CASE STUDY

What Elite Threat Hunters see, that others can't.

Organizations are turning to **Team Cymru** to get ahead of high criticality cyber threats.

We spoke with a multinational corporation with several business units that employs threat reconnaissance to improve security. This walkthrough will illustrate the value of employing analysts in more strategic ways to optimize the incident response process, as well as improve prevention and detection.

Their analyst teams are taking threat hunting to the next level by employing true threat reconnaissance against high priority, and typically the most stubborn, threat actors. After all, threat actors conduct reconnaissance on their targets' infrastructures. It's time to turn the tables and conduct recon on them.

So, What is Threat Reconnaissance?

The purpose of threat reconnaissance is to gain visibility far beyond your perimeter to trace threats to their origin and map out the extended infrastructures. This allows you to watch threat actors at work, monitor their infrastructures as they evolve, and trace lines between them and their victims.

The objective is to give you the best chance of, not just surviving, but defeating cyber-attacks even before they start. Adding a threat recon program to your security practice allows you to manage risks or deal with active threats more effectively and move the needle of cyber resilience from reactive to proactive.

Many cyber security veterans may not recognize threat reconnaissance as an option for them, as the activity conjures thoughts of intelligence agencies and military. For many, reconnaissance is simply part of the cyber kill chain – something bad actors to do good organizations. The idea that good organizations can have the ability to conduct recon on the bad actors is only recently surfacing among the most risk averse enterprises. However, it is threat hunting as it should be.

Threat Hunting Maturity Model

Wanted: **Elite Analyst Teams**

Gain longer lasting network defense benefits as your team unlocks more advanced capabilities.

THREAT INTELLIGENCE

Traditional threat intelligence is curated and usually dated. Due to its fragmented nature, analysts must juggle a variety of sources to flesh out a more complete picture. Many companies prioritize using it to enrich automated prevention and detection.

THREAT HUNTING

Typical teams use intel to identify threats on their networks that security tools have missed. They are limited by lack of visibility into unknowns beyond the firewall. This approach is just threat detection with little proactive benefit.

THREAT RECONNAISSANCE

At this stage, analysts can use seeds of intel to expose previously unknown threat infrastructure, wherever it exists globally. Watching threat actors as they work allows organizations to defend against them indefinitely.

The idea that good organizations can have the ability to conduct recon on the bad actors is only recently surfacing among the most risk averse enterprises.

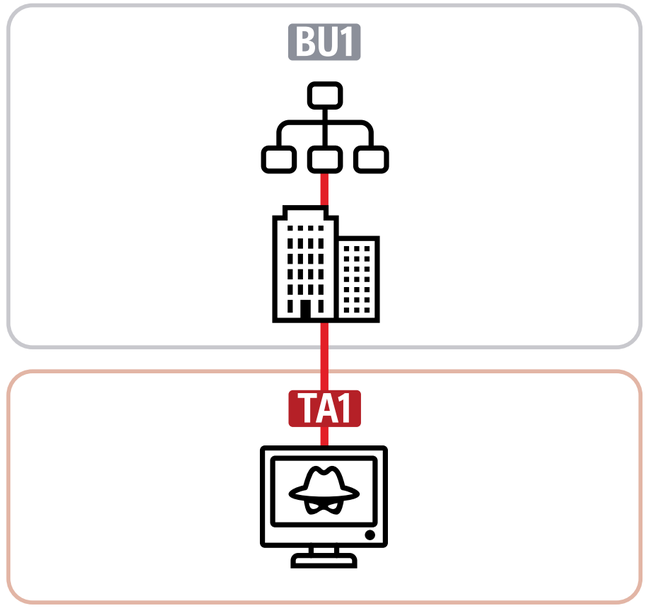
TEAM CYMRU™

DISCOVERY 1

Faster Root Cause Analysis and Illuminating Shadow IT

Of the four main business units, each with their own distinct networks and Internet access, **Business Unit 1 (BU1)** was discovered to have been compromised. Using global Internet traffic telemetry available via **Team Cymru's Pure Signal™ Recon,** the team was able to wind the clock back to the time when the breach took place and identify the source; **Threat Actor 1 (TA1).**

What made this discovery compelling was it revealed an unknown part of infrastructure that was being targeted. At the time, there were no indicators of compromise from sensors, endpoints, alerts or incidents reported. The ability to trace the threat, looking at their attack surface from the threat actor's perspective, identified their own security weaknesses and improved their ability to remediate follow on attacks.



