Gartner Security & Risk Management Summit

17 – 20 June 2019 / National Harbor, MD

Threat Intelligence: The Thing That Has the Thing to Do the Thing

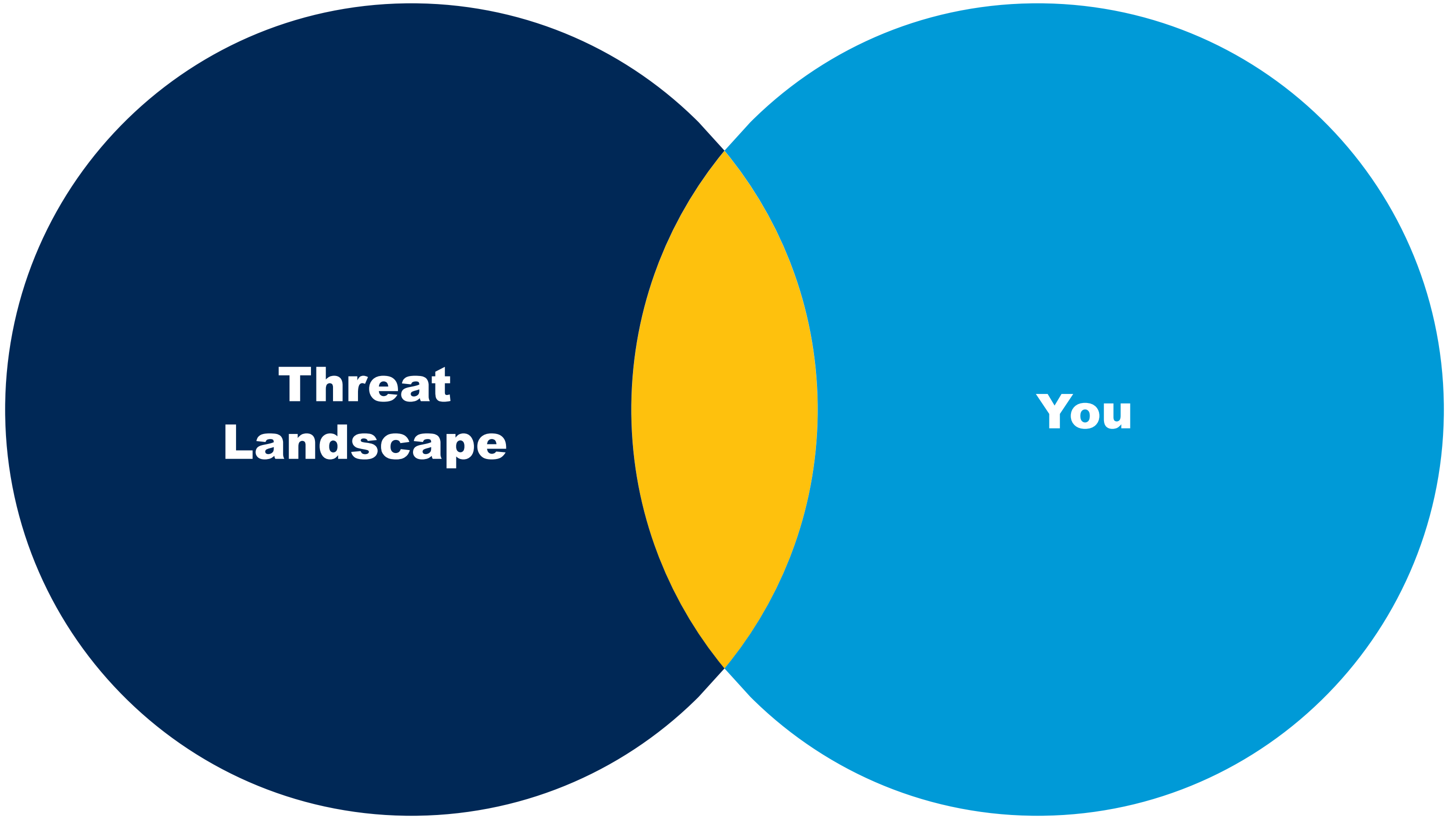
Craig Lawson
@craiglawson

Gartner®

Key Issues

1. The State of the Threat Intelligence Market
2. The Gartner Maturity Model for Threat Intelligence
3. The Main Use Cases

Threat Intelligence Helps You Understand Something Fundamental



Key Issues

1. The State of the Threat Intelligence Market
2. The Gartner Maturity Model for Threat Intelligence
3. The Main Use Cases

What Is Threat Intelligence?

Threat intelligence is **evidence-based** knowledge, including context, mechanisms, indicators, implications and **actionable advice** about an existing or emerging menace or hazard to assets to that can be used to **inform decisions** regarding the subject’s **response** to that menace or hazard.

Source: “How Gartner Defines Threat Intelligence” (G00299526)

We Are Tracking Well Over 100+ Vendors in This Market

abuse.ch
NCC Group-Fox-IT
Symantec
Anomali
ThreatQuotient
BlueLiv
Exploit Database maintained by Offensive
Digital Shadows
FireEye
Cofense
ThreatBook
IBM
InCyber
Carbonite-Webroot
CyberInt
ZeroFOX
RiskSense
Secureworks
NopSec
AusCERT
Tenable.io
BAE Systems
United States Computer Emergency Readiness Team (US CERT)
Infoblox
Flashpoint
ReversingLabs
Perch
Security
Team Cymru
Farsight Security
Proofpoint
Group-IB
Critical Stack
Verint Systems-SenseCy
Intel 471
SANS Institute
Financial Services Information Sharing and Analysis Center (FS-ISAC)
DomainTools
ThreatConnect
Australian Cyber Security Centre (ACSC)
EclecticIQ
Sixgill
Kenna Security

Figuring Out What You Want vs. Need Is Actually Hard

- Breadth of Coverage
- Depth and Accuracy
- Ability to Execute
- Extensibility
- Industry Specialization

