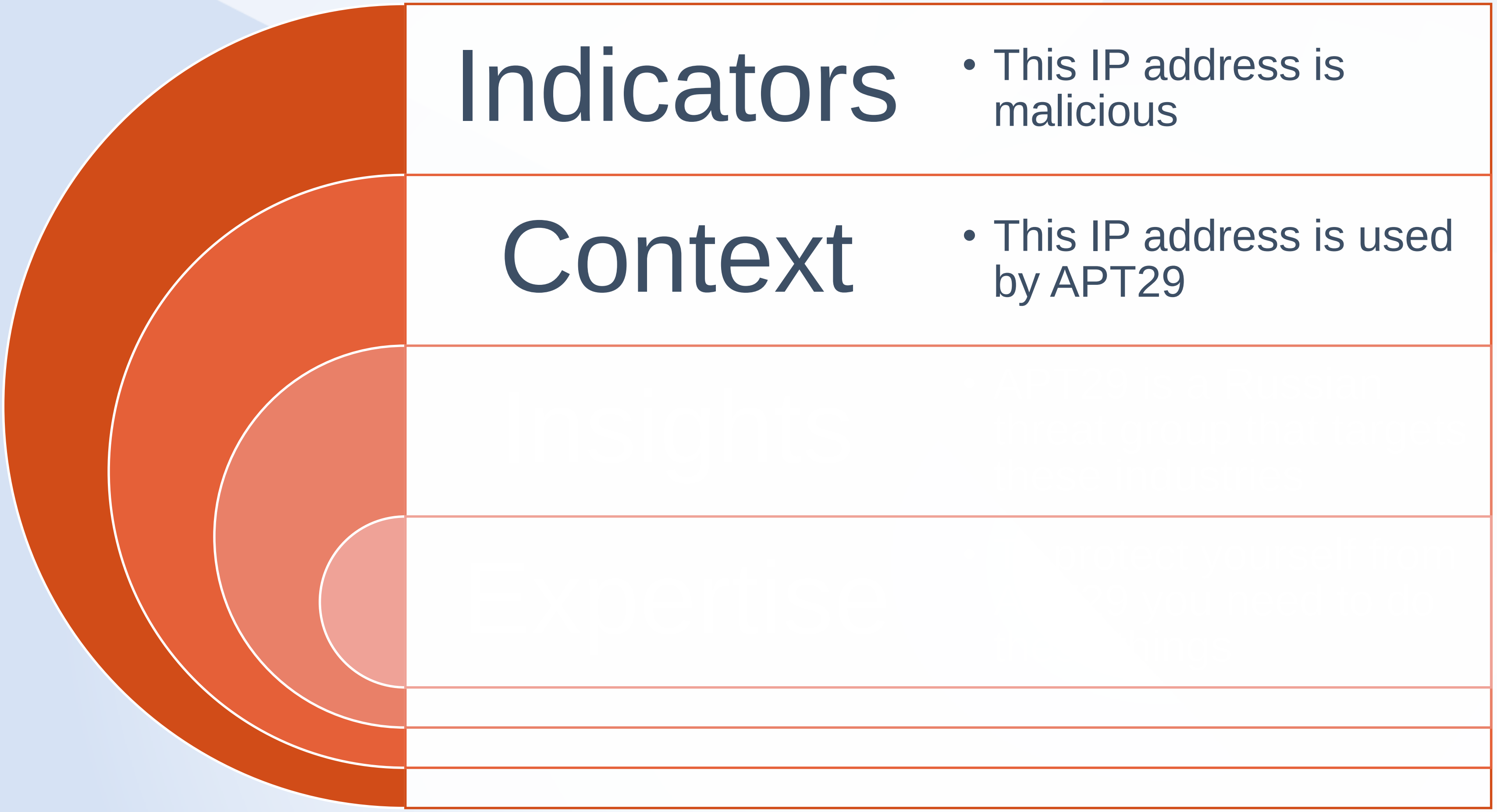
Insights

- APT28 is a Russian [illegible] that [illegible] these industries

Expertise

- [illegible]

Not all threat intelligence is equal



Indicators

- This IP address is malicious

Context

- This IP address is used by APT29

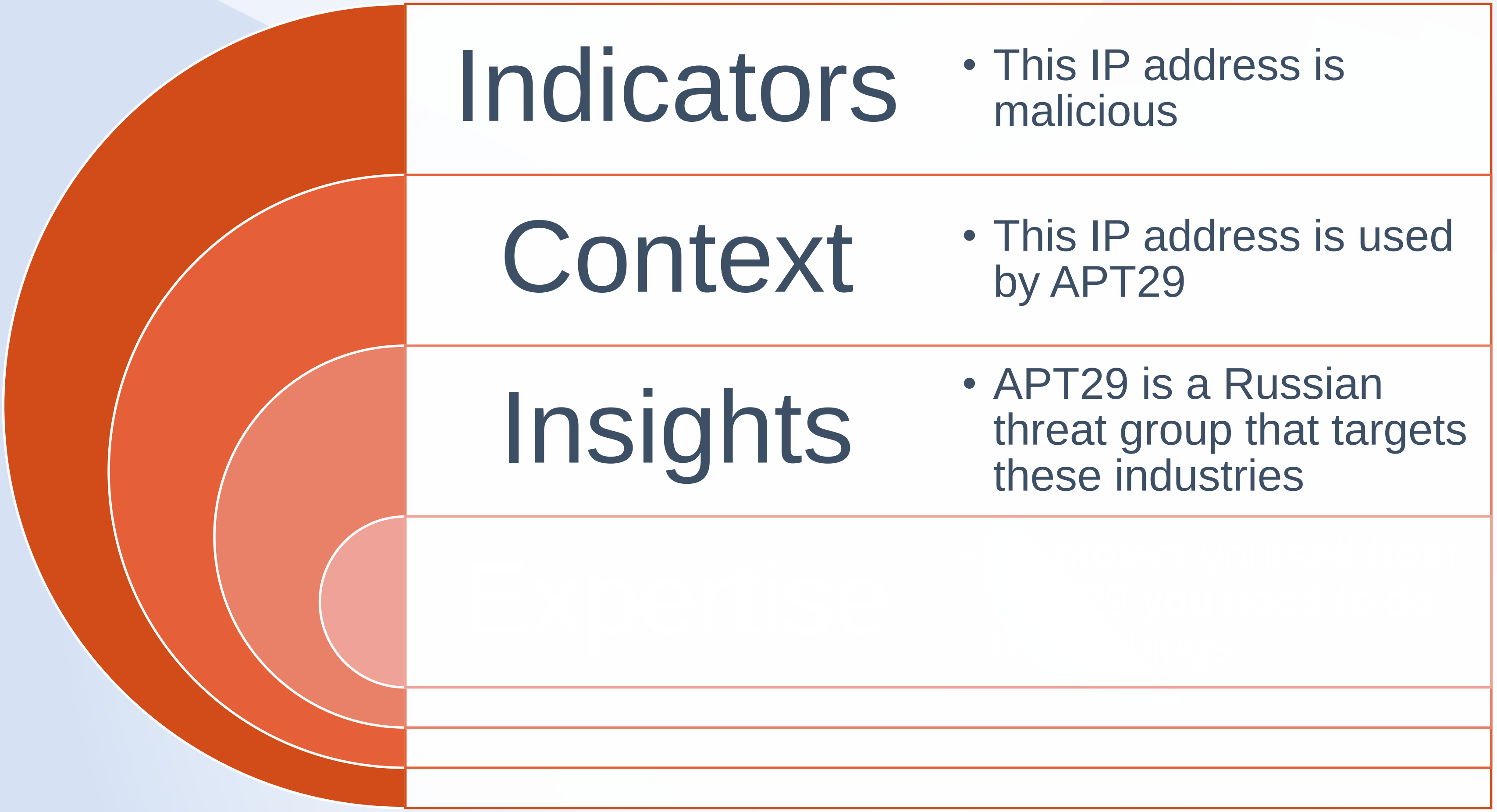
Insights

- APT29 is a Russian intelligence group that targets these industries

Expertise

- [illegible]

