Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 115-119

Cyber Threat Intelligence Based Scoping of Red Team Exercises

Svilen Kamdzhalov
IT Department
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
s.kamdzhalov@naval-acad.bg

Dimitar Nikolov
IT Department
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
d.nikolov@naval-acad.bg

Abstract – One of the most effective ways to test a company's security posture is through red team assessments and targeted penetration testing. This article defines one of the most effective approaches for determining the scope of the tests and the stages they go through. The stages include getting to understand the potential attackers, their tactics, techniques and procedures, the modus operandi and the objective with which they operate. The paper also discusses the importance of people, business processes, technology and distinguishing between important and critical assets as part of effective testing. It discusses the best tool for proper scoping is contextualized threat intelligence-based analysis and red team assessment frameworks such as TIBER-EU, CBEST and iCAST. This paper describes an approach that can be used to improve the scoping of the mentioned tests and hence increase their value.

Keywords – Asset classification, contextualized threat intelligence, penetration testing, red team assessments, threat modeling

I. INTRODUCTION

Over the past decade, cybersecurity assessments have evolved significantly - moving beyond traditional penetration testing toward more sophisticated, scenario-driven methodologies. While penetration testing focuses on identifying and confirming the exploitability of specific vulnerabilities, modern red team assessments evaluate an organization's broader security posture: its ability to detect, contain, and recover from realistic, targeted attacks. To meet this expanded mandate, disciplines such as adversary emulation, purple team exercises, and threat-informed red teaming have emerged, incorporating factors like social engineering, operational security, and situational awareness into the assessment model.

The red team concept originated [1] in Cold War-era military exercises, gaining large-scale adoption in the 1980s when the NSA pioneered its application in the intelligence community. The discipline entered the cyber domain following Mandiant's landmark 2013 APT1 report [2], which documented state-sponsored cyber espionage campaigns and introduced the concept of Advanced Persistent Threats (APTs). This catalysed systematic TTP documentation efforts, culminating in the release of the MITRE ATT&CK [3] framework in 2015 - a comprehensive, community-driven knowledge base of adversary behaviours that has since become the common language of threat-informed defense. As APTs became better understood [4], regulated red team frameworks emerged to formalize assessment practices across the financial sector, including CBEST, TIBER-EU, iCAST, and others. While these frameworks affirm the central role of Cyber Threat Intelligence (CTI), they stop short of prescribing how assessments should be scoped and executed in practice - leaving a critical gap between high-level guidance and operational implementation.

The entry into force of the EU Cyber Resilience Act in December 2024, alongside updated NIST guidance, has sharpened a second, related gap: the near-exclusive focus of existing frameworks on financial institutions with conventional IT infrastructure. Critical infrastructure sectors - including power grids, industrial control systems, ports, and maritime assets - face comparable and in some cases greater APT exposure, yet no structured red team assessment framework governs their evaluation. While OT red teaming is described in practitioner literature, replicable methodologies for scoping and executing adversary emulation exercises in ICS, SCADA, and OT environments remain absent.

This paper addresses both gaps. Its primary focus is on defining penetration testing and red team assessment scope using CTI as the foundational input - a step that is underprescribed in existing frameworks yet disproportionately consequential for assessment quality. The intelligence cycle, threat actor profiling, TTP mapping, and asset contextualization are each examined in turn, and a worked example using a fictitious defense supply chain company is provided to illustrate how a complete, credible, and operationally relevant scope is constructed from first principles. The same approach is equally applicable to

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.210

penetration test scoping and to environments beyond the financial sector, including those dependent on operational technology.

II. RED TEAM ASSESSMENT FRAMEWORKS

One of the most common situations on the customer's side is the lack of understanding of the above mentioned approaches and the overall organization and execution of a Red Team assessment. Since many financial and political institutions have been in this position and guidance was definitely needed, several frameworks were developed. A not definitive list would include:

- CBEST Intelligence Led Testing, created by the Bank of England .
- Threat Intelligence-Based Ethical Red Teaming – TIBER-EU [6] (EU Red Team Assessment framework).
- Red Team: Adversarial Attack Simulation Exercises (AASE) – created and adhered to by the Association of Banks of Singapore [7].
- Iintelligence-led Cyber Attack Simulation Testing (iCAST) – HKMA (the Hong Kong Monetary Authority adversary emulation exercise framework)
- G-7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT) [9].
- GFMA (Global Financial Markets Association) – a framework for the Regulatory Use of Penetration Testing and Red Teaming in the Financial Services Industry.
- Intelligence-led Cyber Resilience Testing (I-CRT) Framework

A deeper look into the above listed frameworks shows that all of them consider threat intelligence based scope, fundamental to the assessment.