The Three “A”s Still Apply

Acquire

- Commercial
- Open-Source
- End-User Led
- Community-Driven
- Industry-Led

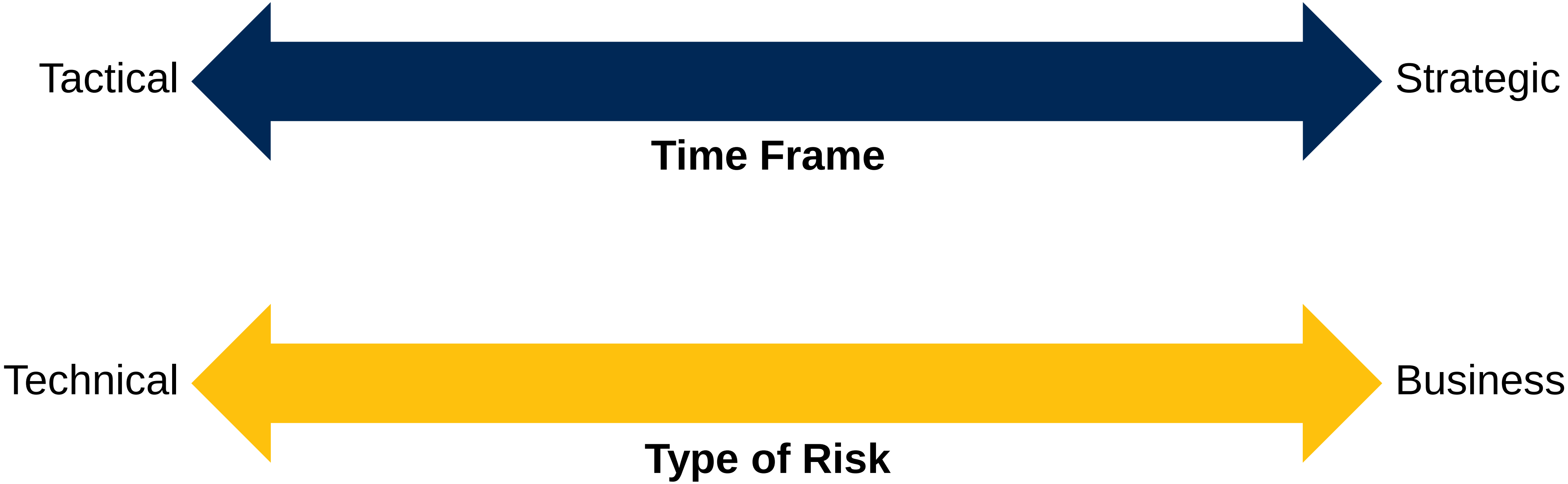
Aggregate

- Threat Intelligence Platforms (TIPs)
- SOAR
- Existing Controls

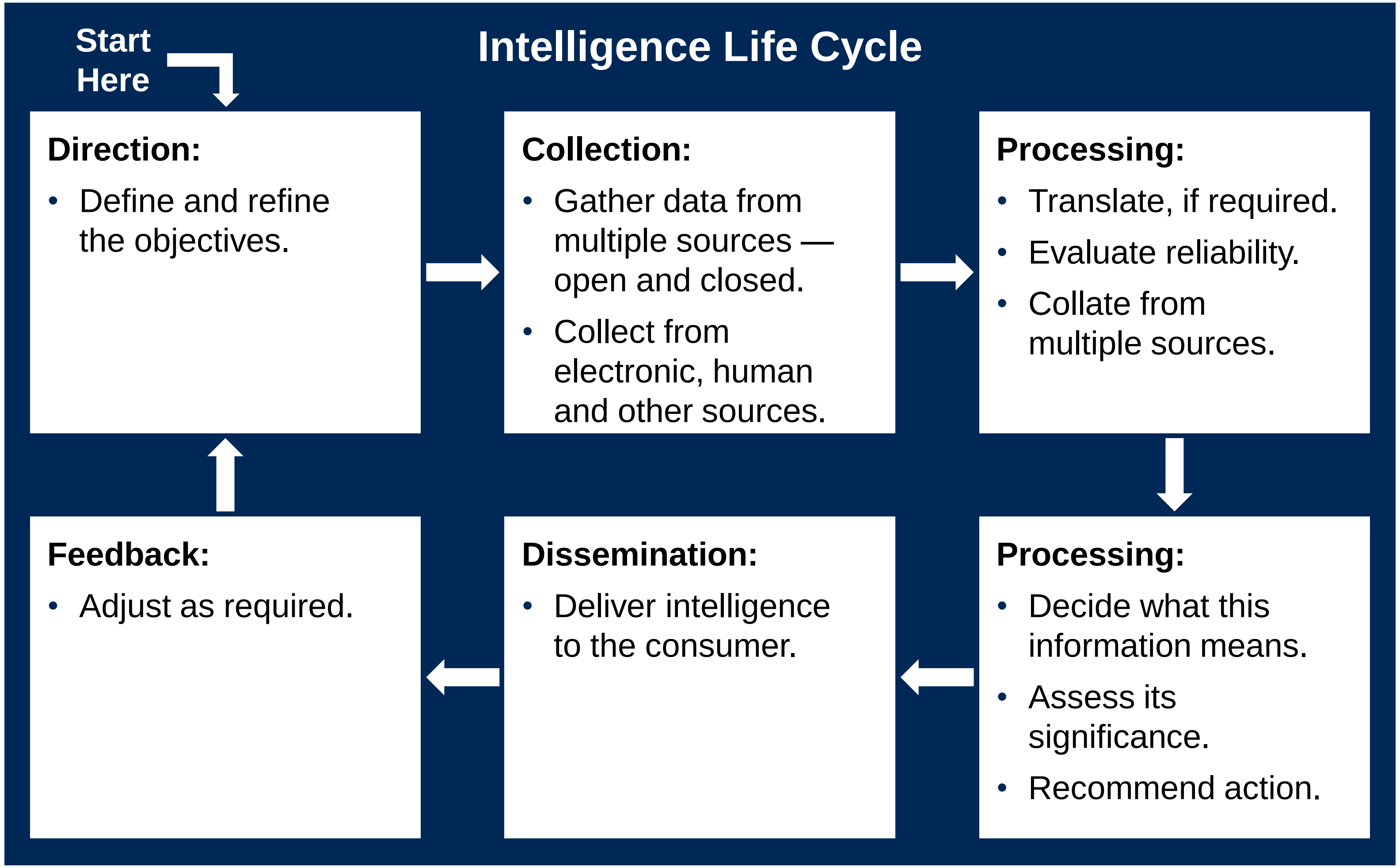
Action

- Predict
- Prevent
- Detect
- Respond

How TI Services Can Add Value to Your Security Program



The Typical Intelligence Life Cycle



Intelligence Life Cycle

Start Here

Direction:

- Define and refine the objectives.

Collection:

- Gather data from multiple sources — open and closed.
- Collect from electronic, human and other sources.

Processing:

- Translate, if required.
- Evaluate reliability.
- Collate from multiple sources.

Processing:

- Decide what this information means.
- Assess its significance.
- Recommend action.