Not all threat intelligence is equal



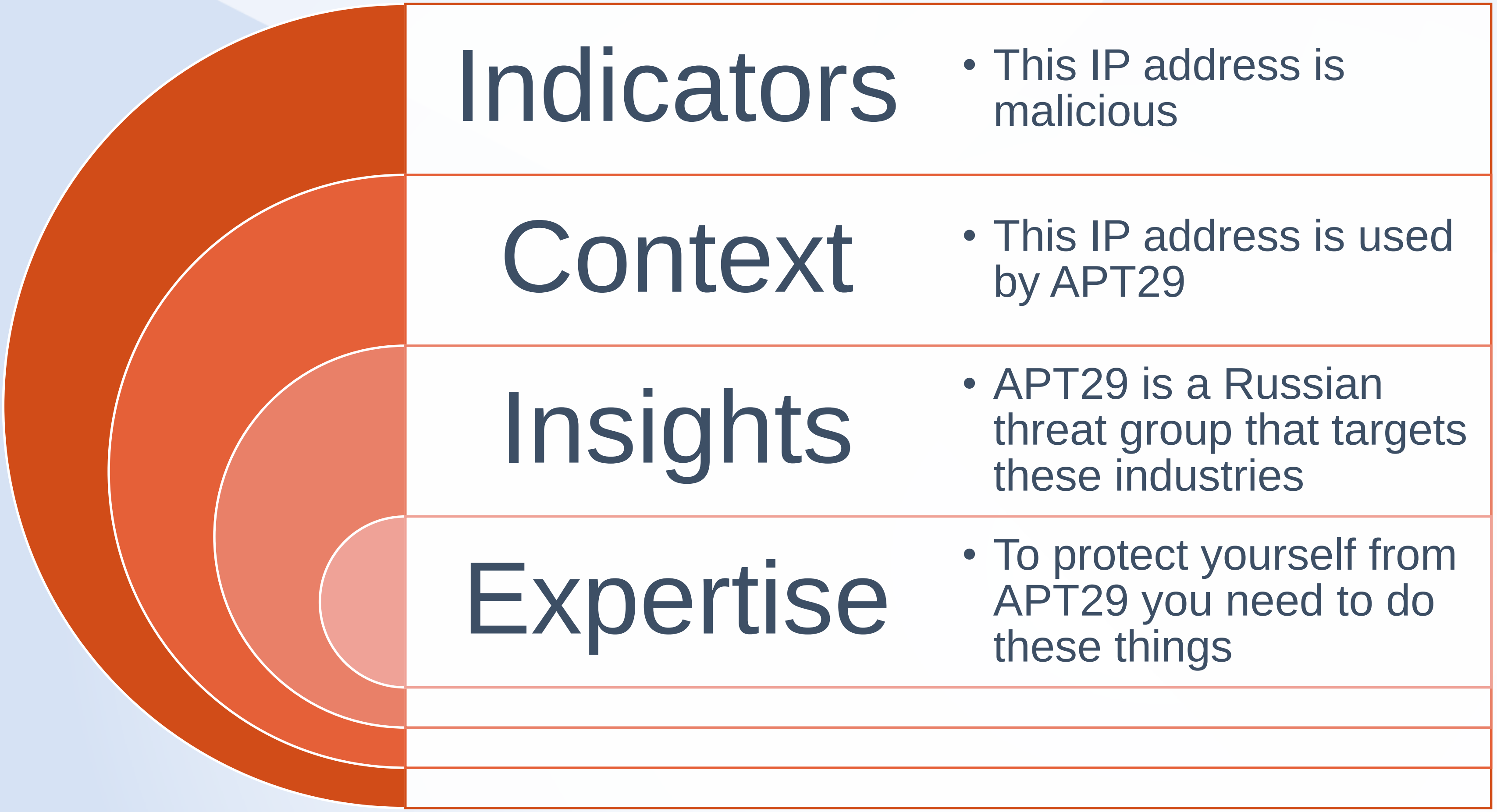
Indicators
- This IP address is malicious

Context
- This IP address is used by APT29

Insights
- APT29 is a Russian threat group that targets these industries

Expertise
- [illegible]

Not all threat intelligence is equal



Indicators

- This IP address is malicious

Context

- This IP address is used by APT29

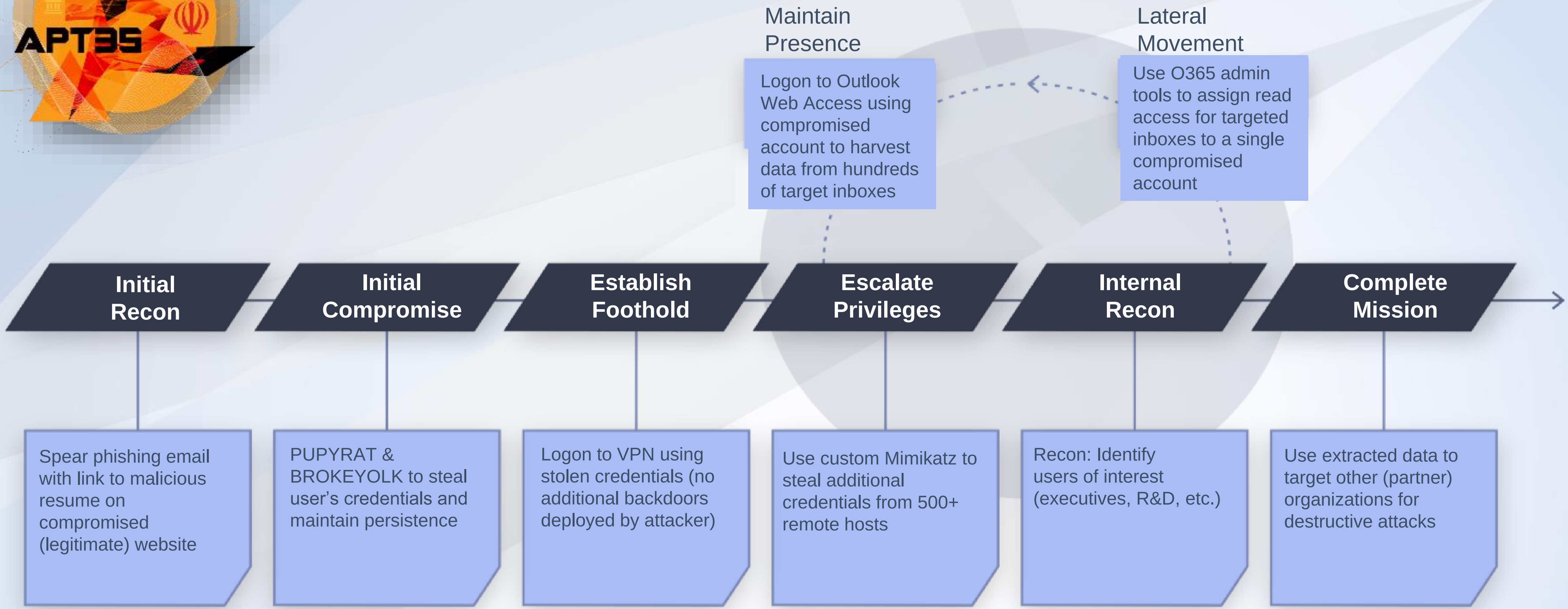
Insights

- APT29 is a Russian threat group that targets these industries

Expertise

- To protect yourself from APT29 you need to do these things

APT35 (Newscaster) Case Study*



Initial Recon

Spear phishing email with link to malicious resume on compromised (legitimate) website