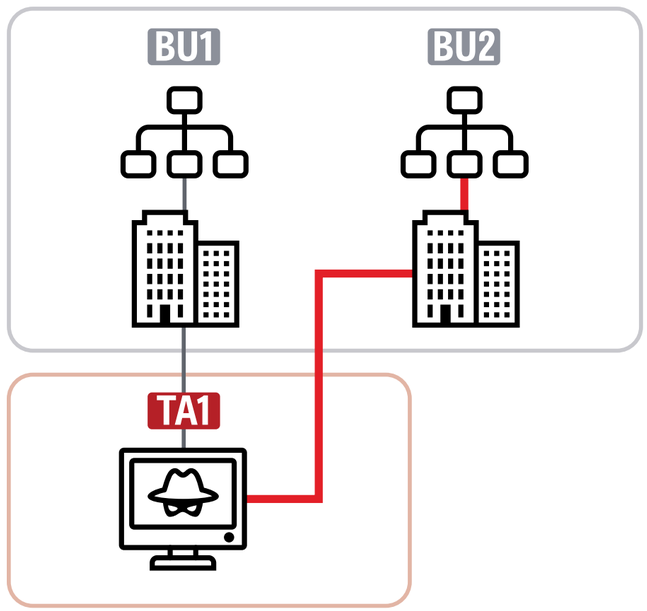
DISCOVERY 2

Incident Recurrence Prevented

Pivoting off existing data fragments or evidence is a key upside for threat hunters employing reconnaissance methodologies. This is where recon begins. They now have a seed they can use to trace this threat actor.

Once **TA1** had been discovered, it was then possible to watch them work on other victims.

During observation of **TA1** the team saw that **BU2** was being actively targeted, as well. This threat could then be monitored more closely to prevent recurrence. Further, they were able to confirm that **TA1** was targeting them specifically, allowing further prioritization of their network defense efforts.



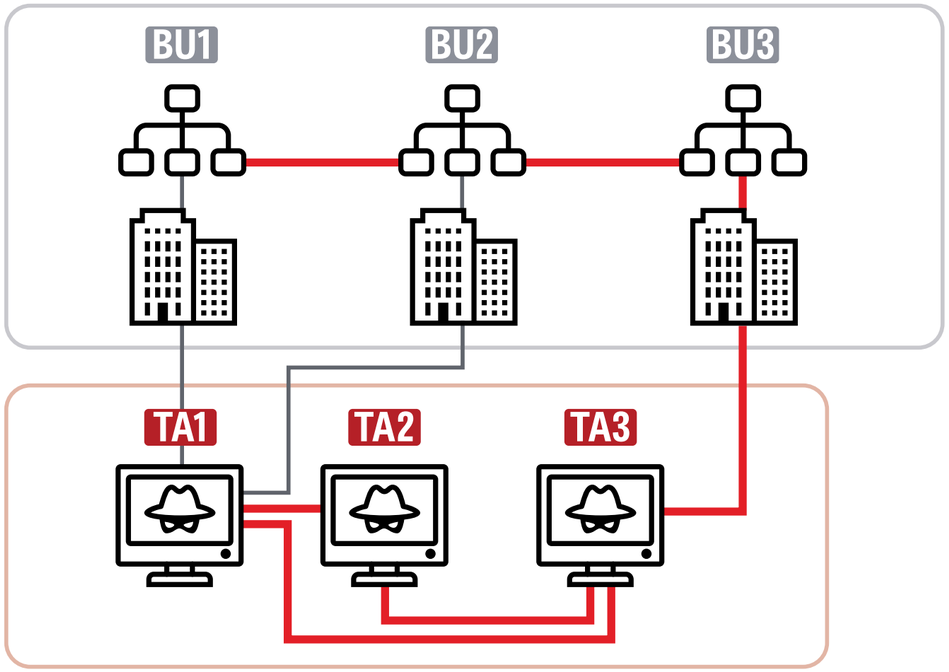
DISCOVERY 3

Blocking Attacks Before They're Launched

An IP address was doing targeted scanning of BU3 infrastructure. Observing activity around this IP address, the client was able to attribute the scanning to a new threat actor **(TA2)**, it was then that a connection was identified between **TA2** and **TA1**.

Due to Team Cymru providing Internet-scale visibility, the details of this connection allowed mapping to all the threat actor infrastructure. During the course of this mapping process, the client made another discovery: a third threat actor **(TA3)**. It became clear through further observation that these individual threat actors were working together.

The client was able to block the extended infrastructure of these individual, but cooperating, threat actors and monitor for changes to defend themselves in the long term.

