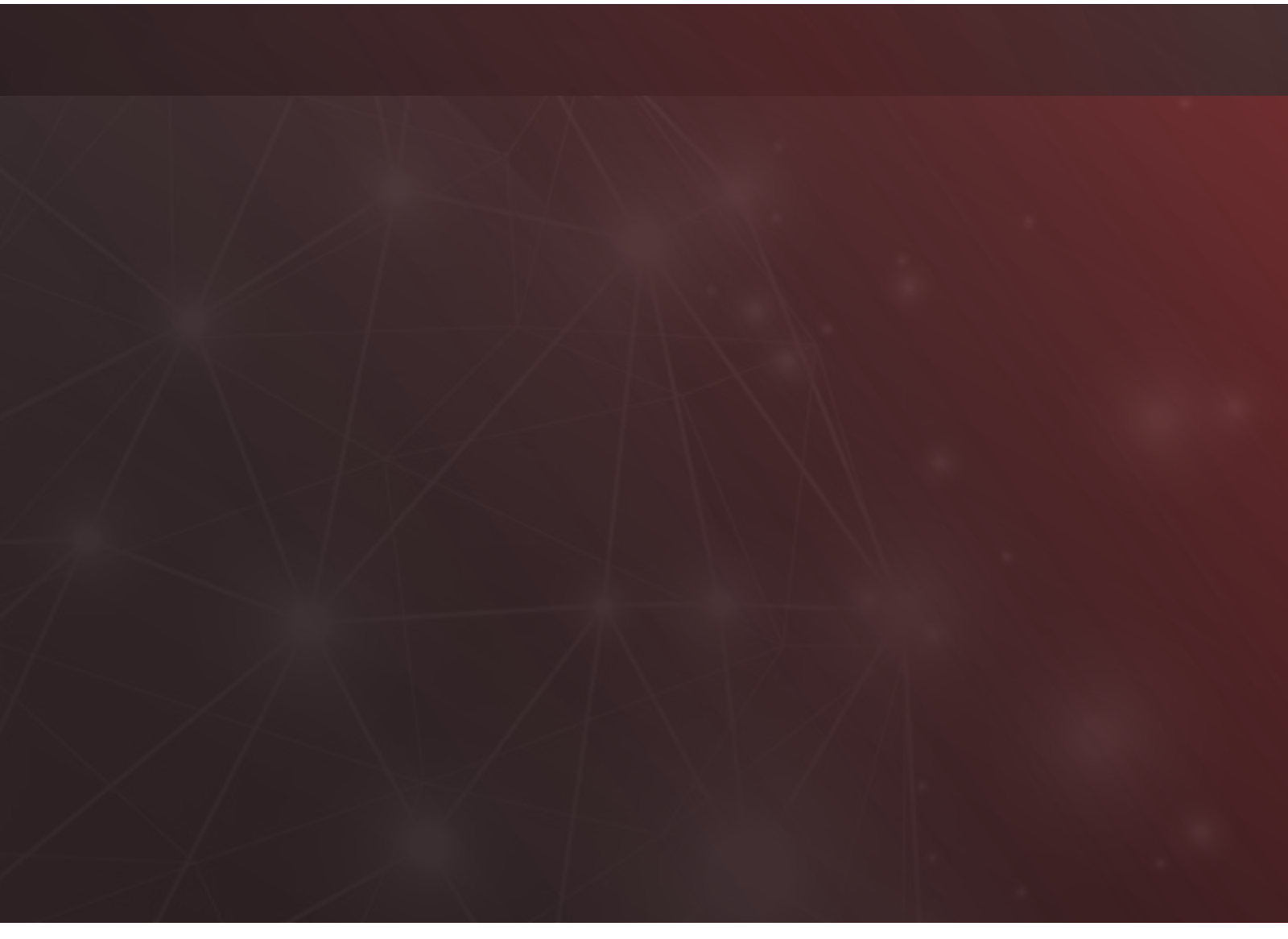
EBOOK

Pure Signal™ Recon

Threat Investigations at a leading UK Bank Paves the Way Toward Proactive Cyber Defence

Pure Signal™ Recon Empowers Threat Analysts to Prevent Data Breaches, Supply Chain Compromises, and Defend against Repeat Attackers



TEAM CYMRU™
THE POWER OF PURE SIGNAL™

The Vicious Circle From Lack of Visibility

> "We found great utility in being able to pre-emptively stop an attack with visibility into changes that threat actors were making to their infrastructure in an effort to attack us again."