Initial Compromise

PUPYRAT & BROKEYOLK to steal user’s credentials and maintain persistence

Establish Foothold

Logon to VPN using stolen credentials (no additional backdoors deployed by attacker)

Escalate Privileges

Use custom Mimikatz to steal additional credentials from 500+ remote hosts

Internal Recon

Recon: Identify users of interest (executives, R&D, etc.)

Complete Mission

Use extracted data to target other (partner) organizations for destructive attacks

Maintain Presence

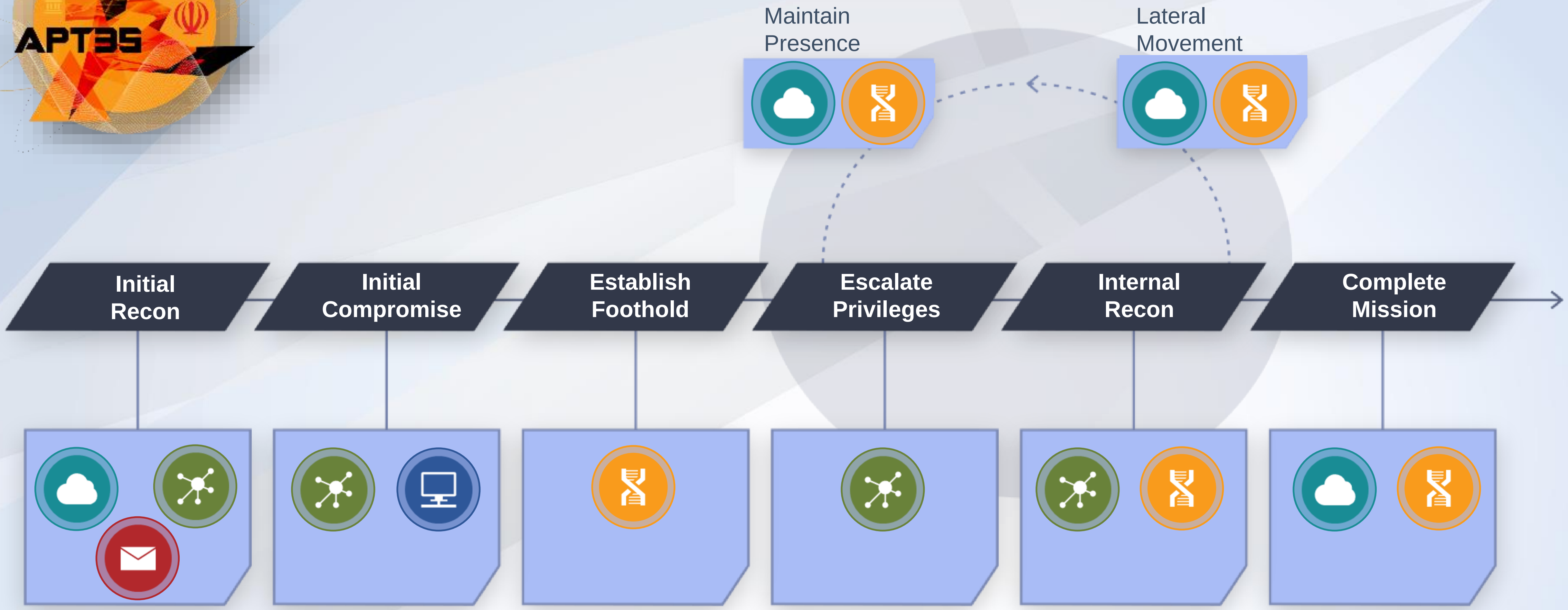
Logon to Outlook Web Access using compromised account to harvest data from hundreds of target inboxes

Lateral Movement

Use O365 admin tools to assign read access for targeted inboxes to a single compromised account

