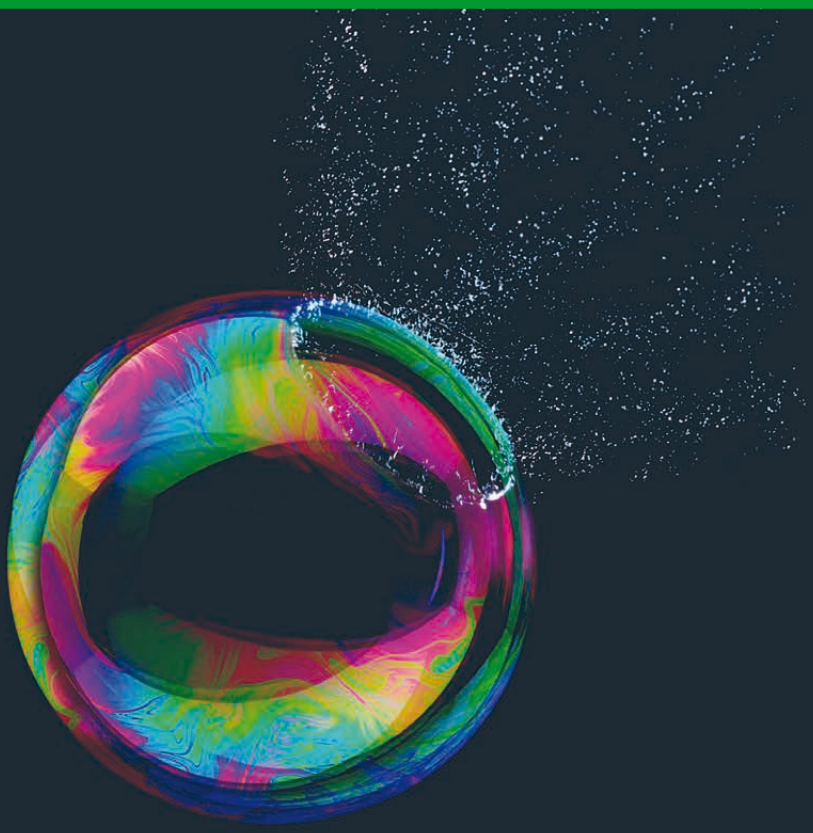
NETITUDE

AN LRQA COMPANY

GBEST Intelligence-led Penetration Testing and Red Teaming



Contents

01 Nettitude's GBEST programme

Nettitude's GBEST programme caters for the requirements of Threat Intelligence-led Penetration Testing and Red Teaming to assess an organisations ability to identify, protect, detect, respond and recover against known threats. Nettitude's approach utilises our extensive experience to deliver GBEST programmes, providing assurance through the simulation of real-world tactics, techniques and procedures.

In addition, Nettitude has been delivering Security Assurance services for more than a decade. As a CREST accredited company, we have a team of in-house, highly-skilled and certified individuals, supported by a team of consultants that have been active contributors to the Simulated Target Attack & Response (STAR) and the GBEST programme, namely CCSAM, CCSAS, CCTIM and CRTIA.

STAR and GBEST testing have been developed to provide an organisation insight and assurance through the simulation of real-world threat actors using known tactics, techniques and procedures (TTPs) to assess and enhance your organisations security posture.

Nettitude's offering will help you to identify the likely threat actors and the tools and techniques they may use to gain access to your data and networks. Nettitude will also simulate the identified sophistication levels of those threat actors which will assess your organisation's security posture, allowing you to verify how your people, process and technology are able to collectively defend your organisation and its' data.

02 GBEST Threat Intelligence Requirements

GBEST requires organisations to commission a Threat Intelligence gathering exercise by a GBEST approved provider. Nettitude are an approved Threat Intelligence provider and can deliver the following:

- Intelligence on Geo-political threats known to be operating in the sector and sub-sector
- TTP and Modus Operandi of threat actors known to be targeting similar types of organisations including MITRE references
- Open Source Intelligence (OSINT) relating to the organisation and the industry they operate within
- Gather and review closed source intelligence relevant to the organisation
- Creation of a series of scenarios that reflect real-world 'likely' threats
- Inclusion of TTP's to be simulated, goals to be executed and targets to be pursued
- All Threat Intelligence are reviewed and ratified by NCSC prior to execution

Nettitude has comprehensive methodologies for Threat Intelligence, and is continually adapting its information sources and collection techniques, providing you with relevant and timely actionable intelligence and advice.

