SECURITYALLIANCE

STAR and STAR-FS

STAR Threat Intelligence

STAR-FS Threat Intelligence

Intelligence Led Penetration Testing

Security Alliance is one of the leading provider of Threat intelligence assessments. Having performed numerous CREST STAR threat assessments, we are one of the most experienced and best qualified providers of CREST STAR and STAR-FS threat intelligence assessments in the market.

Our Intelligence Driven structured approach to performing this service provides the customer with a clear picture of the most likely and dangerous threats they face, how those threats will likely manifest, and the elements of the organisation's digital footprint threat actors would exploit in an attack.

What is STAR and STAR-FS

CREST STAR (Simulated Targeted Attack and Response) is a framework similar to CBEST, which allows organisations outside CBEST or similar frameworks, of any maturity, in any industry to conduct a structured and professional intelligence led penetration test (simulated attack/ Red Team) with accredited providers and certified individuals.

CREST STAR adopts the same core principles of CBEST, where the threat intelligence guides the testing, replicating credible threat actors, leveraging up-to-date tactics, techniques, and procedures (TTPs). STAR FS Follows the exactly the same principles except that is designed to be applied to the financial sector without geographic constraint, again outside the remit of CBEST and with limited involvement from the regulator.

CREST STAR is an ideal vehicle for preparing you for the likes of a CBEST, GBEST, TBEST, iCAST or TIBER assessment; as part of a two yearly testing cycles, to drive overall cyber resilience or to generally understand:

- What are the threats and threat actors applicable to my organisation, my eco-system and my sector(s)
- How these attacks will likely manifest
- What affects could be on my core business functions/important business services
- What our digital footprint looks like to an attacker and how will it be exploited
- How well do my security controls perform against a simulated attack of these actors
- What remediation steps do I need to perform to better predict, prevent, detect and respond to these attack scenarios

Ultimately, adopting the CREST STAR and STAR-FS frameworks ensure the same expectations, quality, and professionalism are applied to intelligence-led testing as other frameworks driven by the regulator.

CREST STAR Threat Intelligence STAR-FS Threat Intelligence CBEST THE BRITISH ASSESSMENT BUREAU ISO9001 THE BRITISH ASSESSMENT BUREAU ISO27001 CYBER ESSENTIALS PLUS Crown Commercial Service Supplier

Why Security Alliance for CREST STAR / STAR-FS engagements

- We are a pure-play cyber threat intelligence company and specialise in threat assessments within this framework and equivalent schemes such as CBEST, GBEST, TBEST, iCAST andTIBER
- We understand the value of intelligence-led red teaming when it is performed by fully qualified and experienced intelligence professionals.
- We have experience in conducting STAR engagements in a wide range of geographies outside of the UK and Europe, and in all key business and government sectors.
- Based on our experience and qualifications, we are confident that there is no other CTI provider better placed to conduct STAR engagements.

The Reporting

The assessment offered by Security Alliance covers two main areas: the Threat Intelligence Assessment and Targeting Intelligence:

Threat Intelligence Assessment

This contains the detailed analysis of your unique threat landscape. It is an assessment leveraging structured analytical techniques to identify the most relevant threat actors to you based on your organisation and critical business functions. A key output of this phase is the creation of realistic threat scenar-ios, which can be used by the red team to simulate during their attack. These are underpinned by threat level scoring, relevant use cases, and threat actor profiling.

Targeting Assessment

In combination with the threat assessment, we also provide an in-depth review of your digital footprint. The purpose is to perform reconnaissance - in the same way an attacker would - against your organisation and to explain how these findings, which will be gathered through technical and manual collection techniques, can be leveraged by threat actors. These findings feed into the final attack scenarios. We also provide supporting mitigation and remediation advice for the findings.

Detailed Attack Scenario Generation

To create the threat scenarios we fuse the likely attack scenarios, business functions, compromise actions, and infrastructure with the identified targeting findings, modus operandi and TTPs of the relevant threat actors. This provides you with detailed, tech-nical and narrative based scenarios, fully mapped to MITRE ATT&CK

During the engagement we ensure

Our delivery fully aligns with the requirements of the CREST STAR / FS frameworks

- Our reports are of consistent high quality and depth - The intelligence on threat actors and their TTPs contained in the reports are taken from our Threat Intelligence Platform (TIP), ThreatMatch, which is constantly enriched with the latest information and analysed by our fusion team.
- As well as the customer, we will work closely with either a Security Alliance partner or client preferred red team, and any other stakeholders to provide a truly collaborative and smooth engagement
- 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.

+44 (0) 20 7148 7475
info@secalliance.com
@secalliance
www.secalliance.com
14 East Bay Lane, Queen Elizabeth Olympic Park, London, E20 3BS

SECURITYALLIANCE