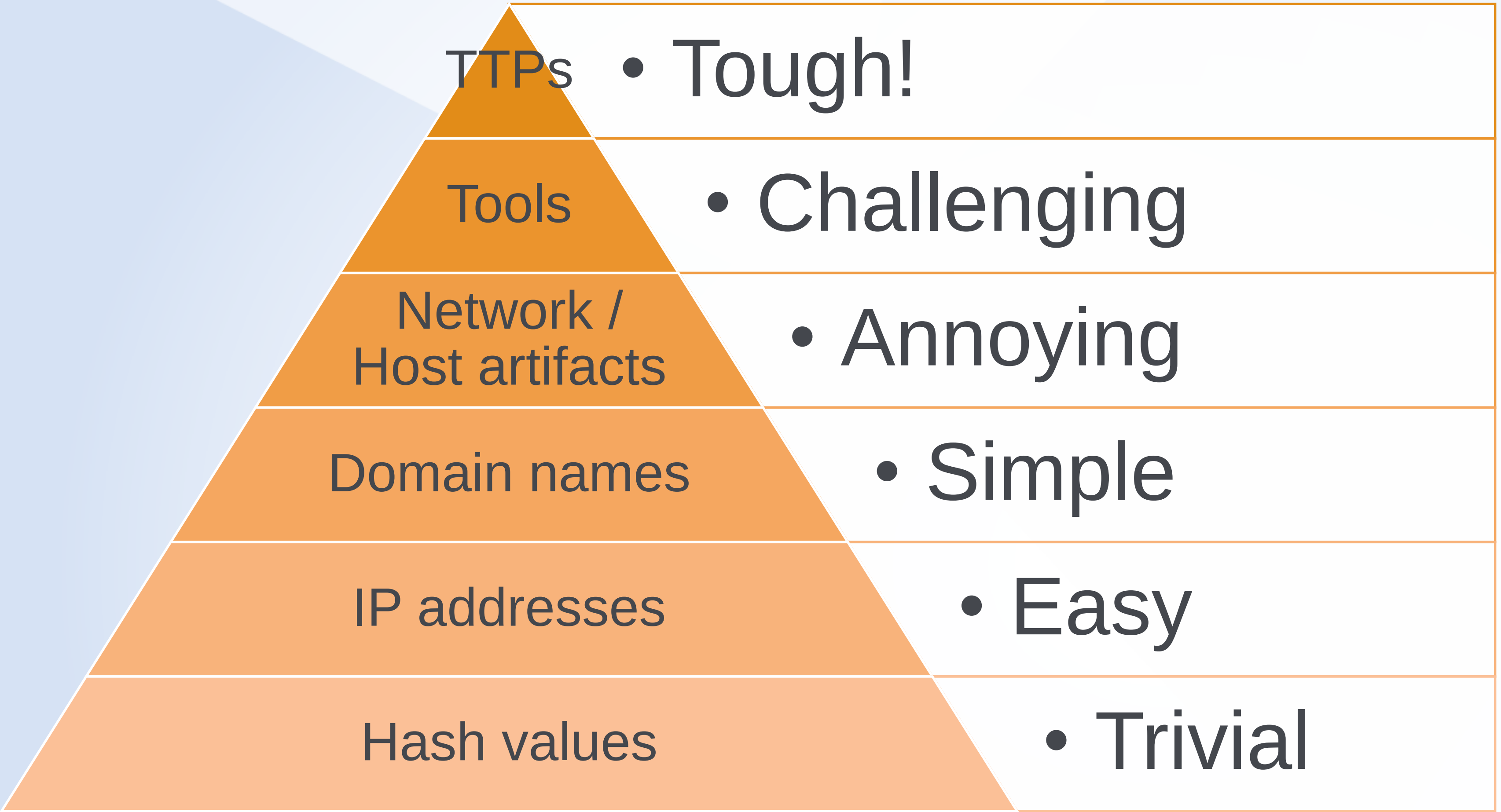
* Mandiant M-Trends 2018

Multiple opportunities to stop an attack



* Mandiant M-Trends 2018

Make attackers work harder



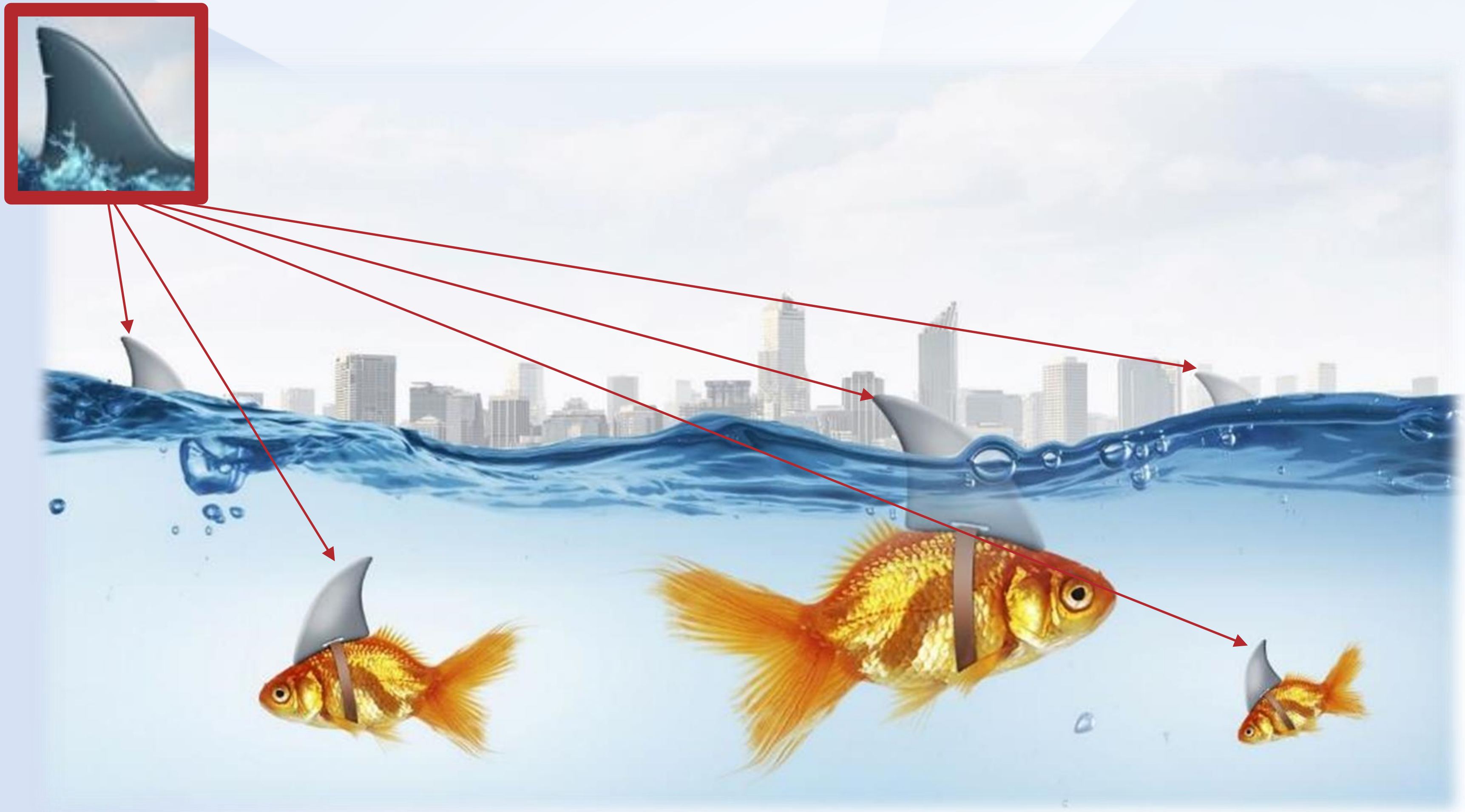
TTPs	• Tough!
Tools	• Challenging
Network / Host artifacts	• Annoying
Domain names	• Simple
IP addresses	• Easy
Hash values	• Trivial

* Bianco, David. “The Pyramid of Pain.” Available online at http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