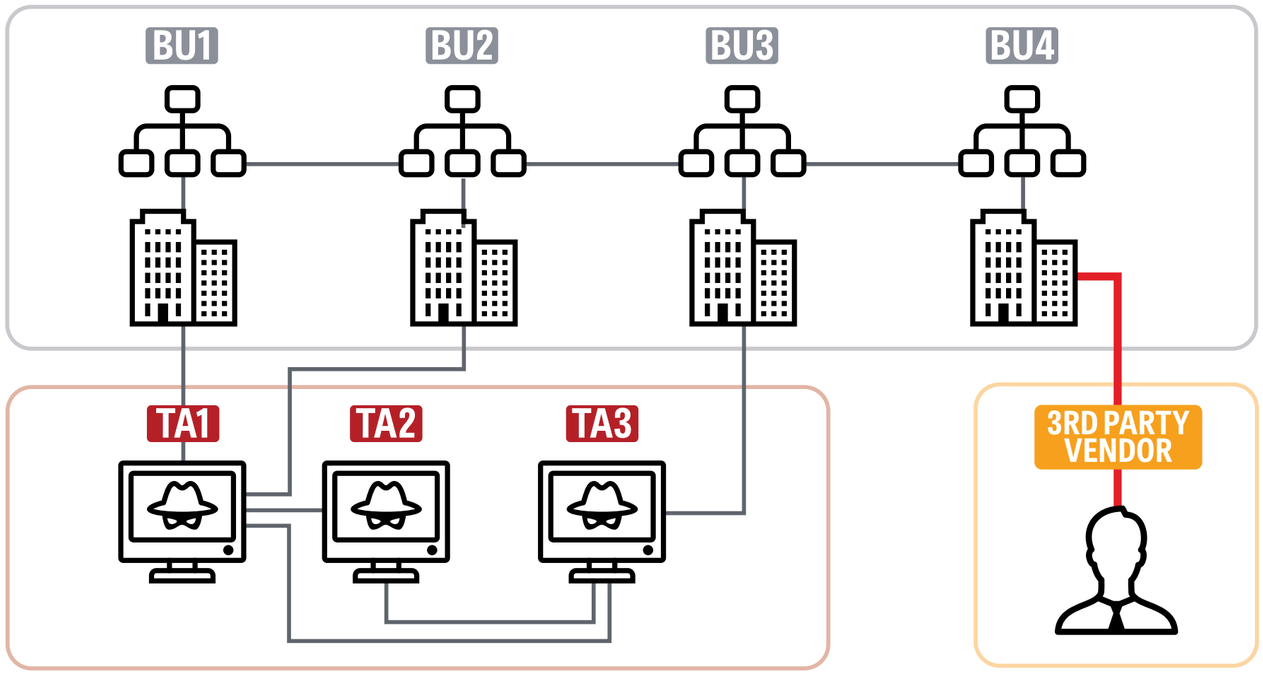


DISCOVERY 4

Fast Alert Triage

Very suspicious scanning activity of **BU4** triggered a full incident response process.

During investigation, our customer quickly traced this activity back to a supply chain vendor. The CISO from the vendor confirmed this was a **Red Team exercise** straying out of scope and beyond their own borders. The ability to quickly trace a potential threat back to its origin allowed the IR team to validate the false positive, saving wasted time and resources. With help from the analyst team, the incident response team avoided business disruption and kept its reputation intact among senior stakeholders for sounding a false alarm.