If you are a security leader looking to take a more proactive stance against defending your organisation, and want to achieve the same outcomes, keep reading.

Are bad actors continually targeting your company? Do they retool and stand-up new infrastructure in their never-ending pursuit to gain access to your critical systems? Are supply chain and business partners also on the receiving end of these nefarious actors and their targeted attacks?

If this sounds all too familiar, then it is very possible you work for an organisation that must defend against stubborn bad actors that are always probing for a way in, and you are looking for a more proactive approach to stop them. One that provides better visibility into the external telemetry of malicious communications that impacts your perimeter as well as your business partners.

We had a chance to sit down with a leading UK retail banking organization to talk about how they took a proactive approach to defending their infrastructure against sophisticated adversaries. They shared with us how they use Pure Signal™ Recon to develop specific intelligence into patterns, tactics, techniques, and changes in adversary infrastructure. It also helped them develop a view into their business partners' infrastructure and were able to pinpoint suspect activity, even before their peers or partners knew about the potential for compromise.

Sharing Threat Intelligence and Peer Collaboration is Vital to Cybersecurity in the Financial Sector

The Cyber Threat Intelligence Manager has multiple analysts in his group. They take a proactive approach to threat intelligence to help the company keep ahead of a growing list of adversaries. For example, they pass both internal and external intelligence about adversaries to Incident Response (IR) teams and other groups so they can use that knowledge to update their block lists. The team looks for specific patterns, tracks changes in techniques and tactics by threat actors, and provides that information to other parts of the security organisation. Collectively, their efforts allow the bank as well as peers and partners to benefit from real-time threat intelligence to defend their environment.

When we spoke, he gave the following example to highlight why sharing threat intelligence is an important part of a Security Operations Centre (SOC). Ensuring continuity of services that banking customers depend on has equal importance to security. When one of the banks' foreign exchange

partners were hit with a Ransomware attack, the effects were two-fold. “First, we were losing an important service that we rely on, and customer experience was definitely affected.

“But the more worrisome implication was the issue of contagion.” When asked for further details, he elaborated by talking about some of his concerns.

“Are they going to be sending us emails with malicious attachments?”

“How far did the actor go into their infrastructure and then what kind of direct connections, like API connections do we have that might have privileged access to our bank systems?”

One of the things he pointed out was some of the more worrying things that can happen in a supply chain attack. “The worst part when thinking about supply chain security is the software supply chain compromise which is just a horror show, and when you look at all the news that comes out every day, it's turning into more of a horror show by the moment.”

He talked about how these concerns weighed on his Threat Intelligence Team as they did everything possible to protect themselves from malicious activity that came from an attack on the partner

Benefits of External Visibility of Telemetry: It’s the Real-Time Threat Intelligence that Analysts Need

It was clear that the team needed to operate with better visibility into adversary infrastructure, C2 communications, and how and where business partners may be affected when compromised. The team knew they didn’t want more of what they already had; curated news, reports from a month ago, and scanning that only tells half the story. He explained that as a threat intelligence organisation, they wanted insight into the external factors that put their business at risk. Regardless of the overlap in information, every financial institution subscribes to multiple threat intelligence feeds and curated intelligence about threat actors. That’s always good foundational knowledge but how does it help a threat intelligence organisation in the moment, when it matters the most?

Those were some of the top-of-mind questions we discussed, as well as their criteria to investigate a better way to solve their challenges. He explained by saying, “Any new solution would need to give them better visibility into business partner infrastructure, adversary movements, and what was happening in the moment.” Was this even possible? Not everyone in the threat intelligence group knew about Team Cymru and the unique capabilities that access to global internet telemetry could offer a threat intelligence organisation. After all, most threat intelligence offerings do not offer a way to see what is going on external to your perimeter, in a similar way you might view your internal networks.

The Threat Intelligence Team was more familiar with the usual curated and dated information that aids in baseline knowledge. But they already knew it wasn’t what they needed to get ahead of potential attacks and prevent them from happening in the first place.

Fortunately, the manager of the threat intelligence group knew of Team Cymru. He felt confident that the origination of real-time telemetry that Pure Signal™ Recon provides would identify adversary infrastructure and help them stay ahead of attackers. He told us more about how he learned about us. “I had a friend that knew about Team Cymru, we had discussions about it previously and it sounded interesting. So, when we had the opportunity to trial Pure Signal™ Recon and then use it within the group, I jumped at the chance.”