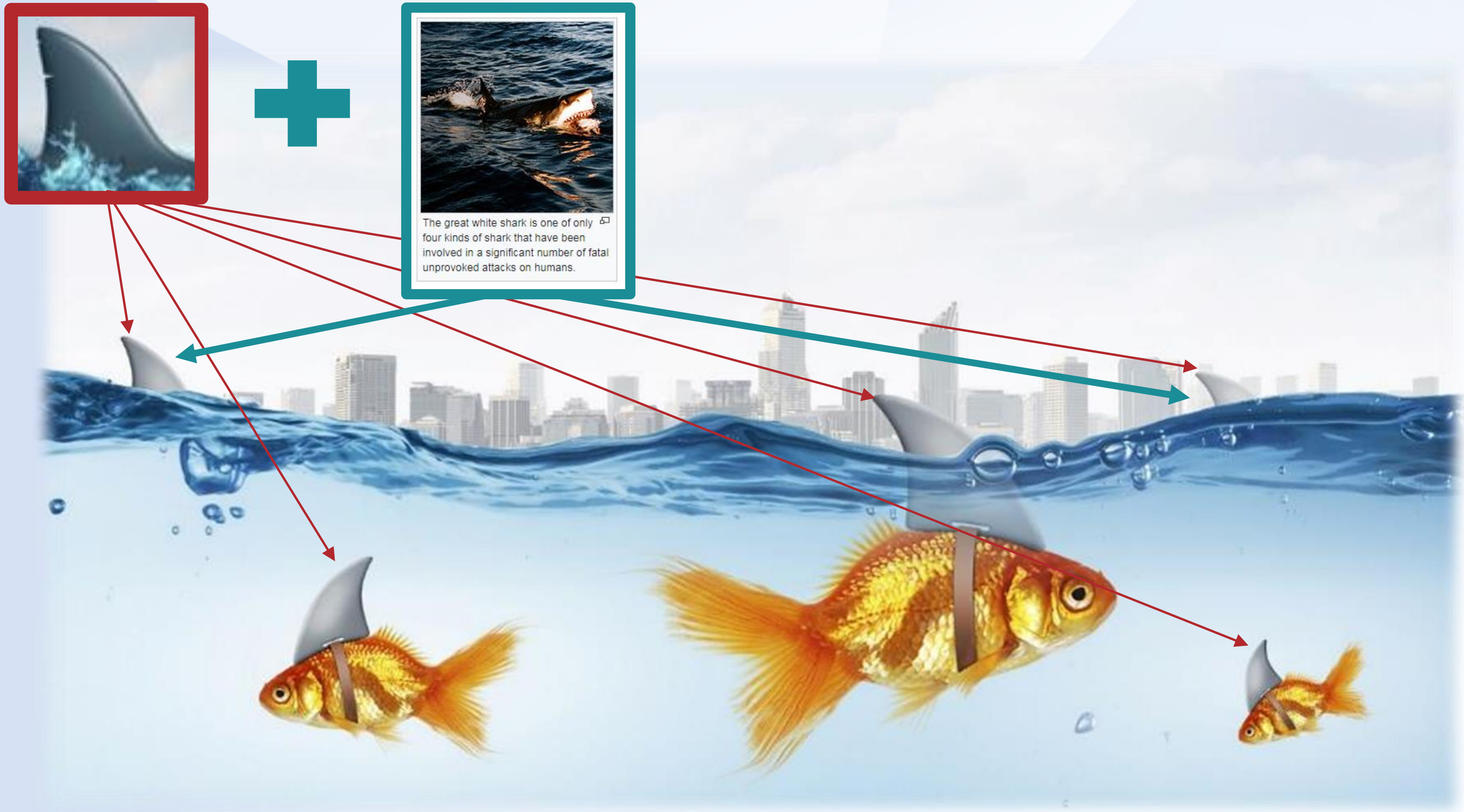
Threat Intelligence vs Machine Learning

Machine Learning can help you detect

Challenges to ML detection

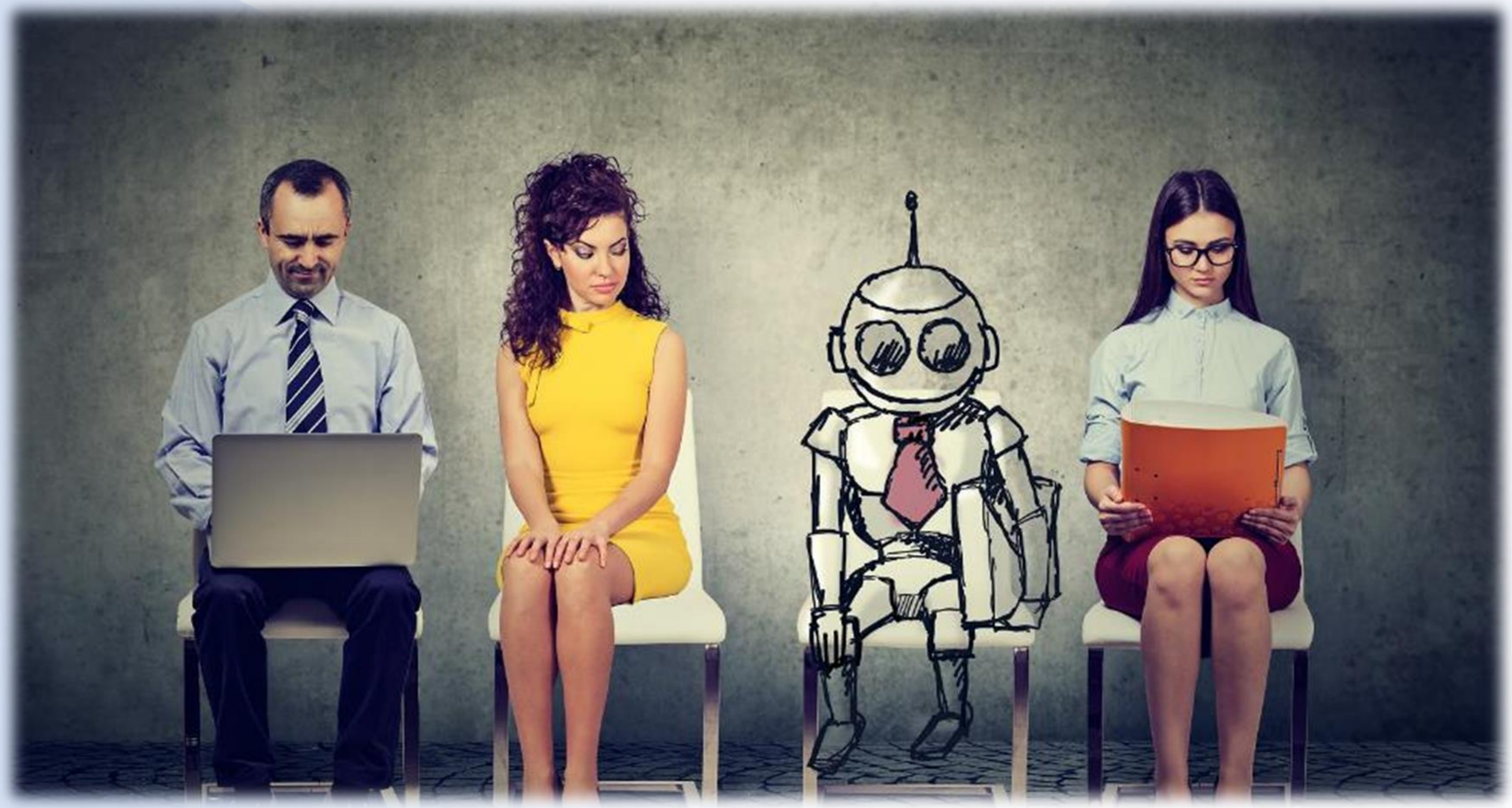


Better intelligence improves ML



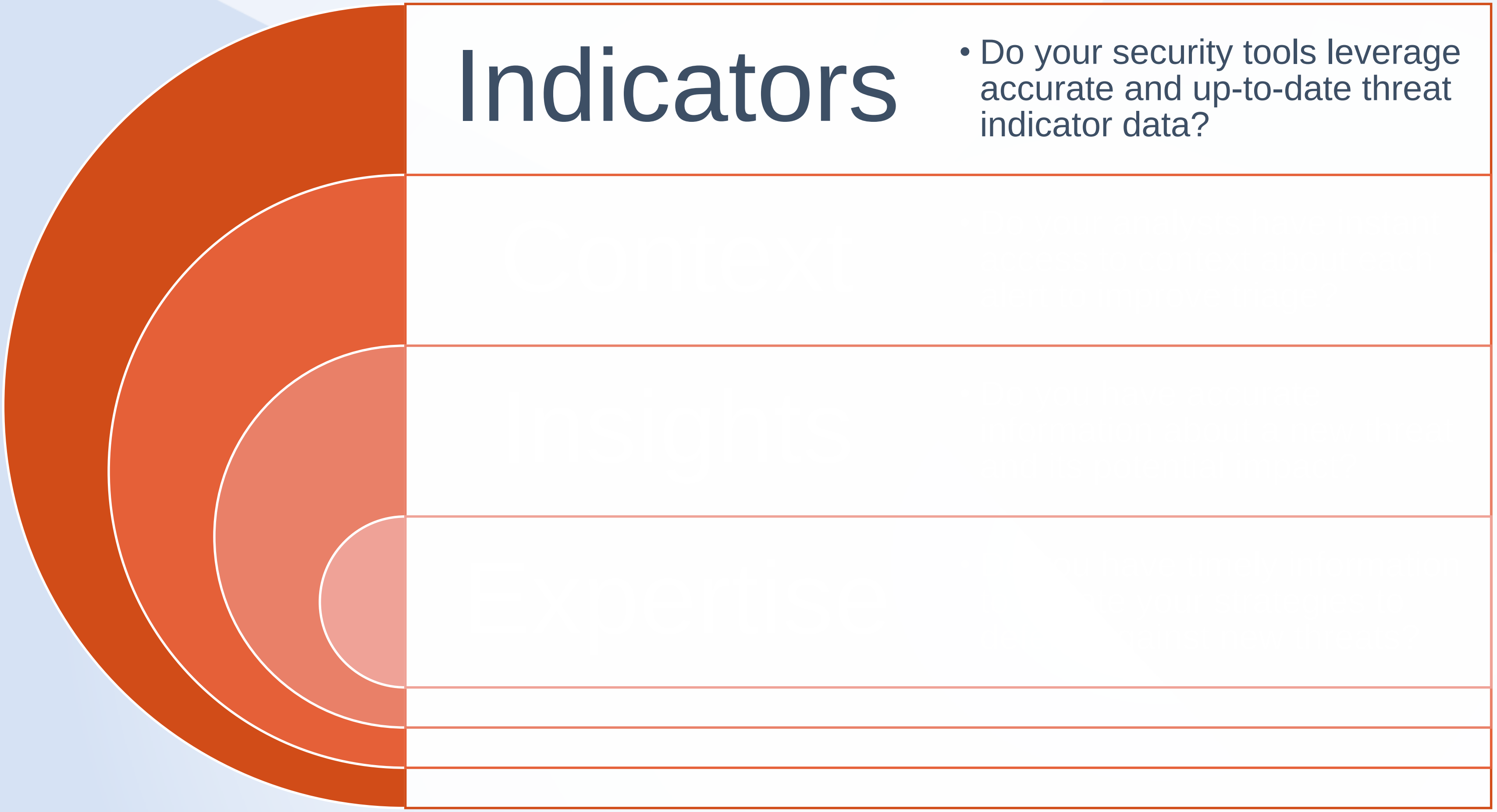
The great white shark is one of only four kinds of shark that have been involved in a significant number of fatal unprovoked attacks on humans.

What about "autonomous AI" solutions?



Applying intelligence to your cybersecurity program