Dissemination:

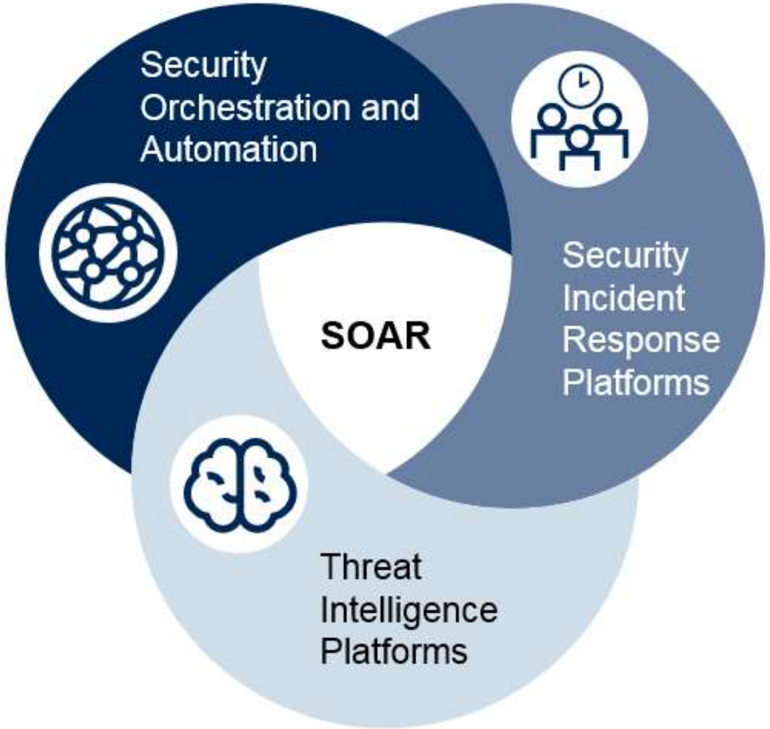
- Deliver intelligence to the consumer.

Feedback:

- Adjust as required.

Security Orchestration Automation and Response = SOA + SIR + TIP

SOAR Types


Security Orchestration and Automation
Security Incident Response Platforms
Threat Intelligence Platforms
SOAR

SOAR = SOA + SIR + TIP

Open Standards — We Need to Get Behind This Folks

STIX™ Structured Threat Information eXpression

A Structured Language for Cyber Threat Intelligence Information

TAXII™ Trusted Automated eXchange of Indicator Information

Enabling Cyber Threat Information Exchange

CybOX™ Cyber Observable eXpression

A Structured Language for Cyber Observables

OpenIOC

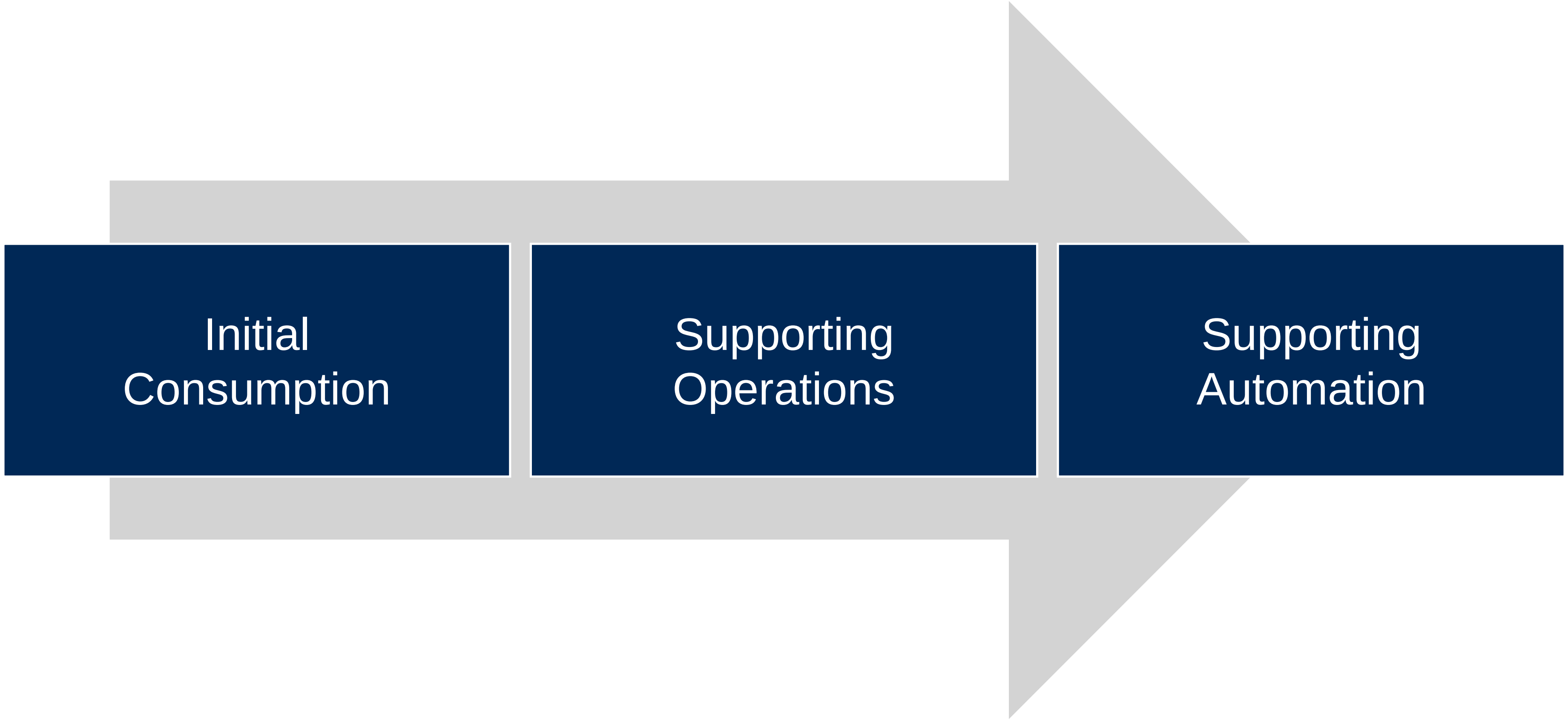
An Open Framework for Sharing Threat Intelligence

Sophisticated Threats Require Sophisticated Indicators

Key Issues

1. The State of the Threat Intelligence Market
2. The Gartner Maturity Model for Threat Intelligence
3. The Main Use Cases

