www.pipelinepub.com
Volume 20, Issue 2

A New Framework for Cybersecurity

By: Jacob Ukelson, D.Sc.

It is no secret that current approaches to cyber defense are failing to stem the tide of successful attacks on enterprises of all sizes. An approach to reducing risk called Continuous Threat Exposure Management (CTEM) is emerging that Gartner predicts will reduce the chances of system breaches by a factor of three. This article explains the CTEM process, why it is needed, and how businesses can implement it.

Current Cybersecurity Basics

But before getting into the details of CTEM let us review some basics of how organizations typically do their cybersecurity and examine why they all too often fail to prevent security breaches.

There are essentially three components to any cybersecurity system. The central component is cybersecurity controls. Simply put, the purpose of controls is to establish and enforce the rules governing who may access what and when within an IT system. There are hundreds if not thousands of products on the market that provide these controls. Generally, however, they include (a) *firewalls* – of which there are many types; (b) *identity and access management tools* – Active Directory for example; and (c) *encryption* – for both data at rest and in motion.

Putting these controls in place is not a matter of "set it and forget it." That brings us to the other two components of the cybersecurity system. The first is a system and methodology for ensuring the controls are deployed, operational, and working as intended. The tools and methods for this include periodic audits and compliance verification, vulnerability and patch management, and penetration testing.

The last component is best described as monitoring, prevention, detection, and response. In spite of best efforts to deploy strong security controls and ensure the controls are up to date and working well, attacks continue to occur, and some will breach the security defenses. To prevent or limit damage from successful attacks we need systems to detect and respond to them. Tools for intrusion prevention, detection and response include Security and Information Event Management (SIEM); Security Orchestration, Automation and Response (SOAR); and Detection and Response (EDR, NDR, XDR).

The foregoing components are encapsulated in Figure 1 below. From a timeline perspective, they comprise the activities designed to prevent a successful attack ("Left of Bang") and activities that take place after a successful attack ("Right of Bang").

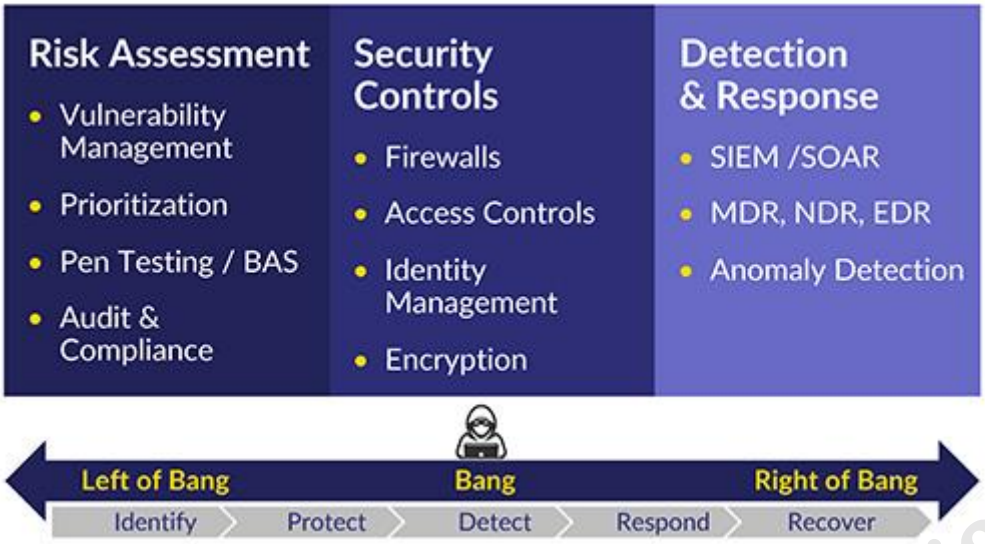

Figure 1: Standard Framework for Cybersecurity

Where Cybersecurity Fails

Yet despite increased organizational investments in cybersecurity products, services, and personnel, cybersecurity risk is on the rise, and the frequency and cost of successful attacks are increasing.

This increased risk is evidenced by the rising cost of cyber insurance (see Figure 2, on next page). Premiums are not only rising; carriers are also lowering payouts and coverage.