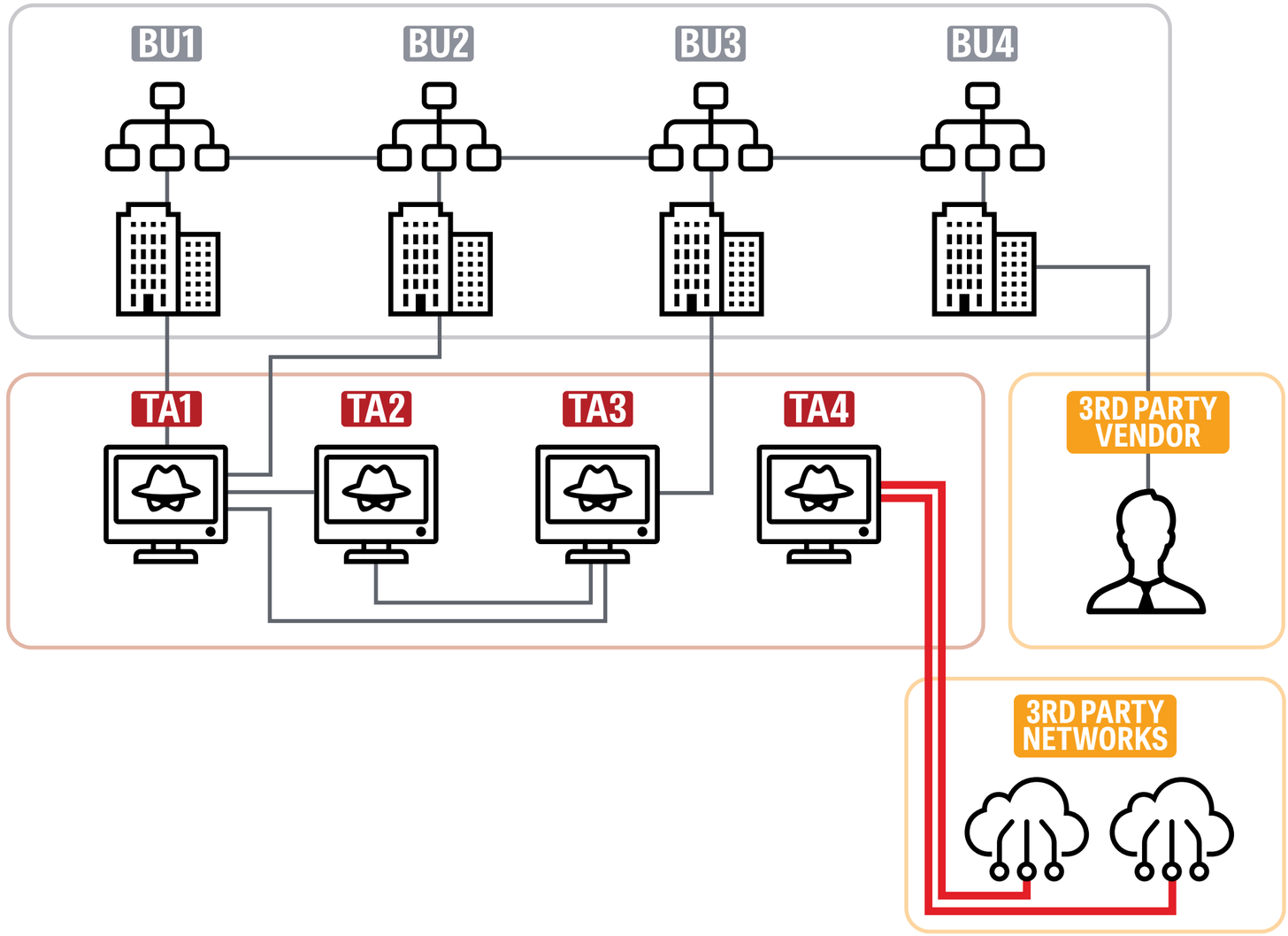


DISCOVERY 5

Identifying Impending Attacks

This is a great example of using reconnaissance to gain far-off visibility into attacks beyond the network perimeter, in order to dodge bullets or brace for impact.

A threat **(TA4)** was observed targeting multiple other third parties in the same industry as our client. This enabled the client to observe the threat and extract tangible insights to prepare defenses and mitigate the impending attack before any attempts by the threat actor could be made.