Roadmap to TI Implementation Success



Initial Consumption

Supporting Operations

Supporting Automation

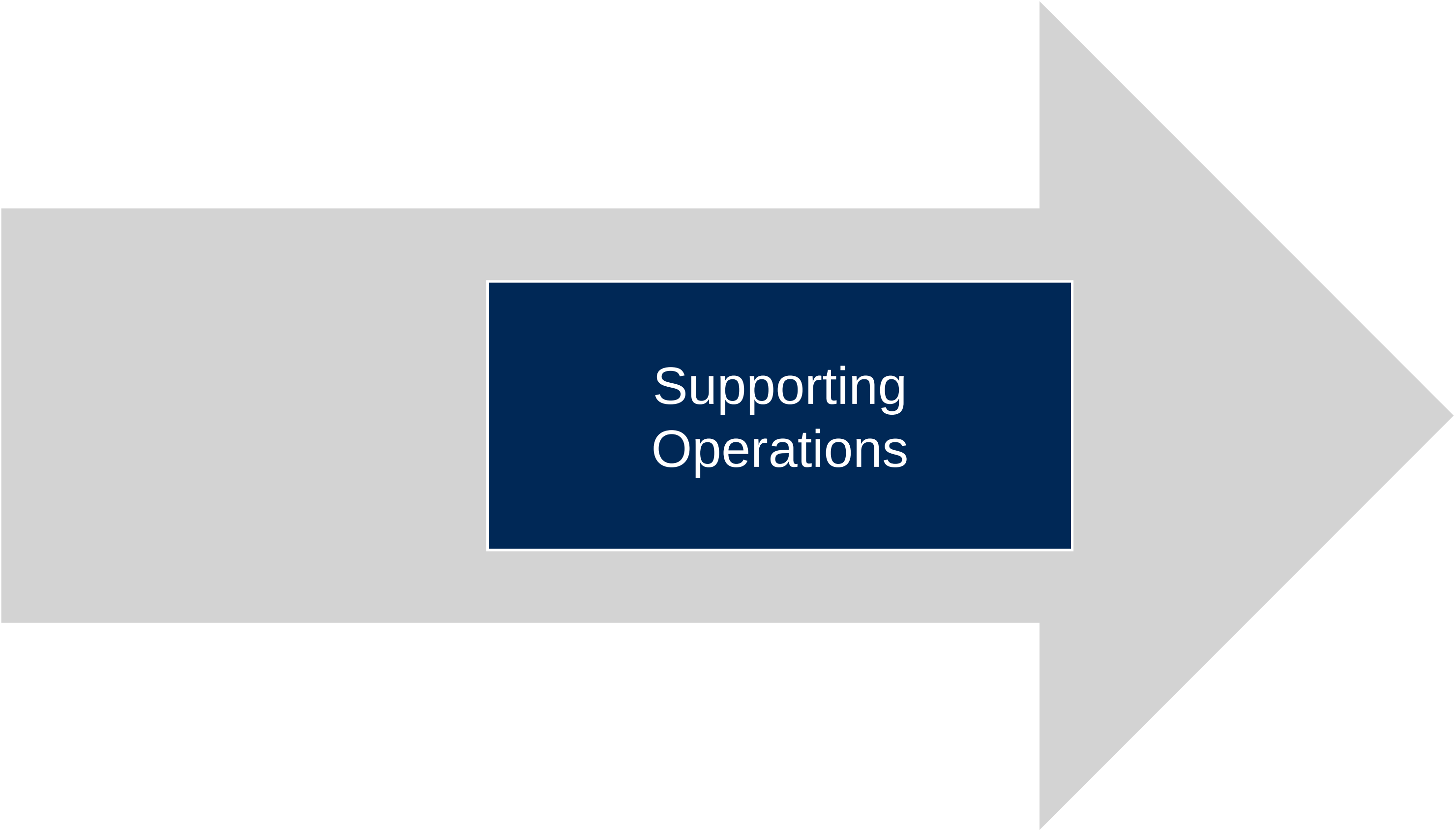
Source: “Use a Capability Matrix for a More Effective Threat Intelligence Program” (G00370099)

Start Consuming TI and Learn How to Deal With Alerts

Initial Consumption

Source: “Use a Capability Matrix for a More Effective Threat Intelligence Program” (G00370099)

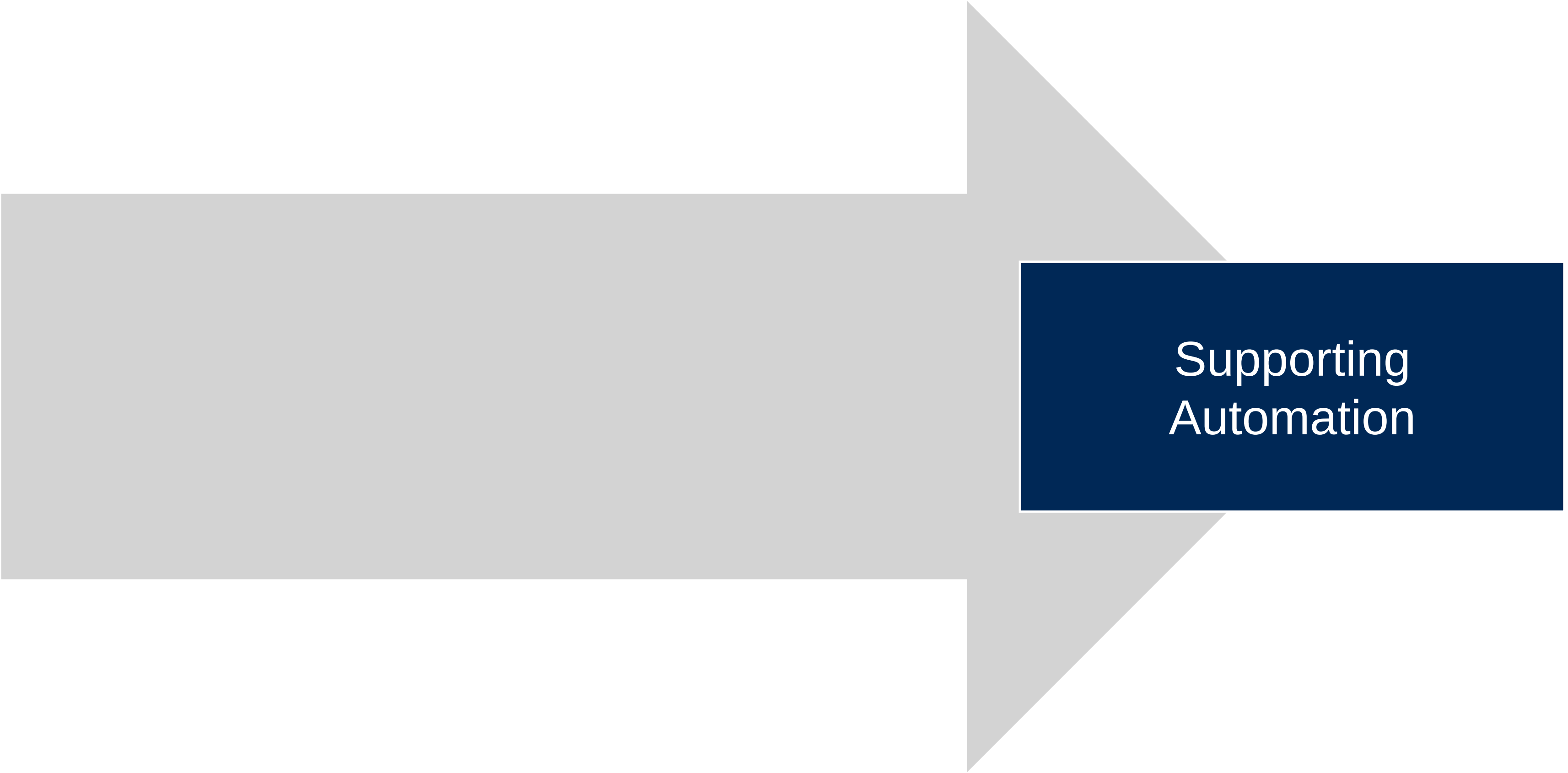
Mature Beyond the "Initial Consumption" Stage Supporting Security Operations