03 GBEST Penetration Testing Requirements

The GBEST testing phase must simulate identified known real-world threat actors, as identified by Threat Intelligence. As an approved GBEST Intelligence-led Penetration Testing supplier, we provide and deliver a fully risk managed simulated attack, known as Red Teaming, to safely test your organisations defences.

What is Red Teaming

Unlike typical Penetration Testing, Red Teaming is a mature approach which focuses more on depth and looks to exploit both known and unknown vulnerabilities in an organisations attack-surface. Red Teaming does not follow automated patterns, and is not an emulation of a threat actors TTPs. Instead it is a bespoke and tailored simulation of threat actors sophistication levels and capabilities, enabling the testing team to make decisions similar to the threat actor, based on new intelligence as the attack unfolds.

Red Teaming is objective based with defined targets that concentrates on depth and impact.

Nettitude's approach to GBEST:

Features

- Intelligence-led Penetration Testing and Red Teaming for government
- Real-world attack simulation using known threat actors and their TTPs
- Assesses an organisations ability to detect, respond and recover from known-threats
- Continual risk management with both CREST CCSAS and CCSAM consultants
- Additional services as required (red, blue, purple teaming)
- Reporting and recommendations to all levels (executive/management/technical teams), enabling capability uplift across people, process and technology
- In-depth detection and response assessments (DRA) with custom reporting
- Reporting and recommendations aligned to the MITRE ATT&CK framework

Benefits

- Designed to simulate real-world attack scenarios and attack paths
- Trains and measures the effectiveness of people, process and technology used to defend the organisation
- Conducted by Nettitude's CREST certified consultants CCSAS, CCSAM and CCTIM
- Includes physical security, social engineering, malware insertion and human manipulation
- Dedicated Technical Team Leader, Risk Manager and Project Manager assigned
- Enhances the security posture, ensuring responses are measured and repeatable
- Improves the ability to identify, protect, detect, respond and recover
- Remediation and threat strategies to manage risks and improve capabilities
- Awareness of the key issues which can compromise a GBEST assessment
- Extensive knowledge of common findings and thematic vulnerabilities, which need to be monitored throughout a GBEST

Advanced Tooling

Nettitude has developed its own state of the art custom tooling that allows the simulation of a wide range of threat actors from commodity threat actors to advanced persistent threats (Nation State) that are known to be prevalent.

As a consequence, when we deliver GBEST engagements, we are able to deliver a true reflection of the types of TTPs that threat groups are known to be leveraging. This toolset is unique within the industry and is one of the reasons why Nettitude's team has been highly successful in supporting organisations intelligence led assurance strategies.

Nettitude have also developed open source tooling which allows for a wider range of threat actors to be accurately simulated which is backed by subject matter experts in Red Teaming, with high levels of skill and experience in mature and complex environments.

04 Nettitude's Five Stages to GBEST

A GBEST exercise will be delivered in the following five high level stages:

05 Complimentary Services

Nettitude have a range of additional services that have found to compliment pre and post GBEST engagements to help further enhance an organisations ability to detect and respond to known threats:

- Incident Response and forensics
- SOC Maturity Assessment and/or playbook review
- Threat Hunting service
- Purple Teaming
- Simulated Attack Replay
- Red / Blue team Training