CBEST is a framework to deliver controlled, intelligence-led cybersecurity tests. The tests replicate the threat actors TTP's, considered by the UK Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions[10]. Institutions that are part of the United Kingdom's Financial Services Sector must remain resilient to cyber attack. To help these organizations achieve this, CBEST security assessment framework was implemented. CBEST proposes an intelligence-led penetration testing approach that replicates the actions of a cyber attacker's intent on compromising an organization's Critical Functions and the technology assets and people supporting those functions. Collaboration, evidence and improvement lie at the heart of CBEST [5] as well as a close liaison with the Bank of England and relevant regulators. For those organizations that form part of the Critical National Infrastructure liaison with GCHQ may also be required. The most specific feature of CBEST is its intelligence-led approach. The assessment process consists of four phases of work:

- Initiation Phase assessment: is formally launched, the scope is established, and TI/PT service providers are procured.
- Threat Intelligence Phase: the core threat intelligence deliverables are produced, threat scenarios are developed into a draft Penetration Test Plan, threat intelligence is assessed, and handed over to the PT provider.
- Penetration Testing Phase: an intelligence-led penetration test is planned, executed and reviewed, and detection and response capabilities are assessed.
- Closure Phase: Intelligence, Detection, and Response Report and Remediation Plan are finalized.

During the Threat Intelligence Phase and Penetration Testing Phase, the CBEST assessment is led by the TI service provider and PT service provider respectively.

TIBER-EU is a framework that delivers an intelligence-led red team PT. Intelligence-led red team assesments replicate the TTP's of real threat actors who, on the basis of threat intelligence analysis, are considered a genuine threat. An intelligence-led red team penetration test/red team assessment involves the use of a variety of techniques to simulate a complex attack on people, processes and technologies and measure the effectiveness of the client detection and response capabilities. The Threat Intelligence-based Ethical Red Teaming (TIBER-EU) Framework enables EU authorities to build a program to test and improve the EU financial institutions resilience against sophisticated cyber attacks.

TIBER-EU is designed to be adopted by the relevant authorities in any jurisdiction, on a voluntary basis and from a variety of perspectives, namely as a supervisory or oversight tool.

Hong Kong Monetary Authority (HKMA) has developed a Cyber Fortification Initiative (CFI), which comprises three components [8]:

•Cyber Resilience Assessment Framework (C-RAF)

•Cyber Intelligence Sharing Platform

•Professional Development Program(PDP)

C-RAF compromised the following elements:

•Inherent risk assessment

•Maturity assessment

•Intelligence-led cyber attack simulation testing (iCAST)

Under iCAST, the traditional penetration test is augmented by taking in consideration the knowledge of the penetration test provider and the relevant threat intelligence to build end-to-end testing scenarios (from attack initiation to achieving pre-defined test goals.

All of the mentioned frameworks' practical efficiency depends on cyber threat intelligence [11] and stress the importance and benefits of proper threat intelligence analysis. Unfortunately, the analysis and its results are often generalized and taken out of context.

The cyber threat intelligence lifecycle consists [12], in general, of five stages. It is a process model and has the

purpose of systematically collecting, processing and analyzing data in order to answer specific questions. The five stages are as follows:

1. Planning and direction
2. Collection
3. Analysis
4. Production
5. Dissemination and Feedback

Due to improper implementation of some of the phases or in some cases even breaking the Cyber Threat Intelligence Cycle, the result and correspondingly the scope are suboptimal and lead to suboptimal results.