Supporting Operations

Source: "Use a Capability Matrix for a More Effective Threat Intelligence Program" (G00370099)

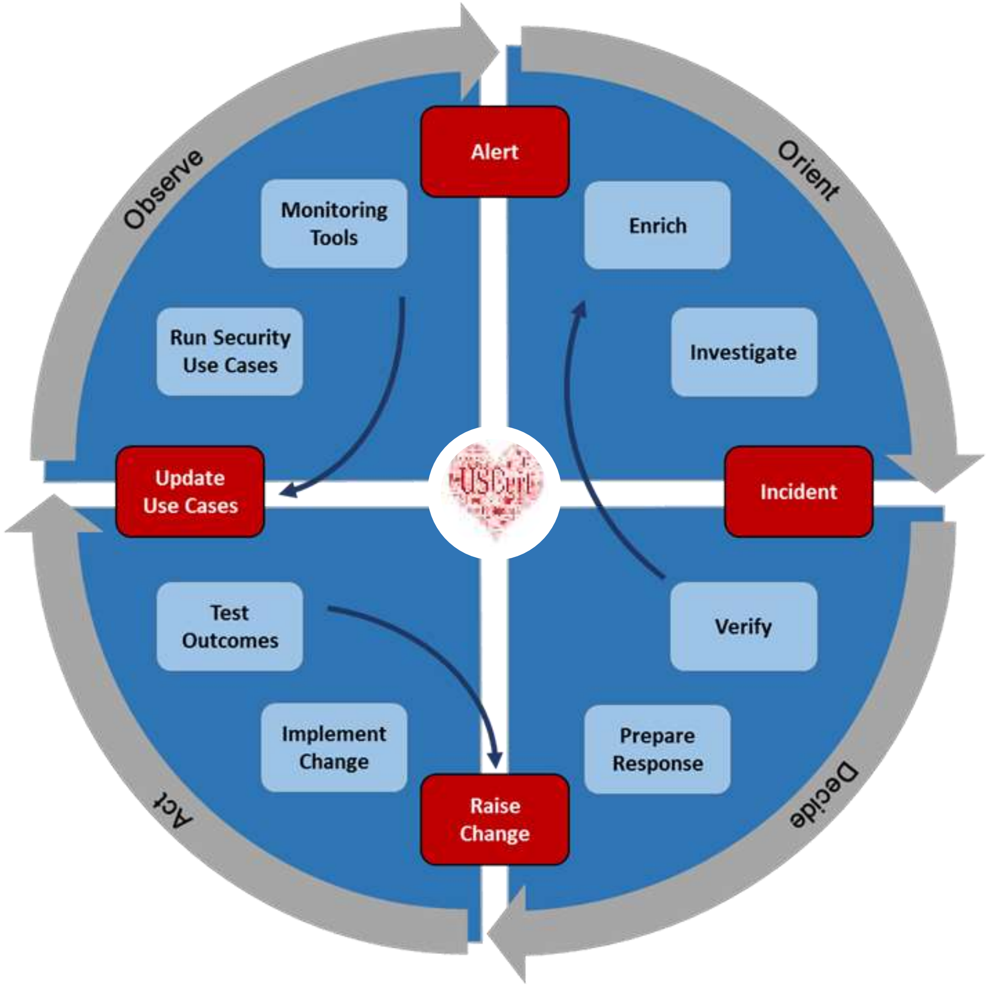
Improve Utilization of TI to Automate and Orchestrate Security Processes



Supporting Automation

Source: “Use a Capability Matrix for a More Effective Threat Intelligence Program” (G00370099)

Outcome: Leveraging TI Leads to Better Threat Models and Faster Response



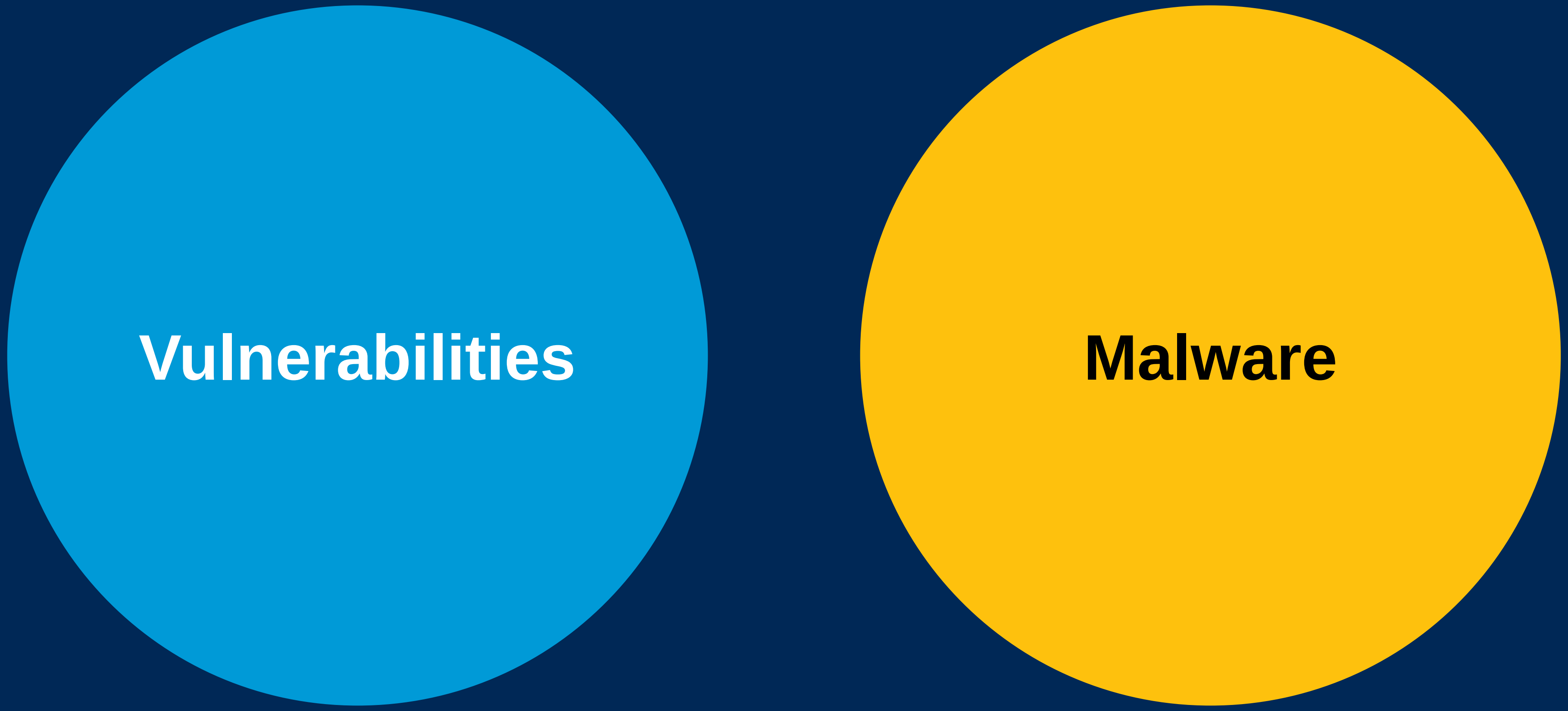
Key Issues

1. The State of the Threat Intelligence Market
2. The Gartner Maturity Model for Threat Intelligence
3. The Main Use Cases and Vendors