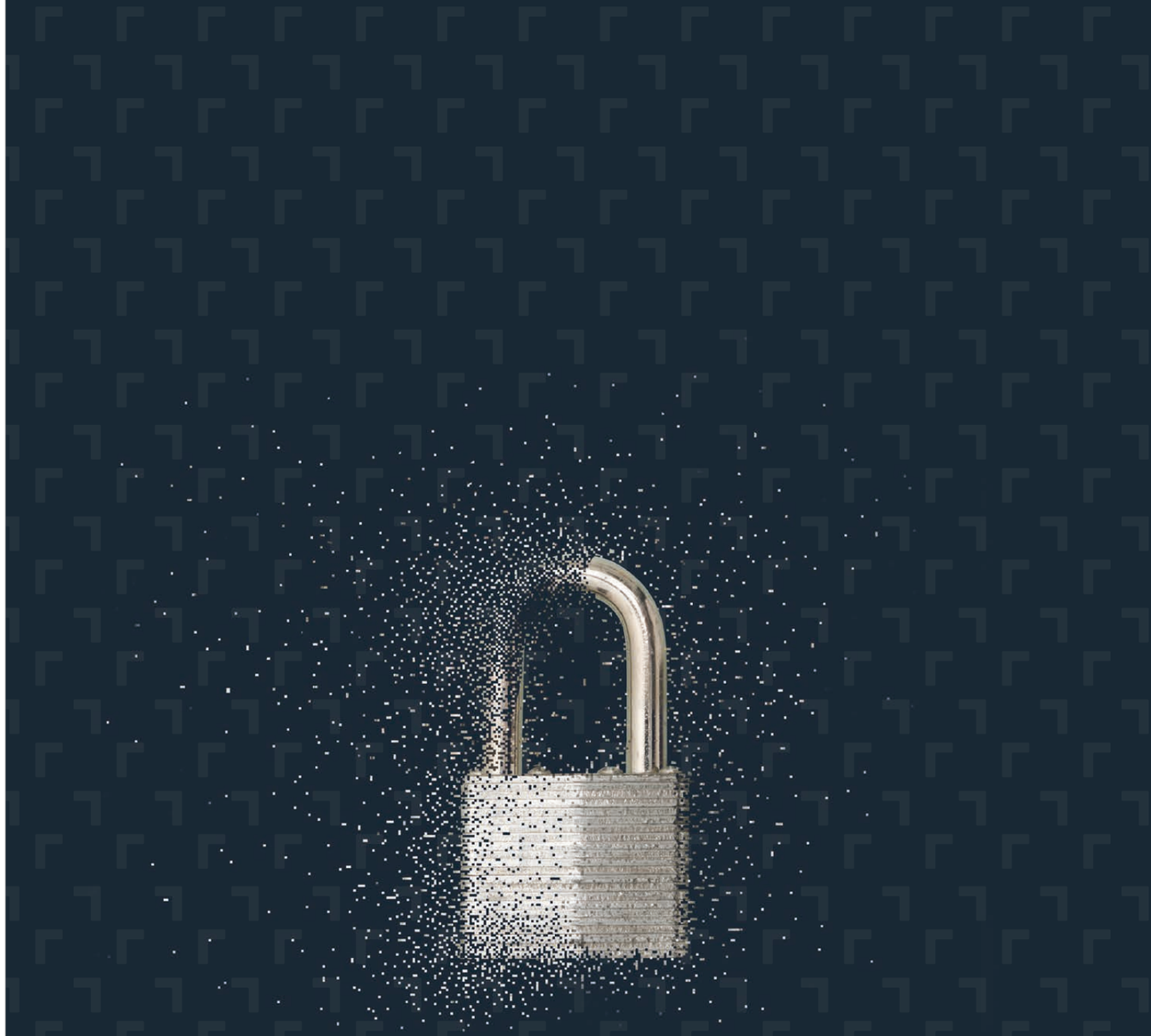
06 How can Nettitude help?

Get in touch with your local Nettitude team to find out how we can help you improve and advance the approach to security for your organisation.

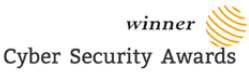
Nettitude is a member of The Council of Registered Ethical Security Testers (CREST) and certified by the UK Government to deliver cyber security testing as a CHECK green light company and part of the GBEST simulated attack scheme.

Nettitude has a team of cyber security consultants qualified in areas such as ISO 27001, PCI DSS, PA-DSS, P2PE and much more. We also have a, incident response team with forensic investigation unit deployed for activities including data breach analysis and data discovery. We are an Approved Scanning Vendor (ASV) registered by the PCI Security Standards Council (SSC) to conduct authorized vulnerability scans for PCI compliance.

Sample reports are available on request.
For more information on Nettitude's cyber ecurity services please visit our websites:
www.nettitude.co.uk and **www.nettitude.com**
or contact us directly at **solutions@nettitude.com.**



NETTITUDE
AN LRQA COMPANY



NETTITUDE
AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com