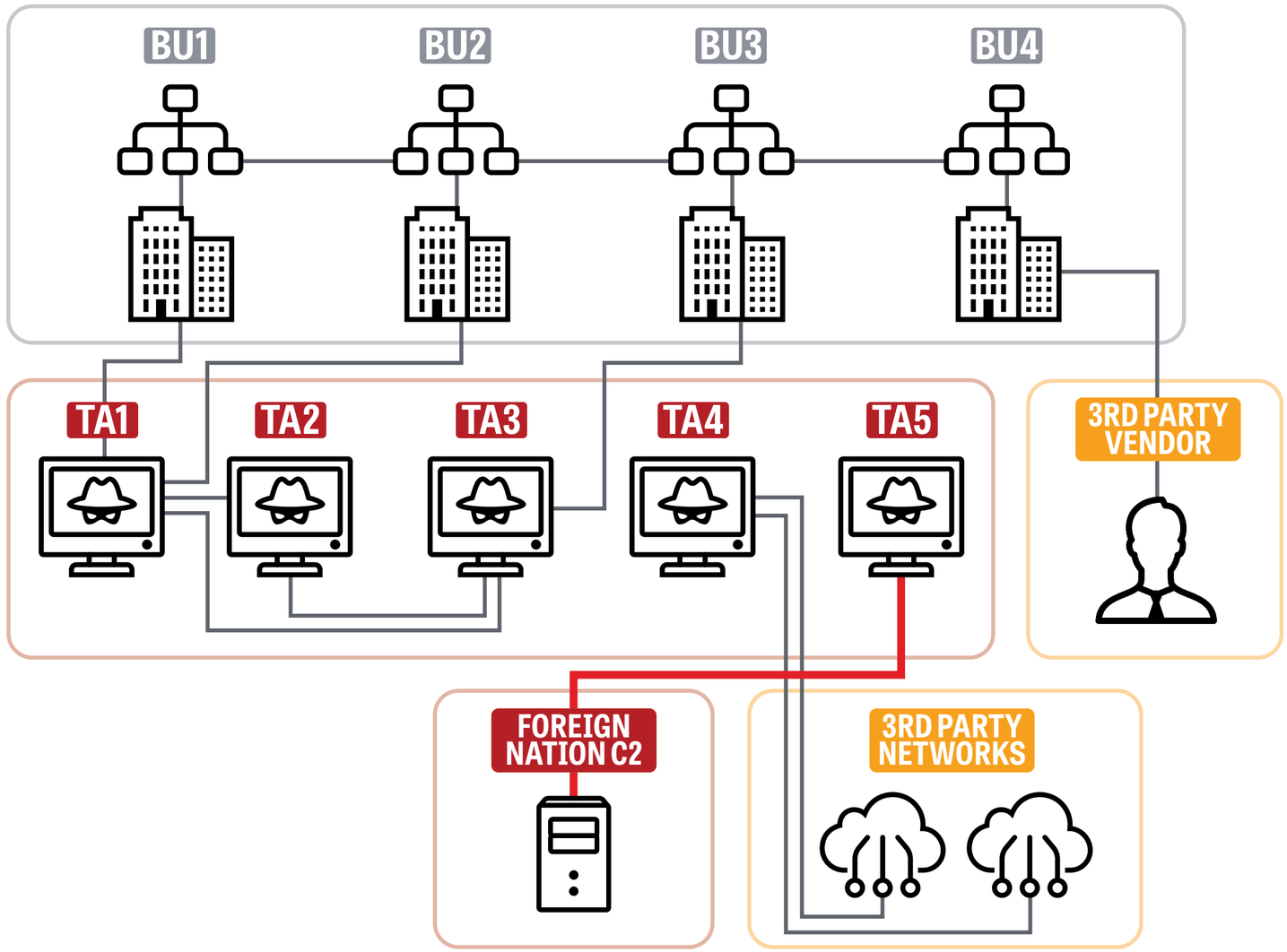


DISCOVERY 6

Enriching Threat Detection Tools

By looking at global Internet traffic, a node outside the organization that was compromised by a new threat actor **(TA5)** was seen calling out to a foreign-nation-hosted command and control **(C2)** server that was identified by other sources.

At this point in time, antivirus and other threat intelligence vendors were not sharing details on this activity. The correlation of **TA5** infrastructure with a specific strain of malware was only discovered using **Team Cymru's Pure Signal™ Recon.** This enabled active monitoring for specific signatures, creating a swift response mechanism should the malware be directed towards the corporate network.



TEAM CYMRU™

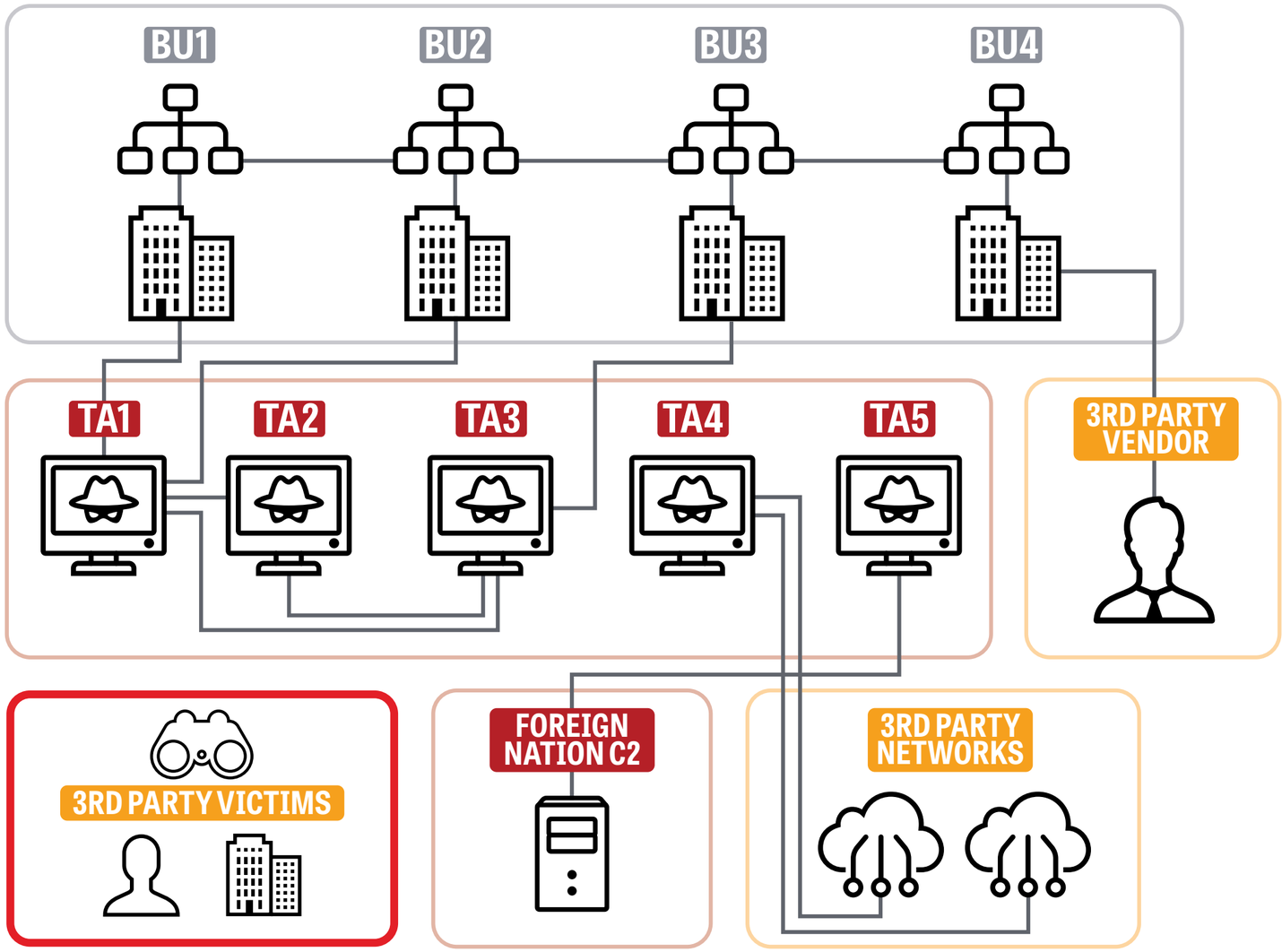
DISCOVERY 7

Protecting Supply Chain and Customers

Threat hunters employing threat recon beyond their own perimeter will often observe attacks and map the associated infrastructure, as described in **Discovery 5** whilst researching risks that relate to their own organization.