How are you using intelligence today?



Indicators

- Do your security tools leverage accurate and up-to-date threat indicator data?

Context

- [illegible]

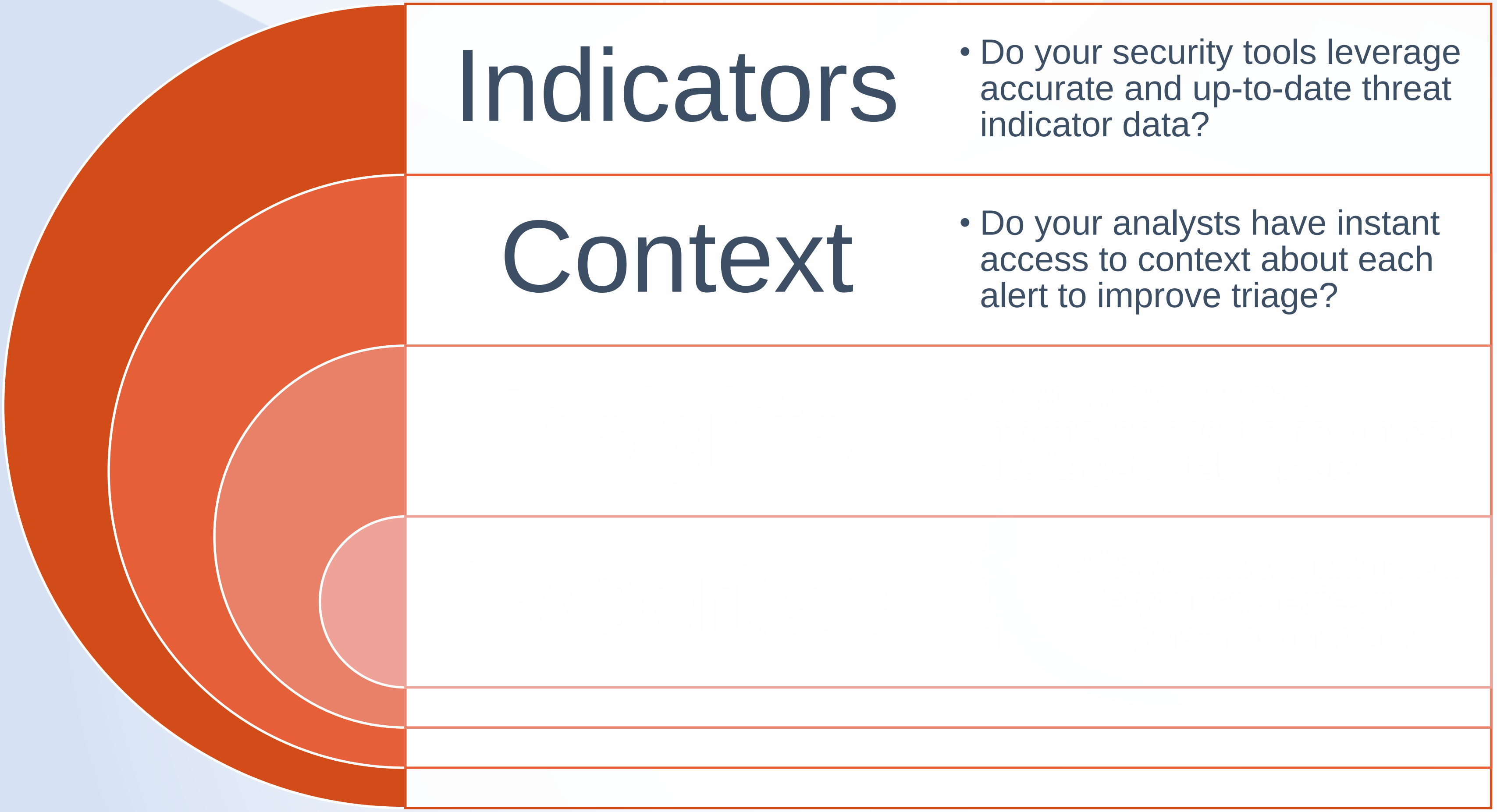
Insights

- [illegible]

Expertise

- [illegible]

How are you using intelligence today?



Indicators

- Do your security tools leverage accurate and up-to-date threat indicator data?

Context

- Do your analysts have instant access to context about each alert to improve triage?