Use Cases — Vulnerability Intelligence

- Easily the most undervalued TI use case today
- Knowing which vulnerabilities you have that are being leveraged by attackers is incredibly valuable

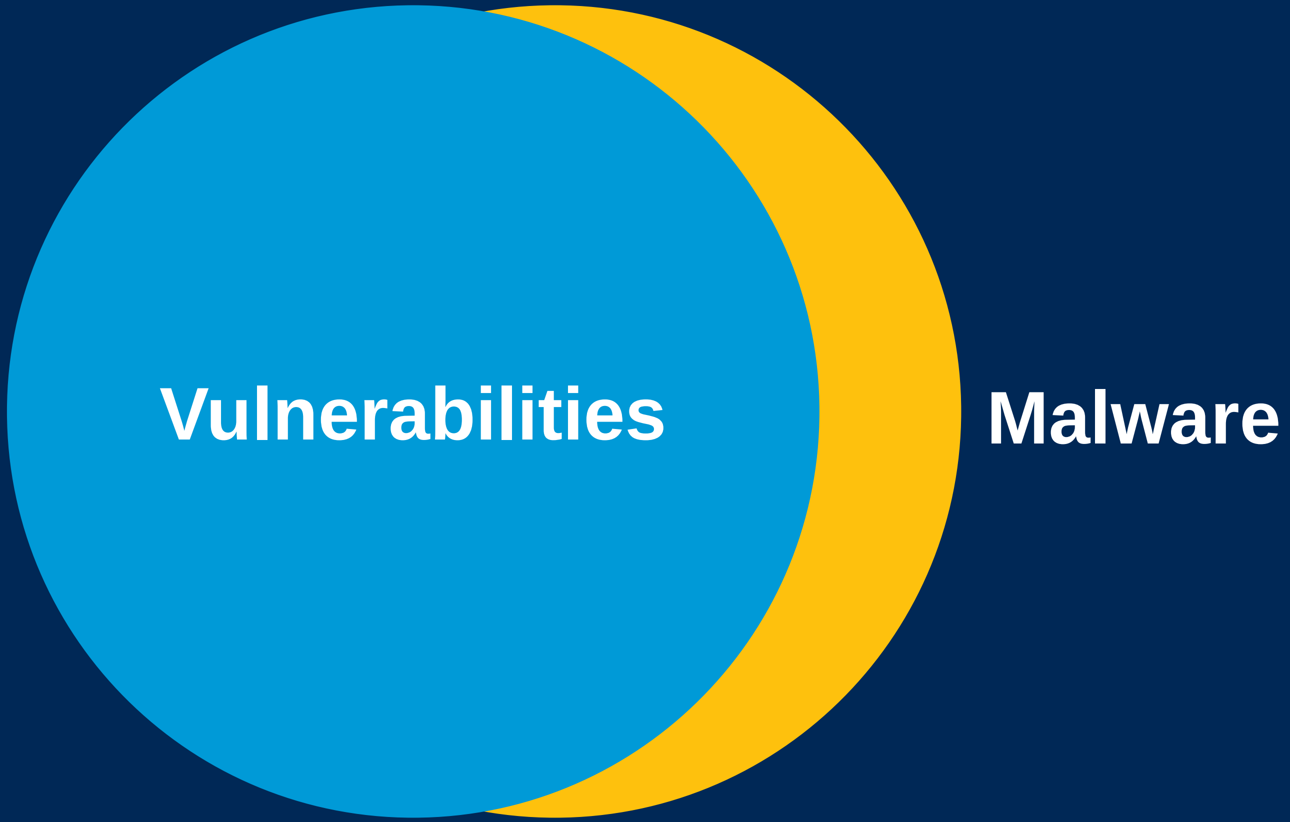
This Is How People Think the Threat Landscape Works



Vulnerabilities

Malware

This Is How It Actually Works



The Threat Landscape Ratio You Won’t Hear About

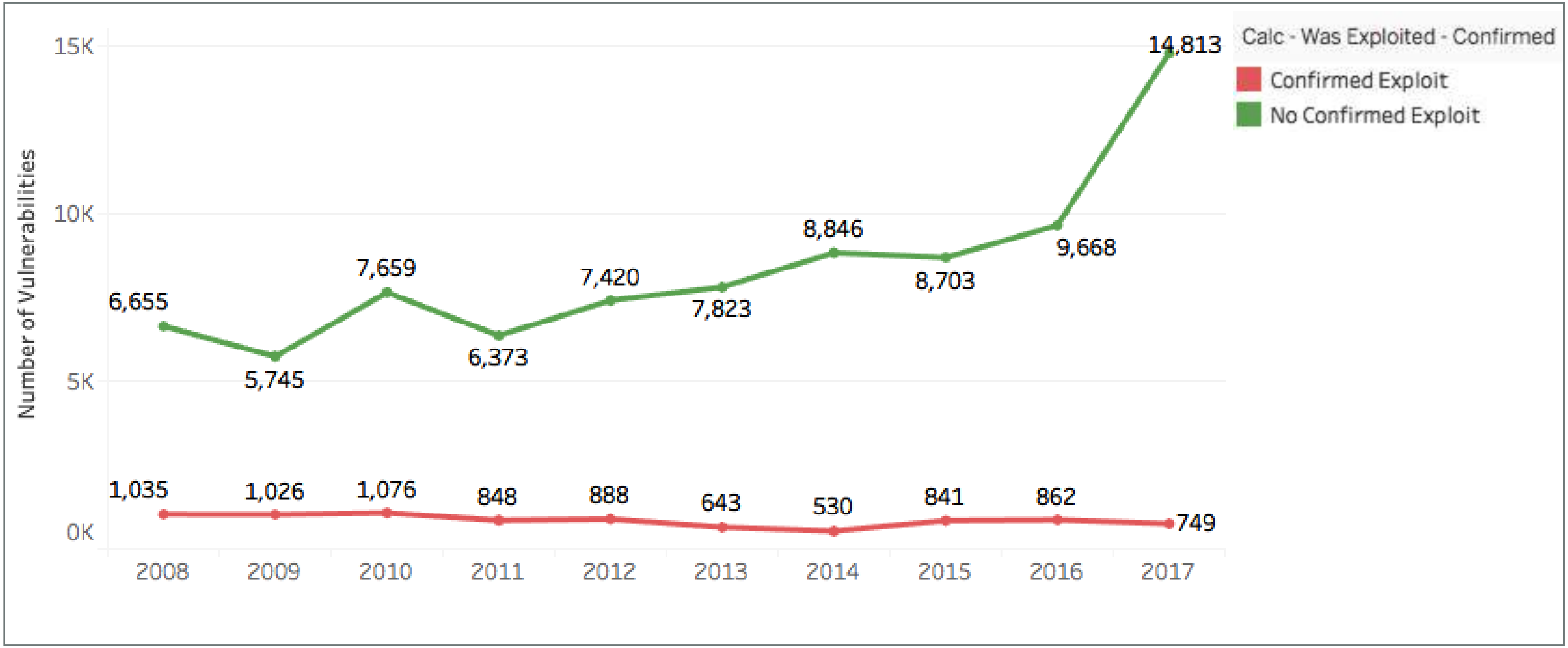
<vuln> : <malware families> : <malware samples>