Our client uses this method to gain a more comprehensive understanding of their own threat landscape and compile a list of suspects that might threaten their supply chain and customers.

This team found many unrelated third-party victims, as well as victims within their circle of trusted business partners. Each victim identified provides a new pivot point that can be used to illuminate more **C2**s, and it allows them to detect victims among their subscribers globally.



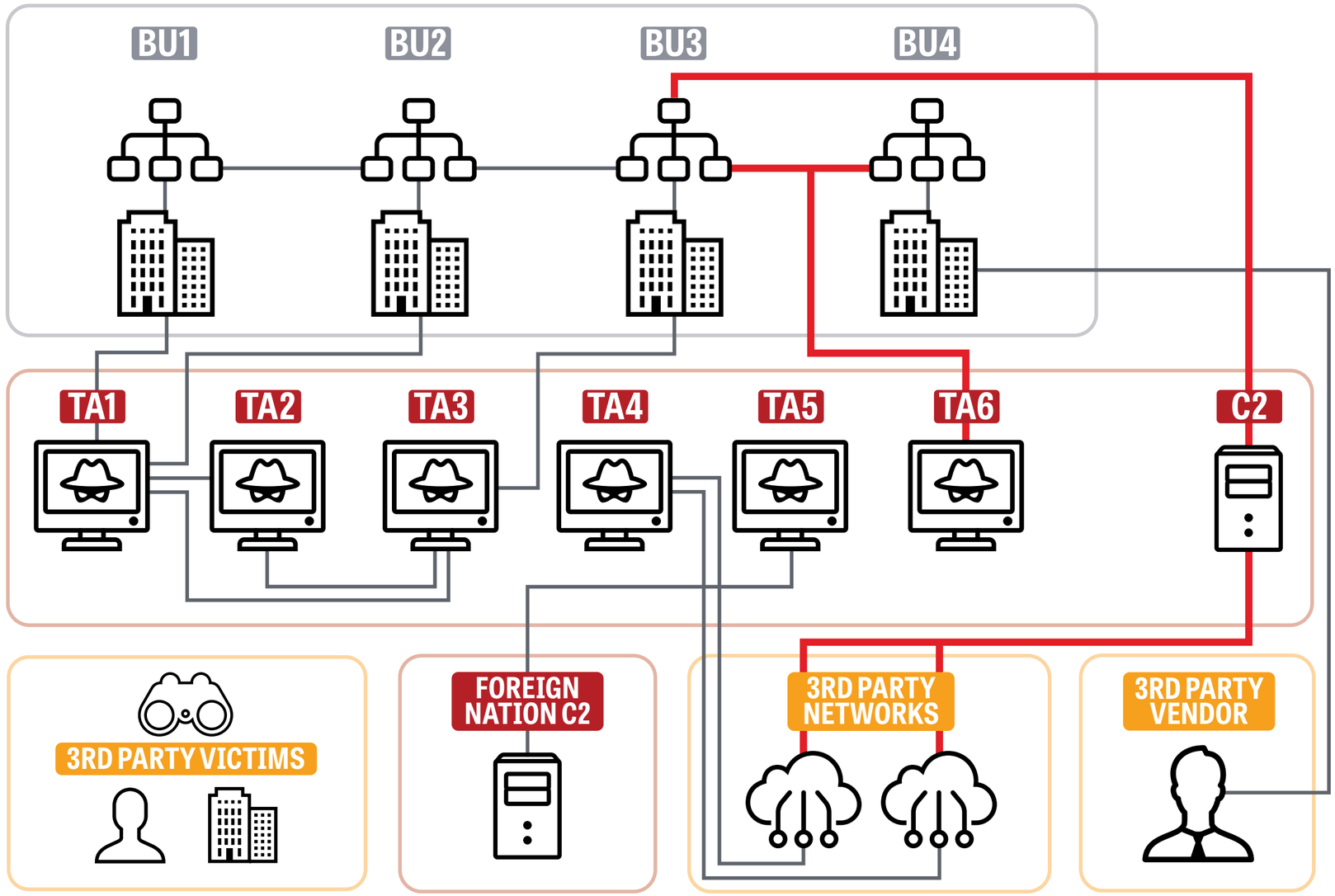
DISCOVERY 8

Gaining an Industry-wide Perspective

Monitoring threats that are impacting your industry peers provides ground-truth understanding of your threat landscape and what to do next.