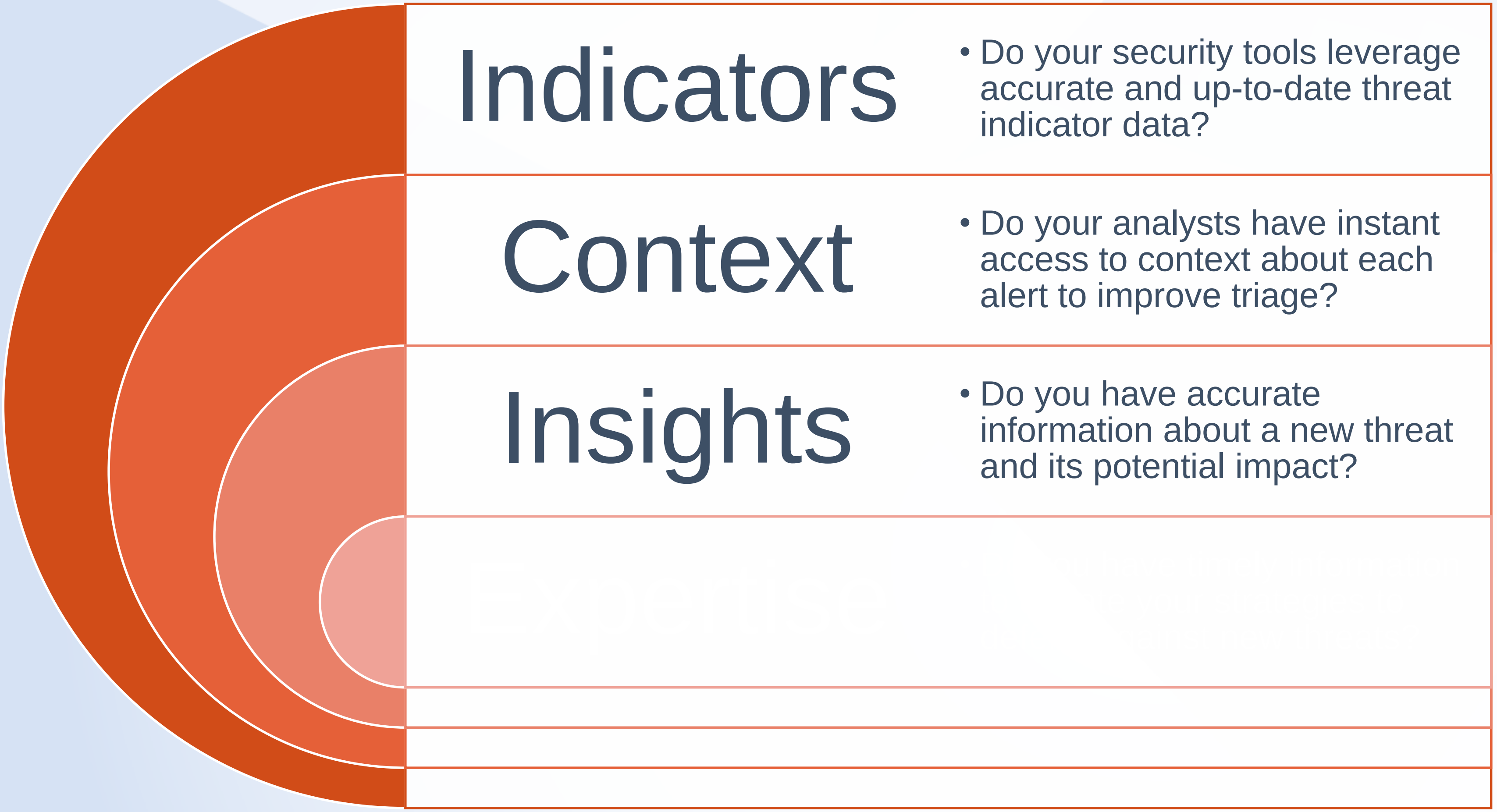
Insights

- Do you have accurate information about adversaries and its potential impact?

Expertise

- [illegible]

How are you using intelligence today?



Indicators

- Do your security tools leverage accurate and up-to-date threat indicator data?

Context

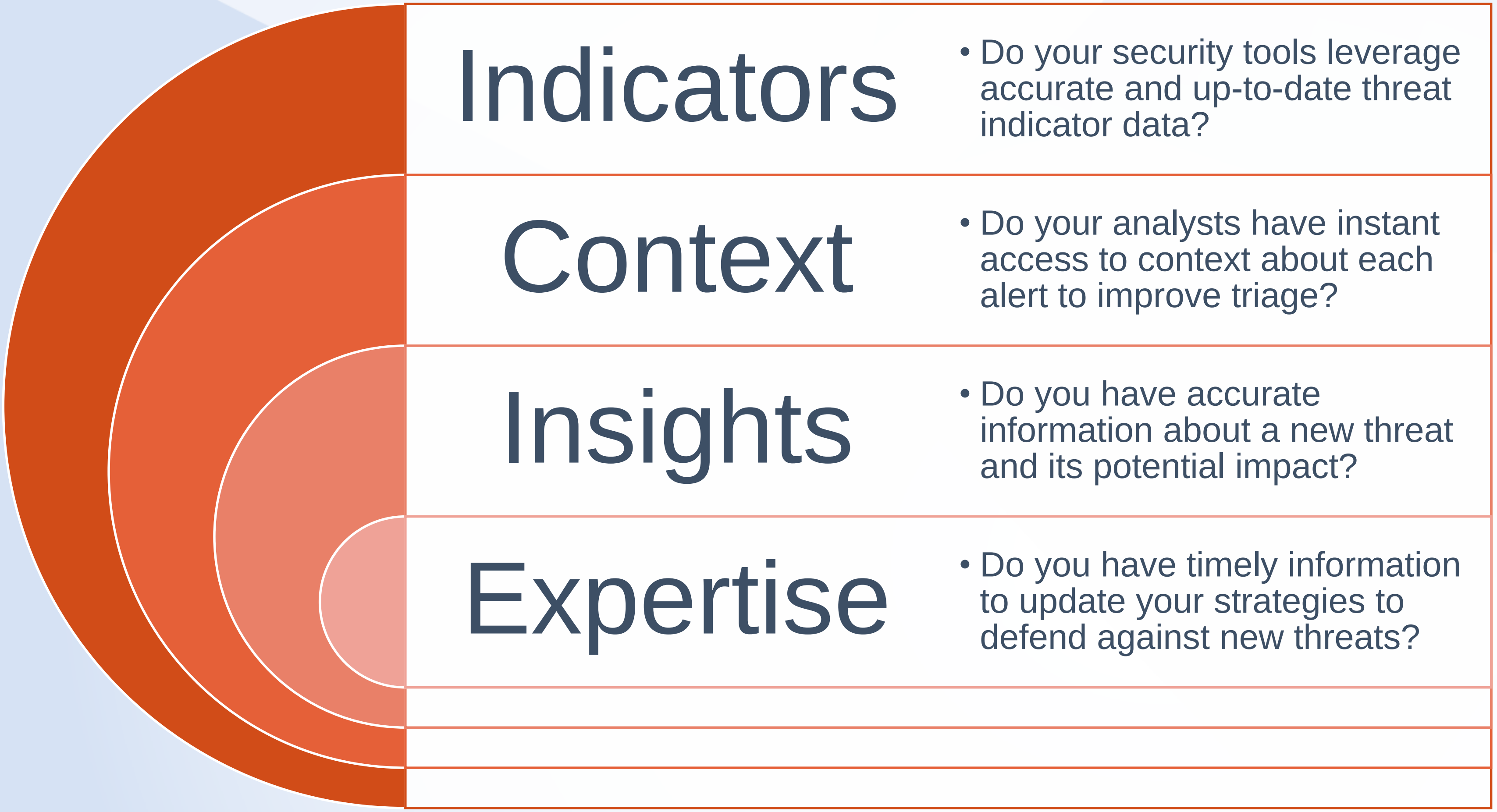
- Do your analysts have instant access to context about each alert to improve triage?