1

10’s

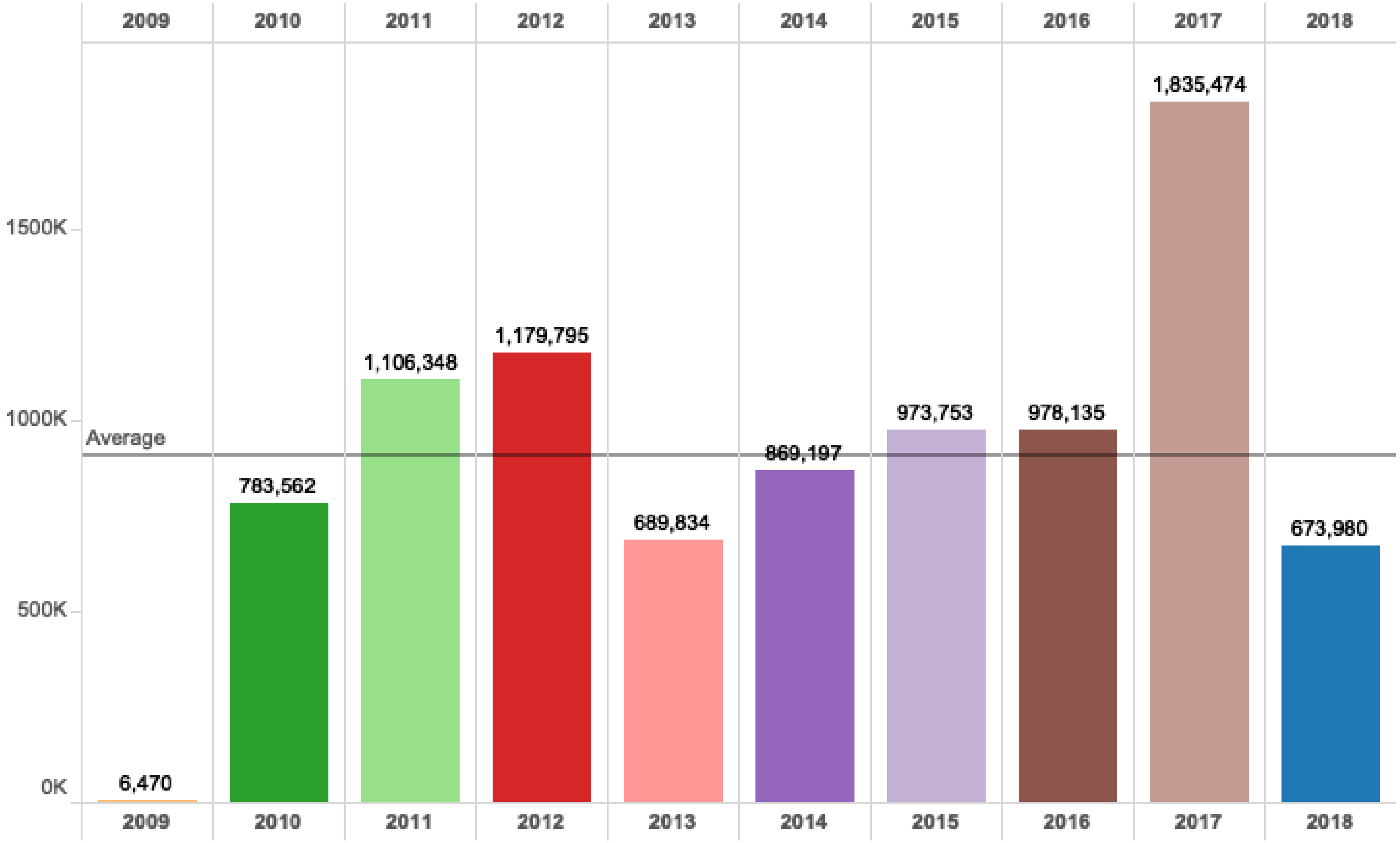
10’s of thousands

Here Is a Better View of Risk



Source: IBM X-Force Exchange
Analysis: Gartner Research

Malware Samples Per Day



Source: Symantec ISTR
Analysis: Gartner Research

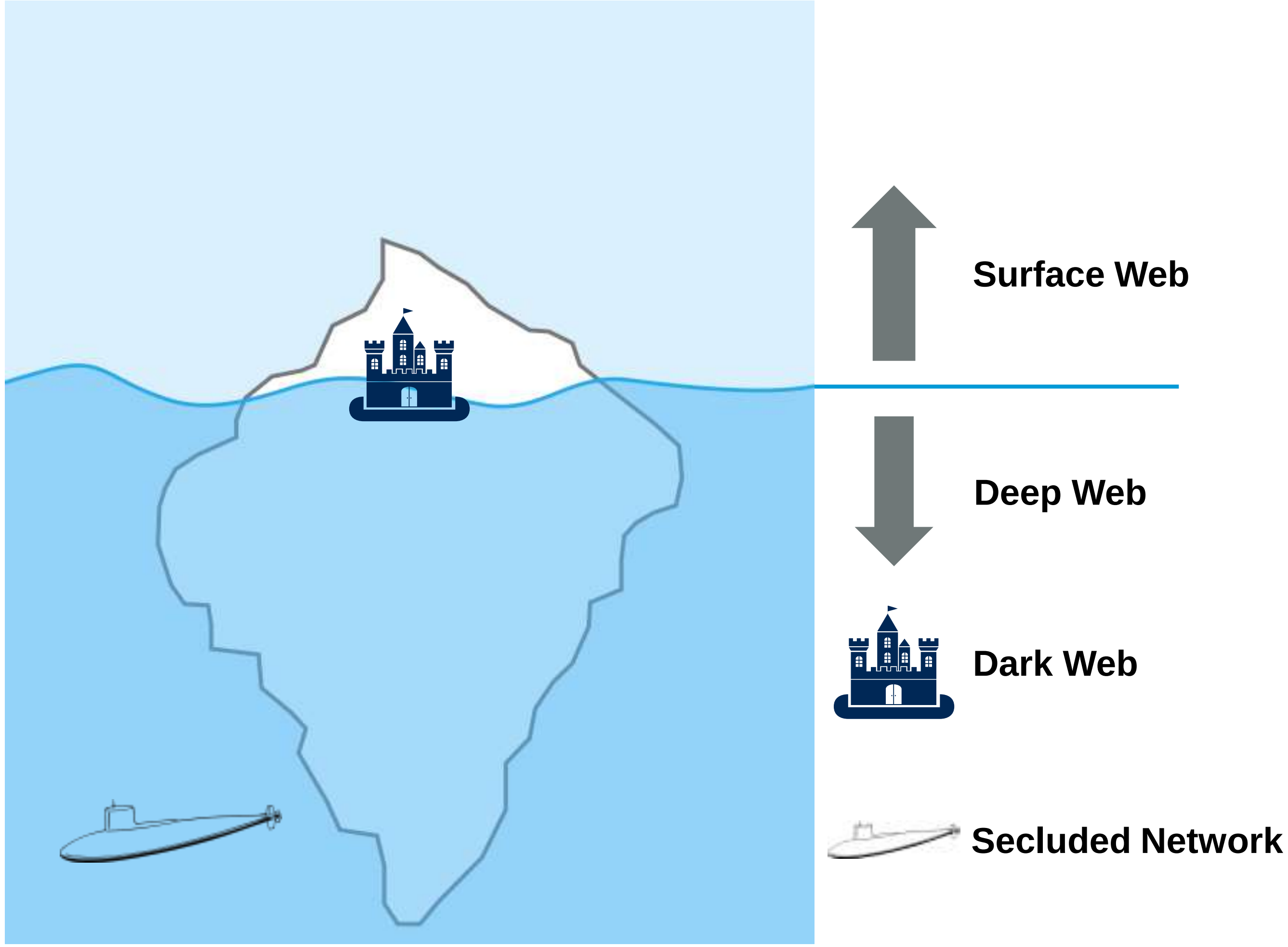
Use Cases — Phishing Response

- Very popular use case.
- Using TIP/SOAR to process suspect phishing email.
- Have MRTI/TI enrich and do a large amount of the heavy lifting in early-stage investigation of potentials. Check attachments by plugging into sandbox, lookup URLs and domain names, investigate hosters of the domain name of the emails
- This removes a huge time sink from the SOC.
- Tools can then start to quarantine future examples on your SEG, block phishing URL’s on your SWG/FW, block DNS resolution of C2 domains

Use Cases — Social Media Monitoring

- Social Media — it’s a jungle out there.
- Many new breaking threats are very often initially discussed here first, including the occasional 0day being dropped.
- Great way to start to piece together TTP’s, threat actors, threat actor interconnectedness.
- Phishing for example works really well from social media, so it’s a reliable attack path that is leveraged against your users:
  - Monitoring for things like fake profiles that are interacting with things like your company hashtag, LinkedIn profile, Facebook pages etc.

Deep and Dark Web Monitoring



Surface Web

Deep Web

Dark Web

Secluded Network

This capability is becoming very popular from TI providers and underpins multiple use cases described here today.

Deep and dark web are vastly different. Deep web has a low point of technical entry to it as its primarily just web crawling content.

Dark web needs a skill set that is both rare and nuanced and won’t be commoditized anytime soon.

The most challenging to uncover or monitor are secluded networks which are operated by well-funded groups or nation states.

Use Cases — Threat Modeling and Supply Chain

- Linking vulnerabilities to threats to probability
- External coming in view of your risk
- You might be okay, how’s that supply chain of yours though?
  - We see many organisations often have 100’s of suppliers
  - It is even larger if you were to map it to the second degree (suppliers of suppliers)
  - Who are these people? What do they do? How risky are they? Have they been breached and don’t know it?

Use Cases — Threat Indicator and IR

- Getting valuable “context” is key.
  - What else is known about this content:
    - Vulnerabilities
    - IoC’s — IP addresses, URL’s, file hashes, domain names, registry keys, AS numbers etc.
    - TTP (tactics, techniques and procedures)
- Mapping these all back to threat actors
- If you have better context, you can make better decisions, faster.
- Start pushing STIX/TAXII — we need more open standard adoption.

Use Cases — Fraud Detection

- This is big obviously in the financial services vertical