It exposes additional indicators of compromise our customer can proactively search for within their own network. In this case, by observing peer activity, a **C2** was discovered beaconing out from our customer's internal networks. This provided another win, detecting a stealthy attack that slipped past traditional threat detection solutions.

At **Team Cymru** we see our customers sharing these discoveries with industry peers to great effect. It elevates a whole sector's ability to collaboratively defend itself through information sharing.



TEAM CYMRU™

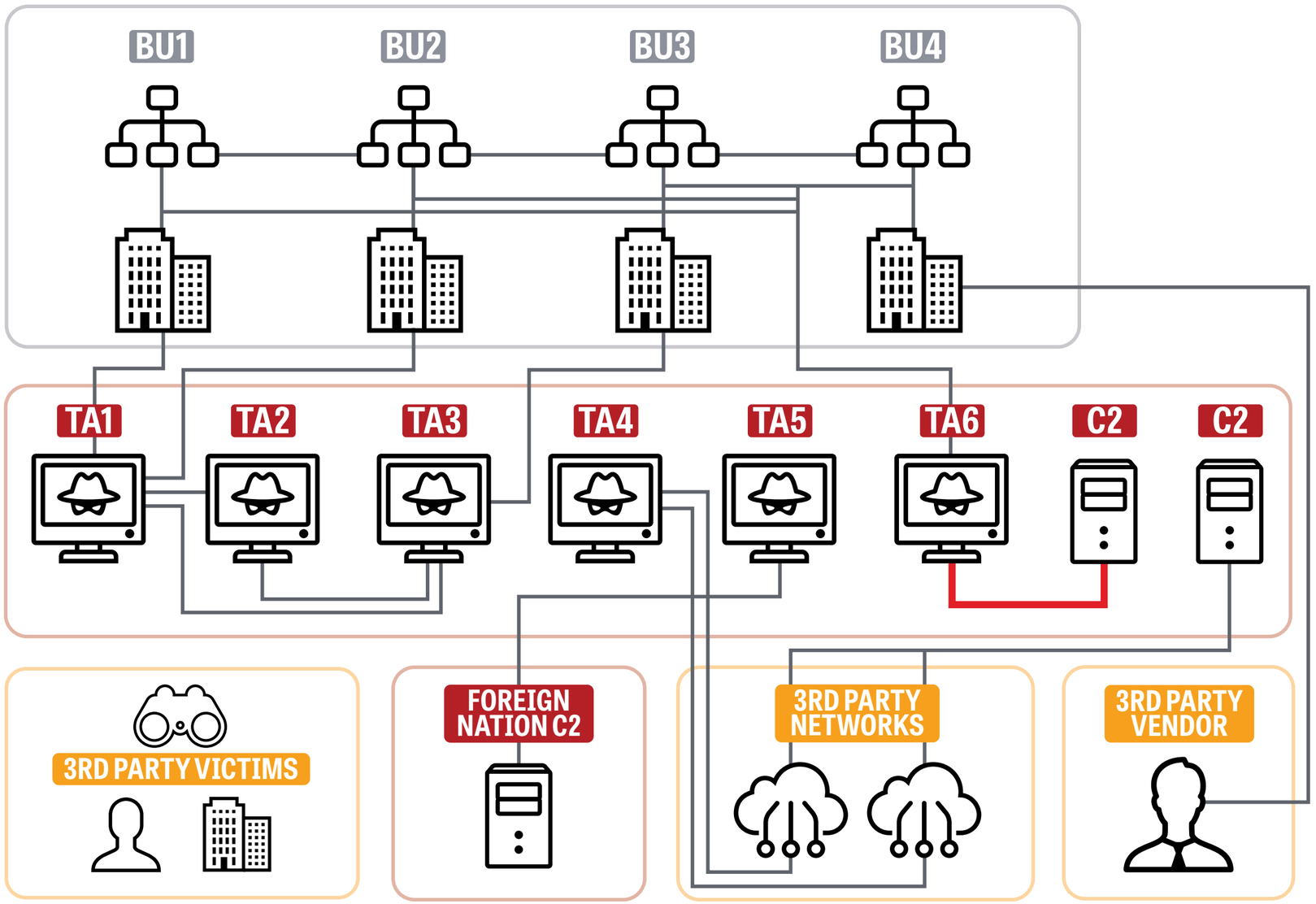
DISCOVERY 9

Closing Detection Gaps

With visibility into new **C2**s on the Internet, connections from **TA6** were discovered.

By tracing these connections, it was clear to our customer **TA6** were operating in their infrastructure without any security alerting or mitigation service being triggered. Fortunately, **TA6** malware payloads had not yet started communications to the **C2.**

With this clear signal of an in-progress attack, our customer added this **C2** to their IOCs list, and averted disaster before the actual attack was executed.