> “It lived up to expectations of good use cases for using Recon. We were able to flesh out third-party infrastructure, monitor it for signs that they might have been compromised and in many cases, we knew that they'd been compromised before our partners knew.”

After completing the procurement process, he talked about the experience. "After a Pure Signal™ Recon demonstration, the team quickly got Recon into production. We realised with this level of unprecedented visibility; we can answer questions that we couldn't answer before."

The Missing Link to Getting Ahead of Supply Chain Attacks With Proactive Defence

Most supply chain security solutions only provide visibility into changes in partner infrastructure. This does not go far enough to help when it comes to observing an attacker pivoting from a compromised business partner with access to your systems. He talked about the visibility and mentioned how Pure Signal™ Recon helped with a wide range of investigative work. “We were able to develop our own intelligence and playbooks for pinpointing things worth investigating and then use that to develop our investigative processes.” Our interviewee explains further, “The Threat Intelligence Team was able to take a small piece of information and pivot around different datasets to find additional infrastructure that an attacker might use.”

Dream Team Results for the Threat Intelligence Group

Cybersecurity leaders are frustrated with reactive security measures that don't thwart attackers or make it more difficult for them to monetize their efforts. Sub-optimal defences are a result of lacking visibility of adversaries, this only encourages the same bad actors to keep coming back again and again. When a threat intelligence organisation has visibility into global external internet telemetry, amazing strides in cyber security defence can happen. Here are some of the results he shared from their investigative efforts using Pure Signal™ Recon.

- 35 IPs were observed attacking their perimeter multiple times. They were identified using Team Cymru's BARS (Botnet Analysis And Reporting Service) intel that no other source had at the time.
- When the Russia/Ukraine conflict broke out, the threat intelligence team used Recon to help identify a foreign bank that was a hacking target and in the midst of a DDoS attack.
- During the Log4j vulnerability incident, Recon was used to identify log4j scanning traffic on peer infrastructure. The threat intelligence team were able to notify their peers and push IP blocks to the perimeter to circumvent any damage
- During sanctioned intel gathering on a peer bank, the threat intelligence team spotted potentially malicious C2 traffic and was able to share findings upon discovery for investigation.
- Recon was also used to ensure maximum application uptime, by identifying legitimate traffic so it was not blocked- A significant cost savings as well as paying dividends towards customer experience.

The Threat Intelligence Manager explained some of his key considerations for using Recon in their investigative work, "Formulating tight use cases and scope was important to our investigative work. We also wanted a certain level of automation so we could run repeatable queries and better understand expected responses and look for anomalies." When it comes to staffing a threat intelligence group, he pointed out that having a good understanding of network protocols is important. "But I think what is most useful in threat intelligence is curiosity above all, asking good questions and often new questions and having a certain level of persistence," he explained.

> "Being able to see external traffic is the big missing link in any threat investigation. When it comes to threat hunting, Recon fills in the missing link. We know a lot about what hits our perimeter. We can make some guesses as to what's happening with third parties by monitoring changes in their site, DNS records, that sort of thing. But Recon allows us to see external traffic and that is the big missing link to any threat investigation."

Transformative Threat Intelligence That Becomes a Strategic Advantage

Pure Signal™ Recon provided the threat intelligence team with unprecedented visibility and the ability to answer critical questions about their network. "Every time I look at Pure Signal™ Recon, there is something that makes me scratch my head and drives me to investigate," he explained. Given the amount of information available, it really does need an analyst's eye to make sense of the data."

With Pure Signal™ Recon, this retail banking organization was able to achieve its cybersecurity goals of gaining visibility and taking a proactive stance against their adversaries. The platform allowed the team to monitor for potential threats, detect ransomware attacks, and perform victim attribution, providing valuable insights to protect sensitive data and customer facing services.

About Team Cymru

Since 2005, Team Cymru has worked with security and analysis teams across the globe, enabling them to track and take down malevolent infrastructure and campaigns of all kinds. With visibility into all the components behind online crime campaigns, the company is a leader in threat intelligence and adversary infrastructure mapping. This Pure Signal™ intelligence powers many security vendors and Fortune 100 security teams. Team Cymru also provides no-cost services to network operators, 145+ CSIRT teams, and hosting providers around the world. For more information, visit www.team-cymru.com/ and follow us on Twitter at @Teamcymru.