Insights

- Do you have accurate information about a new threat and its potential impact?

Expertise

How are you using intelligence today?



Indicators

- Do your security tools leverage accurate and up-to-date threat indicator data?

Context

- Do your analysts have instant access to context about each alert to improve triage?

Insights

- Do you have accurate information about a new threat and its potential impact?

Expertise

- Do you have timely information to update your strategies to defend against new threats?

Focus on people and processes

Embrace the journey…

Questions?

Christian Schreiber, CISM, PMP

christian.schreiber@fireeye.com

Swimming with sharks: Understanding and countering cyber threats in higher education

Q&A

Christian Schreiber
Higher Education
Cybersecurity Lead
FireEye

Have a question for our presenters? Submit it through the Q&A at the right.

Q&A

University Business is the leader in editorial coverage of news, trends and current issues in higher education.

Subscribe for FREE and stay up-to-date through our print magazine, digital edition, enewsletters and web seminars.

UB University Business

UniversityBusiness.com July 2015

eTextbooks for all Page 51

Student success HQ

Designing, marketing and funding centers that help students succeed 30

CAMPUS FINANCE:

Money lessons for parents

10 ways to make financial literacy a family affair 57

Q&A with Michael Crow

A 'New American University' 10

From overseas to the community college

Recruiting internationals 16

Who let the books out?

Digital-only textbook sales changing the campus store 49

TECHNOLOGY:

New look for help desks

Campus tech support gets a retail makeover 53

Building a better campus

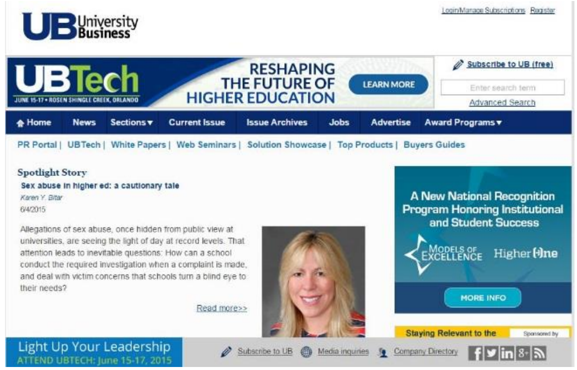
UB's annual construction report 38

Taking your campus to new heights doesn't have to be rocket science.

Visit us at NACUBO Booth 701 to learn more

Follett

Print magazine



UB University Business

Login/Manage Subscriptions Register

UBTech JUNE 15-17 • ROSEN SHINGLE CREEK, ORLANDO

RESHAPING THE FUTURE OF HIGHER EDUCATION

LEARN MORE

Subscribe to UB (free)

Enter search term

Advanced Search

Home | News | Sections ▾ | Current Issue | Issue Archives | Jobs | Advertise | Award Programs ▾

PR Portal | UBTech | White Papers | Web Seminars | Solution Showcase | Top Products | Buyers Guides

Spotlight Story

Sex abuse in higher ed: a cautionary tale

Karen Y. Bitar

6/4/2015

Allegations of sex abuse, once hidden from public view at universities, are seeing the light of day at record levels. That attention leads to inevitable questions: How can a school conduct the required investigation when a complaint is made, and deal with victim concerns that schools turn a blind eye to their needs?

Read more>>

A New National Recognition Program Honoring Institutional and Student Success

Models of Excellence Higher One

MORE INFO

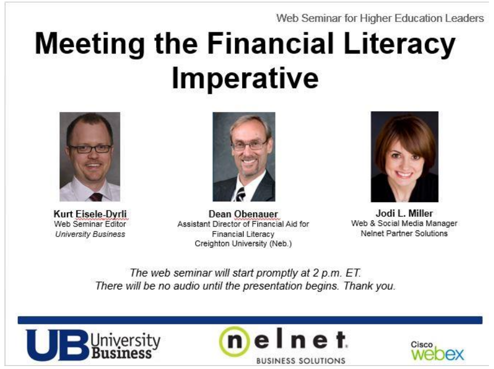
Staying Relevant to the Sponsored by

Light Up Your Leadership

ATTEND UBTECH: June 15-17, 2015

Subscribe to UB Media inquiries Company Directory

Digital edition and website



Web Seminar for Higher Education Leaders

Meeting the Financial Literacy Imperative

Kurt Eisele-Dyrli
Web Seminar Editor
University Business

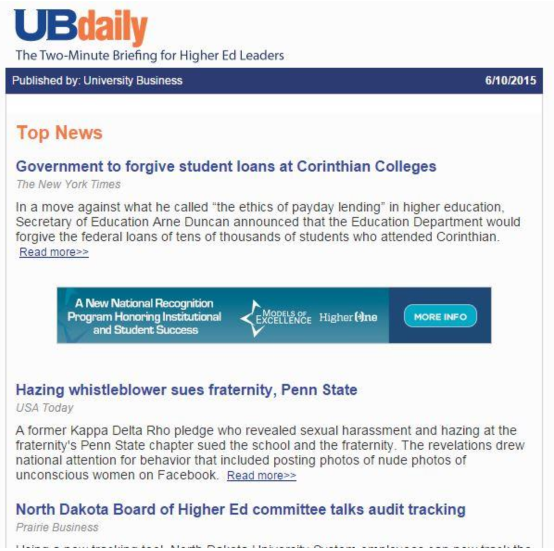
Dean Obenauer
Assistant Director of Financial Aid for Financial Literacy
Creighton University (Neb.)

Jodi L. Miller
Web & Social Media Manager
Nelnet Partner Solutions

The web seminar will start promptly at 2 p.m. ET.
There will be no audio until the presentation begins. Thank you.

UB University Business nelnet BUSINESS SOLUTIONS Cisco webex

Web seminars



UBdaily

The Two-Minute Briefing for Higher Ed Leaders

Published by: University Business 6/10/2015

Top News

Government to forgive student loans at Corinthian Colleges

The New York Times

In a move against what he called "the ethics of payday lending" in higher education, Secretary of Education Arne Duncan announced that the Education Department would forgive the federal loans of tens of thousands of students who attended Corinthian. Read more>>

A New National Recognition Program Honoring Institutional and Student Success

Models of Excellence Higher One

MORE INFO

Hazing whistleblower sues fraternity, Penn State

USA Today

A former Kappa Delta Rho pledge who revealed sexual harassment and hazing at the fraternity's Penn State chapter sued the school and the fraternity. The revelations drew national attention for behavior that included posting photos of nude photos of unconscious women on Facebook. Read more>>

North Dakota Board of Higher Ed committee talks audit tracking

Prairie Business

UB Daily, and other enewsletters

Thank you for joining us!

The archive recording of this web seminar will be available for you to review, or share with members of your team, at:

http://www.UniversityBusiness.com/Web-Seminars

You will also receive an email with a link to the slides.