- Using TI to help figure out bad actors, transactions, phished users, stolen credentials that are being leveraged helps with this use case
- Following threats like banking trojans against your user base

Use Cases — Intellectual Property Protection

- Who wants my IP?
- How have they taken IP before?
- Has my IP leaked:
  - Simple metadata tagging example — embed all docs with a unique and innocuous text string that makes it easy to do regex at scale.
  - New services that can find stolen IP
- Are people offering a bounty of sorts to get my IP
- Who are the threat actors that target IP theft?

Use Cases — TI Analyst Augmentation

- To help or to be the TI analyst for your organisation, either full or part time
- Available on request, for certain specific investigations or as an ongoing service.
- 0% unemployment here as it's a nuanced skill and it takes years to get up to scratch
- Government is the leading feeder into commercial providers

Use Cases — Rogue or Fake Mobile App Detection

- Some “App” stores can be really problematic.
- Easy to fake an “app” in some app stores today.
- Users love the fact “there is an app for that.”
- Monitoring for apps that look like that of your brand or service

Use Cases — Threat Intelligence Sharing

- I’m a big fan for defending in a pack, rather than try to fight in isolation.
- Seeing ISAC’s being especially effective here.
- Great to see encouragement from government.
- There are lots of “TI fight clubs” that are facilitated by TIP’s.
- STIX/TAXII are good things here.
- Other standards like TLP (traffic light protocol) are also really helpful.

Use Cases — Powering New Technologies

- New technologies are built off the back of threat intelligence
  - TIP
  - SOAR
  - TVM
- Most new technologies with machine learning have blended in MRTI in there somewhere.

Recommendations

- If you want to get value from threat intelligence, start with how you'll "action" TI and your use cases first.
- Turn it on in the "stuff" you have first.
- Budget holistically and execute on concurrently being able to **acquire, aggregate** and **action** threat intelligence.
- You **must** to be able to do all three (acquire, aggregate and action) concurrently well to benefit from threat intelligence.

Action Plan

Monday Morning:

- *Review* the primary use cases detailed here and see whether these are issue’s in your organization.

Next 90 Days:

- *Review.*
- *Establish* a “your threat landscape” view of your organization.

Next 12 Months:

- *Stage* any investment in TI to make sure it’s adding incremental value. A big bang approach is likely to overwhelm you and increase the ROI time.

Recommended Gartner Research

- **Use a Capability Matrix for a More Effective Threat Intelligence Program**
  Ruggero Contu, Craig Lawson and Ryan Benson (G00370099)
- **How Gartner Defines Threat Intelligence**
  Rob McMillan (G00299526)

For information, please contact your Gartner representative.