TIBER:

Threat Intelligence-based

Ethical Red Teaming

Security Alliance is one of the leading providers of threat intelligence assessments. We have extensive experience delivering TIBER engagements, providing a comprehensive analysis of an organisation's threat landscape and digital footprint.

We have delivered TIBER engagements since the programme's inception, including pilot projects and framework development support; no one is better placed to deliver a TIBER Threat Intelligence Assessment.

Our unique, structured approach to performing this service provides the customer with clear picture of the most likely and dangerous threats they face.

What is TIBER?

TIBER is the pioneering framework driving intelligence-led resilience assessments that is driven by the European Central Bank (ECB) but adapted and administered at national level by their associated Central Banks or Authorities.

It applies to systemically critical organisations in the European Unions financial services sector. The core principle is that Firms are tested against realistic threat scenarios that are generated by qualified Threat Intelligence providers. Ultimately, this means that testers engage in scenarios mimicking the most credible attackers, using relevant and up-to-date tactics, techniques, and procedures (TTPs).

The Threat Intelligence Product

In line with TIBER requirements, Security Alliance provides the two CTI reports; the Threat Intelligence Assessment and the Targeting Assessment:

Threat Intelligence Assessment

This contains detailed analysis of a customer's threat landscape. It is an external assessment leveraging structured analytical techniques to identify the most relevant threat actors based on the organisation and its critical business functions. This leads to the creation of realistic threat scenarios, which are simulated by a red team during the testing phase. Scenarios are underpinned by threat level scoring, relevant use cases, and threat actor profiling. Scenarios also fuse in relevant findings from the Targeting Assessment and include all associated MITRE ATT&CK® tactics, techniques, and sub-techniques.

Targeting Assessment

This provides an in-depth review of an organisation's attack surface from the perspective of a threat actor. The purpose is to perform attacker-like reconnaissance against the organisation, its assets and its people and to explain how this information, gathered through technical and manual collection techniques, can be leveraged by the threat actor to mount an attack. These findings along with the TTPs of the threat actor feed into the final attack scenarios which are then used by the red teams to mimic a real world attack.

During the engagement we ensure that:

- Our delivery fully aligns with the requirements of the TIBER framework.

- Our reports are of consistently high quality and depth. The intelligence on threat actors and their TTPs is taken from our Threat Intelligence Platform (TIP), ThreatMatch, which is constantly enriched with the latest information and analysed by our fusion team.

- We work closely with all stakeholders in the TIBER programme including the central authority and the red team provider.

- The customer's needs are fully met, and they get as much value as possible. This means fully understanding your requirements and business functions so that our analysis and recommendations are as comprehensive and relevant as possible.

- Support is provided to all parties and work-streams to their fullest until the official end of the engagement. This includes support to the Red Team, Purple Team, 360 and wash-up sessions.

Our position in the TIBER community

- We have been one of the earliest proponents of, and participants in, the TIBER programme. We understand its value to customers and its role in bolstering the operational resilience of the wider sector.

- We have also been actively involved in the creation of sector-wide Generic Threat Landscape (GTL) reports that establish the intelligence baseline for TIBER engagements in multiple European countries.

- We continue to be involved in this process, offering our knowledge and expertise to regulatory bodies and TIBER participants.

- Our ThreatMatch portal is set up as a hub for TIBER engagements. It has the ability to publish profiles, reports, findings, and scenarios, which can then be ingested by your own security systems.

- Based on this position within the framework, we are confident that there is no other CTI provider better placed to conduct TIBER engagements.

Why Security Alliance is different

As a CREST registered company and a CREST approved supplier of Threat Intelligence services, Security Alliance delivers against recognised frameworks with our team of seasoned cyber intelligence professionals.

With a global understanding of the complex threat landscape, Security Alliance is working with some of the world's leading intelligence-based security providers.

We combine the field experience of our highly trained intelligence staff with the deep specialisations of penetration testers, to bring you the highest quality services, designed and delivered by experts.

Every client engagement at Security Alliance is unique, and our threat intelligence is generated based on each client's individual profile.

"We greatly benefited from the threat assessment. The quality of the technical staff and their analysis is outstanding."

CEO, Financial Services organization

SECURITY ALLIANCE