TAG

ANALYST REPORT: SNAPATTACK FOR CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG

SNAPATTACK

TAG

SNAPATTACK FOR CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

Continuous threat exposure management (CTEM) has emerged as a useful designation for proactive assessment and handling of vulnerabilities in an enterprise. The method has evolved from traditional vulnerability management and includes focus on a wide range of different cyber threats across the attack surface, including zero day. Commercial cybersecurity vendor SnapAttack is shown here to map well to salient CTEM functional requirements.

INTRODUCTION

Typical drawbacks in existing vulnerability management programs for enterprise include isolated focus on known security weaknesses, and insufficient coverage of an ever-expanding and often virtualized enterprise attack surface. Traditional vulnerability management programs are also sometimes designed to manage little more than driving emergency patches on an ad hoc basis with manual tracking.

More recently, the most capable cybersecurity organizations have begun to create and manage programs that are more continuous in their operation, automated in their implementation, and driven by refined and justified prioritization schemes that connect with business objectives. Some analysts have begun to refer to such programs as continuous threat exposure management (CTEM), which seems a suitable designation to use here.[1]

In this report, we provide a technical overview of CTEM from the perspective of the enterprise security practitioner, and we then provide a brief overview of commercial cybersecurity vendor SnapAttack. CTEM functional requirements are then mapped to SnapAttack capabilities to demonstrate the use of the model in the context of a live practical commercial solution. A proposed CTEM action plan for enterprise is then offered.

OVERVIEW OF CTEM

Continuous Threat Exposure Management (CTEM) is a new cybersecurity methodology designed to help organizations reduce their threat exposure by implementing a structured and iterative approach to prioritize, safeguard, and to proactively improve security posture. As suggested above, traditional approaches to vulnerability management are less effective due to the rapidly expanding attack surface and reactive nature of the work. CTEM goes beyond common vulnerability management by integrating known and unknown vulnerabilities and control gaps to better understand overall exposure and attempt to mitigate those issues before an attacker capitalizes on them

The Gartner paper cited above describes the CTEM model as being implemented using five key security operational steps, which we repeat below. We will use these steps, organized both as a methodology and as a set of evaluation criteria, as the functional basis for determining how well a given commercial platform (i.e., SnapAttack) supports the goals addressed in the CTEM model:

- **Scoping** – This process involves understanding the organization's critical assets and risks across the full attack surface.
- **Discovery** – This process focuses on identifying assets, vulnerabilities, and weaknesses and documenting them in a usable manner.
- **Prioritization** – This step supports focusing on the most critical threats based on urgency, severity, available controls, and business impact.
- **Validation** – This involves testing and assessing the most likely attack success and potential impact.
- **Mobilization** – This ensures that the identified issues are addressed through collaborative efforts, considering business context and operational feasibility.

As should be obvious from the list of requirements shown above, the CTEM model is not just about implementing a set of tools, but rather represents a more holistic program that requires cross-team collaboration and organizational-level remediation of vulnerabilities and gaps. It helps organizations optimize their security posture and provides a framework for continuous improvement.

The good news is that CTEM complements vulnerability management investments and can be integrated with other security initiatives. It requires a phased approach to deployment, starting with familiarization and gradually expanding to cover areas like attack surface management and security posture validation. By adopting CTEM, organizations can better manage their exposures and make informed decisions to enhance their overall security resilience.

SUMMARY OF SNAPATTACK

Commercial vendor SnapAttack is a new cloud-based software solution spun off by Booz Allen Hamilton, a global cybersecurity firm, which transferred all relevant assets to this new cyber threat hunting and detection company. The SnapAttack platform aims to proactively detect and defend against cyber threats by bringing together actionable threat intelligence and hacker detection capabilities.

SnapAttack supports cybersecurity collaboration by facilitating the sharing of threat intelligence, attack emulations, and detection analytics. The origin of the approach came from Booz Allen DarkLabs, consisting of an elite team of experienced security researchers, threat hunters, penetration testers, and data scientists who specialize in cyber defense, data analytics, threat hunting, and cyber offense.

The platform's focus is to help organizations identify blind spots and close detection gaps in their infrastructure. SnapAttack accomplishes this goal of thwarting the leverage adversaries might have to gain and maintain illicit access undetected, through a technical solution that emphasizes detection and defense. By leveraging advanced technologies and decades of experience in defeating advanced cyber threats, the SnapAttack team provides a novel means for reducing cyber risk.

One aspect of SnapAttack is its focus on detection engineering. The platform enables the rapid development and maintenance of high-quality detections, ensuring that less effort is required each time a new threat is introduced. SnapAttack introduces the concept of detection-as-code, which standardizes how detections can be built using a repeatable and testable detection development lifecycle, making them shareable and repeatable across different environments and platforms.

In addition, SnapAttack supports threat-informed cyber operations through an emphasis on support for purple teaming. As security engineers know, purple teams drive value through the interactions between red and blue teams, thus reinforcing the need for collaboration and continuous feedback and learning. This helps to ensure maximum value from tools, optimization of process output, and other useful security outcomes.