Many of the customers lack or have inefficient Threat Intelligence programs and are unable to define the specific APT's and the campaigns relative to their geopolitical and industry context, technology and infrastructure. Due to that fact it is in general left to the assessor to decide what TTP's (Techniques, Tactics and Procedures) are relevant to the case and how to apply them, but the assessor usually does not have the resource to do a proper profiling of the target and select the most relevant TTP's, nor does he have the needed deep understanding of the business processes and priorities of the client. The CTIC [13] can and should be used in all steps of the definition and refinement of the engagement scope. The first step is to define the geopolitical and industry context of the client. Here a helpful approach for data collection is the interview of the client c-level supplemented by OSINT research. Regarding analysis techniques, some geopolitical and network analysis is a good starting point [14].

Once the industry and business network context are clear, the next step is to analyze the infrastructure and technological stack of the client. The data collection will be related again to document analysis of the provided diagrams and asset management data, and OSINT interpolation in order to understand the technological information readily available to the projected adversary. More than one CTIC [15] iteration might be needed in order to pinpoint the vital parts of the infrastructure.

Once the business and technology analysis of the client are concluded, the resulting product should form the base for the next stages related to the profiling of the potential adversary.

The first step of that stage is the search for threat actors and threat groups (TATG) with a history of attacks on businesses with similar business profile and geopolitical relations to the customer. Analysis should be mainly concentrated on episodes and campaigns in the last 2 years.

In the next step a technical analysis is to be executed, comparing the techniques, tactics and procedures (TTP's) of the potential TATG [16] and the infrastructure and technological stack of the customer. The product should define the relevant and applicable TTP's that could be included in the scope of the assessment.

The steps described above are also used by real threats, although with some differences in the methods and sources. In certain cases the APT's develop their target profile sometimes for over a year before the attack [17].

III. The CTI Lifecycle and Its Role in Scope Definition

The following case study illustrates the practical application of adversary emulation methodology through a fictitious company designated SAT-SOFT, a Taiwan-based manufacturer of satellite hardware components and firmware whose business partners include direct suppliers to the U.S. Department of Defence Strategic Satellite Program. The company operates two production facilities with a third under construction, each site hosting a small office connected through a VPN to the main headquarters in Taipei. The on-premises network infrastructure consists primarily of Cisco and Netgear routers, Fortinet firewall devices, Windows workstations, at least one NAS server, and an Active Directory environment spanning multiple domains - a technological profile that closely mirrors the target architecture documented in Volt Typhoon operational reporting.

Following a threat profile analysis conducted by the Red Team Assessment Provider (RTAP)[18], the chosen Adversary Emulation Candidate was identified as the actor tracked by Microsoft as Volt Typhoon[19], by CrowdStrike as Vanguard Panda, by Palo Alto Networks Unit 42 as Insidious Taurus, and within the MITRE ATT&CK [20] framework as Bronze Silhouette. The selection was driven by the direct correspondence between the client's infrastructure - SOHO network[21] devices, Fortinet perimeter equipment, Active Directory[22], and supply chain relationships with defence contractors - and the documented targeting preferences and technical capabilities of the emulated threat actor. Mapping the actor's tactics, techniques, and procedures to the MITRE ATT&CK framework established a common operational language for all participating parties and formed the basis for scenario design across four assessment phases.

The first phase, Resource Development and Initial Access, targeted externally facing services and applications, with phishing campaigns and supply chain attack vectors directed at the new construction site incorporated to replicate the actor's known initial access methodology. At this stage the emulation replicates the actor's use of compromised SOHO devices - including Cisco, Netgear, ASUS, D-Link, and Zyxel routers - as command and control relay nodes, alongside deployment of custom Fast Reverse Proxy (FRP) clients with hardcoded C2 callbacks and port forwarding configurations established through native Netsh commands. Where phase one objectives were not achieved within defined parameters, the white cell - the controlling and coordinating authority of the exercise - retained authority to introduce assumed breach conditions to preserve assessment continuity.