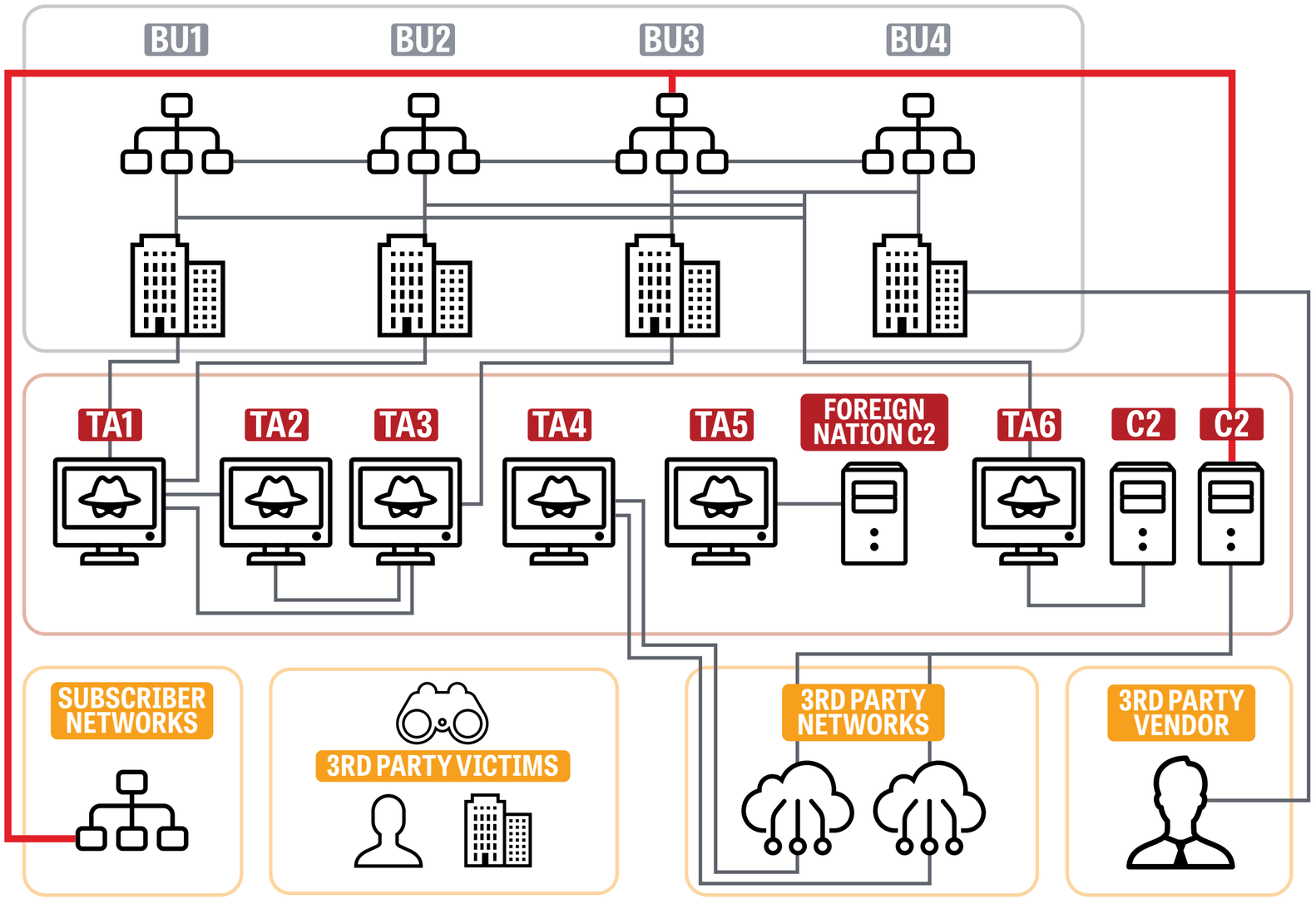
DISCOVERY 10

Fast Path to Longer Lasting Risk Reduction Outcomes

By leveraging public OSINT reports and **Pure Signal™ Recon,** our customer found **C2** communication to **BU3** infrastructure.

Tracing and mapping more of the **C2** infrastructure with **Pure Signal™ Recon,** it was concluded that some of the **BU3** infrastructure was part of **BU3** subscriber networks, creating a problem similar to shadow IT but on a much larger scale.

This exposed potential risks where network segregation was needed to further divide operational and customer networks to ensure risks were reduced for the business as a whole.



Not a conclusion

As the above storyboard shows, the life of an elite threat hunter is a constant process of discovery, analysis, attribution, assessment and action. Where a traditional threat hunting journey ends — usually at the first proxy — the path illuminated by **Pure Signal™ Recon** continues, pointing to threat actors and their infrastructure, their targets, and also their victims.

The difference can be likened to reading a printed paper report versus placing oneself into an immersive virtual reality world, observing the ebb and flow of global network traffic that is the Internet, the malicious activities taking place, and how everything is connected — but always knowing where you are — at the center of it all.

CONTACT US
tel: +1 847-378-3300
fax: +1 407-878-7833
sales@cymru.com

EMERGENCY CONTACT
+1 847-378-3301
support@cymru.com