Security teams will also benefit from SnapAttack's ingesting of closed and open source intelligence to help correlate and interpret collected data. AI-based tools are used to contextualize data using intelligence, and to help security teams understand how threats might operate in their environment. This approach gives enterprise security teams the best chances of having an effective detection environment.

MAPPING SNAPATTACK TO CTEM REQUIREMENTS

One important aspect of the SnapAttack solution is its support for the objectives embodied in the CTEM model described above. That is, the intelligence-led detection engineering and hunting focus inherent in the SnapAttack platform match up well with the functional requirements we've identified as being salient in the CTEM model, as envisioned and reported in the original paper. Below we map SnapAttack functionality to the model to demonstrate such coverage.

SnapAttack Support for CTEM Scoping – This process involves understanding the organization's critical assets and risks across the full attack surface. SnapAttack also aims to simplify the threat intelligence process through the automated creation of unique threat profiles, which highlight for customers relevant, prioritized threat actors and the attacks they are likely to attempt. By definition, the SnapAttack solution is focused across the entire attack surface, as defined by the MITRE ATT&CK framework.[2] This is evident in its emphasis on detection engineering for all forms of telemetry (versus, for example, endpoint detection and response (EDR) using primarily endpoint data).

SnapAttack Support for CTEM Discovery – This process focuses on identifying assets, vulnerabilities, and weaknesses and documenting them in a usable manner. The discovery process inherent in both detection engineering and purple team analysis is comprehensive and will also, by definition, cover all assets, resources, and data that might be involved in some offensive campaign.

SnapAttack Support for CTEM Prioritization – This step supports focusing on the most critical threats based on urgency, severity, available controls, and business impact. This is addressed by SnapAttack through automated prioritization of threats via tailored threat profiles, coupled with machine learning analysis to identify the likely attack vectors and most effective detection strategy for the corresponding threat. The platform also enables the organization to identify detection coverage gaps, which serve as priority requirements for security operations teams. Such prioritization supports contextualization of threats during the discovery phase of detection engineering and threat hunting.

SnapAttack Support for CTEM Validation – This involves testing and assessing the most likely attack outcome and potential impact on valued assets. This CTEM requirement lines up particularly well for SnapAttack, since validation is a major component of all purple team coordination. Detection engineering also involves collection of telemetry to drive better understanding of on-going threats. Specifically, validation occurs in several ways:

1. SnapAttack automatically validates the detection content against the attack that's been emulated in its sandbox. In so doing, the platform proves the detection works in an ideal logging environment.
2. SnapAttack applies a confidence scoring algorithm which takes the detection library and benchmarks it against the customer's dataset, which provides the ability to predict the performance of the detection content in the real-world (i.e., false positiveness, false negativeness, and robustness).
3. SnapAttack recommends the best detection for any given threat based upon both the validation status and confidence score, enabling the security operations team to optimize detection outcomes with pre-vetted content that is aligned to priority threats.
4. SnapAttack can enable the user to launch thousands of pre-curated attacks to validate detection content in the real world. This can be done atomically or by stringing several attacks together to validate detection against an actual adversary campaign. The user can also craft custom attacks using SnapAttack's attack builder to stress test their detection performance however they choose.

SnapAttack Support for CTEM Mobilization – This ensures that the identified issues are addressed through collaborative efforts, considering business context and operational feasibility. As one might expect, support for purple teaming is especially important to ensure proper mobilization of the security team, coordinated with any important adjacent groups in IT, network, or other organizations. This allows multiple teams to be informed about organization's defenses prior to an actual attack occurring.

NEXT STEPS

The presumption in this report is that readers have expressed interest in the CTEM model and might be using this as the basis for review, assessment, or source selection of commercial cybersecurity platforms. This is reasonable since the model does include many important functional capabilities that modern security operation center (SOC) teams will want integrated into their day-to-day tactical and longer-term strategic activity.

As we have shown, the SnapAttack platform lines up well with the model, which implies that deployment of the solution should bring the desired benefits included in the CTEM approach. An action plan might be to contact SnapAttack for review and assessment with respect to local functional requirements. The platform is well-suited to proof of concept (POC) operations since it can be an overlay support function for any existing SOC implementation.

The TAG Infosphere team is available to assist enterprise teams working on this type of review and integration. In particular, reviewing CTEM or similar models in the context of the unique aspects of the local environment is recommended. Evaluation of SnapAttack should also involve a deeper dive into the capability set than the high-level view offered here, but hopefully this short paper provides a useful starting point for security engineers interested in CTEM.

[1] The paper entitled "Implement a Continuous Threat Exposure Management (CTEM) Program" by Jeremy D'Hoinne and others (Gartner analysts) offers an introduction to the CTEM concept. The paper is not generally available on the Internet except for marketing download from paying vendors. Readers are welcome to seek websites offering the paper but will likely be met by a contact wall before download.

[2] See https://attack.mitre.org/.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.