The second phase, Lateral Movement, Privilege Escalation, and Persistence, proceeded on an assumed breach basis and focused exclusively on native tooling and

hands-on keyboard activity to replicate the actor's operational tradecraft as precisely as possible. The primary objectives were the acquisition of highly privileged Active Directory credentials, extraction of the ntds.dit file and SYSTEM registry hive through NTDSutil, and the establishment of durable persistence within the domain environment while maintaining the minimal forensic footprint characteristic of the emulated actor. The third phase, Discovery, directed operators to enumerate network topology, identify operational technology components including SCADA, HMI, and PLC systems where present, and map defensive capabilities including antivirus, EDR, and HIDS solutions using PowerShell, WMIC, and standard Windows command-line utilities consistent with the actor's documented discovery procedures. The fourth and final phase, Collection, Defence Evasion, and Exfiltration, targeted the acquisition of business-valuable data, industrial secrets, financial credentials, and non-destructive proof of control over operational technology systems, with operators required to maintain a low profile throughout and to employ the full range of Living-off-the-Land binaries - including certutil, ldifde, makecab, wevtutil, and impacket - to avoid detection and remove operational artefacts prior to withdrawal.

The primary deliverables of the assessment consisted of a comprehensive technical report and a structured debrief session conducted jointly with the blue team. The report, calibrated to its intended audience, documented targets achieved, successful and failed attack attempts, effective and failed defensive countermeasures, and a complete account of commands executed and their results. The debrief session served the dual purpose of exposing shortcomings in the defensive posture with actionable remediation guidance, and formally acknowledging the defensive activities that demonstrated the organisation's established level of cyber resilience - providing the client's business partners with the documented evidence of security maturity they had requested as a condition of continued supply chain participation.

IV. Conclusion

The definition of scope in red team and adversary emulation assessments is not a procedural formality - it is the foundational analytical act upon which the validity and operational relevance of the entire assessment depends. As this paper has demonstrated, a scope constructed without rigorous threat intelligence integration, without systematic application of the intelligence cycle, and without direct correspondence to the client's geopolitical exposure, technological profile, and business relationships will produce results that are technically competent but strategically meaningless. The SAT-SOFT case study illustrates the alternative: when threat profiling drives adversary selection, when the chosen Adversary Emulation Candidate's documented tactics, techniques, and procedures are mapped precisely to the client's infrastructure, and when assessment phases are structured to replicate the actual modus operandi of the most plausible threat actor, the outcomes of the exercise carry genuine predictive and defensive value. The intelligence cycle is not a preliminary step to be completed before the assessment begins - it is a continuous analytical discipline that must be applied iteratively across every phase of scope definition, refinement, and execution.

The frameworks examined in this paper - whether grounded in MITRE ATT&CK, the Cyber Kill Chain, or structured red team methodologies - converge on a single operational principle: that the quality of an adversary emulation assessment is determined not by the sophistication of the tools deployed but by the fidelity with which the emulated threat reflects the adversary most likely to target the specific organisation under assessment. Clearly defined objectives, measurable targets at each assessment phase, and rigorous documentation of both successful and failed attack and defence activities are the instruments through which this fidelity is verified and communicated. As the threat landscape continues to evolve - and as state-sponsored actors such as Volt Typhoon demonstrate an increasing willingness to conduct long-duration, low-visibility operations against organisations that have never considered themselves high-value targets - the capacity to construct and execute intelligence-driven, threat-relevant assessments will determine whether organisations discover their vulnerabilities before their adversaries exploit them, or after.

ACKNOWLEDGEMENT

This research paper has received funding from Ministry of Education and Science of the Republic of Bulgaria under the National Science Program "SECURITY AND DEFENCE", in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No: 731/21.10.2021 and according to Agreement No: D01-74/19.05.2022.

References

[1] TechRound, "History of Red Team Exercises." [Online]. Available: https://techround.co.uk/guides/history-red-team-exercises/ [Accessed: March 23, 2026].

[2] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 2021. [Online]. Available: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf[Accessed: March. 23, 2026].

[3] MITRE ATT&CK, "ATT&CK Framework." [Online]. Available: https://attack.mitre.org/[Accessed: March 26, 2026].

[4] Fortinet, "Red Team Assessment Solution Guide." [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-red-team-assessment.pdf [Accessed: March 22, 2026].

[5] CREST, "CBEST Framework." [Online]. Available: https://www.crest-approved.org/membership/cbest/ [Accessed: March 23, 2026].

[6] European Central Bank, "TIBER-EU Red Team Test Plan Guidance," 2025. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_red_team_test_plan_guidance_2025.en.pdf [Accessed: March 26, 2026].

[7] Association of Banks in Singapore, "Red Team: Adversarial Attack Simulation Exercises Guidelines." [Online]. Available: https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-

06766a69f299c69658b7dff00006ed795.pdf [Accessed: March 25, 2026].

[8] Hong Kong Monetary Authority, "Intelligence-Led Cyber Attack Simulation Testing (iCAST)." [Online]. Available: https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf [Accessed: March 28, 2026].

[9] G7, "Fundamental Elements for Threat-Led Penetration Testing," 2018. [Online]. Available: https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2018-G7-fundamental-elements-for-threat-led-penetration-testing.en.pdf [Accessed: March. 26, 2026].

[10] Global Financial Markets Association, "Threat-Led Penetration Testing Guidance." [Online]. Available: https://www.gfma.org/wp-content/uploads/0/83/197/231/fff190cf-305a-44a6-a429-39848f22a48b.pdf [Accessed: March 28, 2026].

[11] Z. Wang, O. D. Adeyemo and E. A. Akinsoto, "Summary of Cyber Threat Intelligence," Int. J. Innov. Res. Multidiscip. Field, Vol. 8, № 3, Mar. 2022. [Online]. Available: https://www.ijirmf.com/wp-content/uploads/IJIRMF202203006.pdf [Accessed: March. 28, 2026].

[12] R. Brown and R. M. Lee, "The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey," SANS Institute, 2019. [Online]. Available: https://www.sans.org/white-papers/38790/ [Accessed: Apr. 02, 2026].

[13] Google Cloud, "Hands-On Introduction to Mandiant Approach to OT Red Teaming." [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/hands-on-introduction-to-mandiant-approach-to-ot-red-teaming [Accessed: Apr. 02, 2026].

[14] SANS Institute, "ICS Cyber Kill Chain." [Online]. Available: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf [Accessed: Apr. 02, 2026].

[15] Cybersecurity and Infrastructure Security Agency, "Red Team Assessment Reveals Key Cybersecurity Gaps in Critical Infrastructure Organization." [Online]. Available: https://industrialcyber.co/cisa/cisa-red-team-assessment-reveals-key-cybersecurity-gaps-in-critical-infrastructure-organization/ [Accessed: March 28, 2026].

[16] MITRE, "APT3 Adversary Emulation Plan." [Online]. Available: https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf [Accessed: March 30, 2026].

[17] Hong Kong Monetary Authority, "Cyber Resilience Assessment Framework (C-RAF)," 2016. [Online]. Available: https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc1fe13498132b4fa835b_HKMA%20CFI%20-%20Cyber%20Resilience%20Assessment%20Framework%20-%20Dec%202016.pdf [Accessed: Apr. 02, 2026].

[18] MITRE ATT&CK, "APT Group G1017." [Online]. Available: https://attack.mitre.org/groups/G1017/ [Accessed: Apr. 02, 2026].

[19] D. Dimitrov and E. Andreev, "China's Strategic Competition in Cyberspace: Volt Typhoon and Salt Typhoon as a Projection of Power, a More Aggressive Posture and a Future Beyond Espionage," Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, vol. 2, pp. 115–122, 2025. Available: https://doi.org/10.17770/etr2025vol2.8618 [Accessed: March 26, 2026].

[20] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Advisory AA24-038A." [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a [Accessed Apr. 04, 2026].

[21] Office of the Superintendent of Financial Institutions, "Intelligence-Led Cyber Resilience Testing (I-CRT) Framework." [Online]. Available: https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfis-intelligence-led-cyber-resilience-testing-crt-framework[Accessed: Apr. 04, 2026].

[22] NVISO Labs, "Attack and Defense in OT: Enhancing Cyber Resilience in Industrial Systems with Red Team Operations," Feb. 28, 2025. [Online]. Available: https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfis-intelligence-led-cyber-resilience-testing-crt-framework [Accessed Apr. 02, 2026].