So why is risk rising so dramatically? Is it due to failures in controls, prevention, or detection and response? All the above?

In some cases, controls are at fault. A common control gap, for example, is a failure to implement multi-factor authentication. However, this and other control gaps (such as weak privileged access management) are usually not difficult to identify and address. In fact, such controls are becoming a requirement for obtaining cyber insurance. As organizations implement stronger controls, we would expect risk to decline, not rise.

Nor does the data regarding detection and response explain why risk is increasing. In fact, we have seen some recent improvements (reductions) in mean time to detect (MTTD) and mean time to respond (MTTR). The 2023 data breach report from IBM shows only minor changes over the past several years, including some declineover the past 3 years (Figure 3, bottom of next page). The emergence of better-integrated detection and response tools assisted by learning AI technology seems to be reversing past increases in MTTR/MTTD. In summary, neither a lack of security controls nor a worsening of detection and response times explain the increases in cyber risk.

First, we have compliance audits. These audits are infrequent (annual, quarterly at best) and are basically paper checklists. They do not actually test if controls are working as needed. And because they are infrequent, they quickly become out of date due to the dynamic nature of IT environments. Security professionals have long known that compliance ≠ security.

The next set of tools for ensuring the effectiveness of security controls is penetration testing in various forms. These include manual or semi-automated pen tests, red team-blue team

exercises, and fully automated breach and attack simulation (BAS). A primary impediment to effective testing, however, is the impact a pen test can have on a live production network. To avoid such impacts, the tests are often limited in scope and frequency. Some tests may be restricted to only lab environments. The other issue is the tests typically focus on a specific control (such as firewall, or endpoint security). This approach does not measure overall risk to the IT system. It tells you if something is not working but does not measure the potential impact (risk) of the exposure. Testing techniques in their various forms lack system-wide coverage, are scope-limited, and are often too infrequent to keep up with changing IT environments.

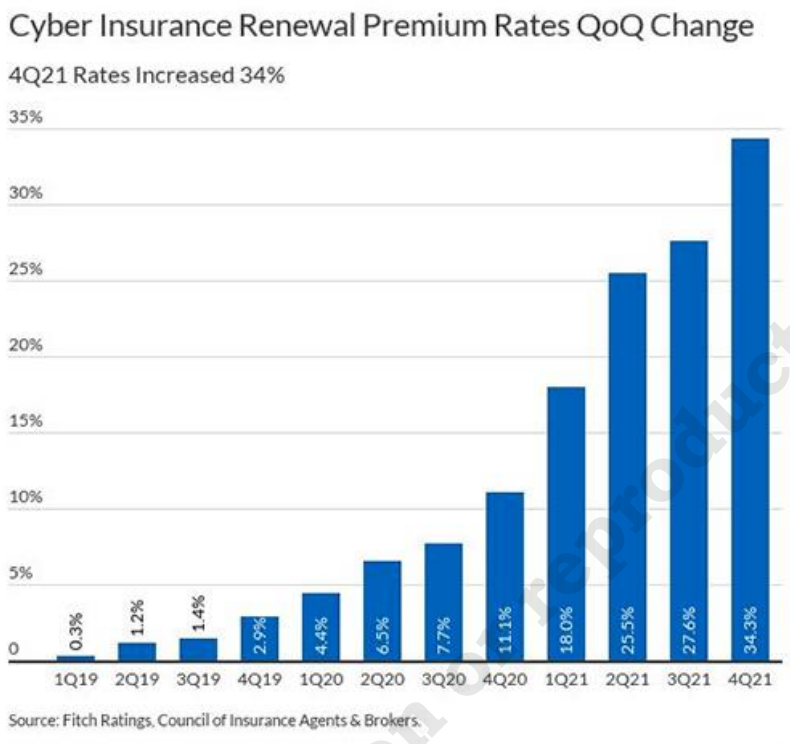

Figure 2: Quarterly change in premiums for cyber insurance

"Left of Bang" Cybersecurity Problems

There is strong evidence that organizations are falling behind in their efforts to ensure their security controls are up to date and working as needed. A look at how this is done today reveals why. Let's take a look at the major tools of the trade in this area.

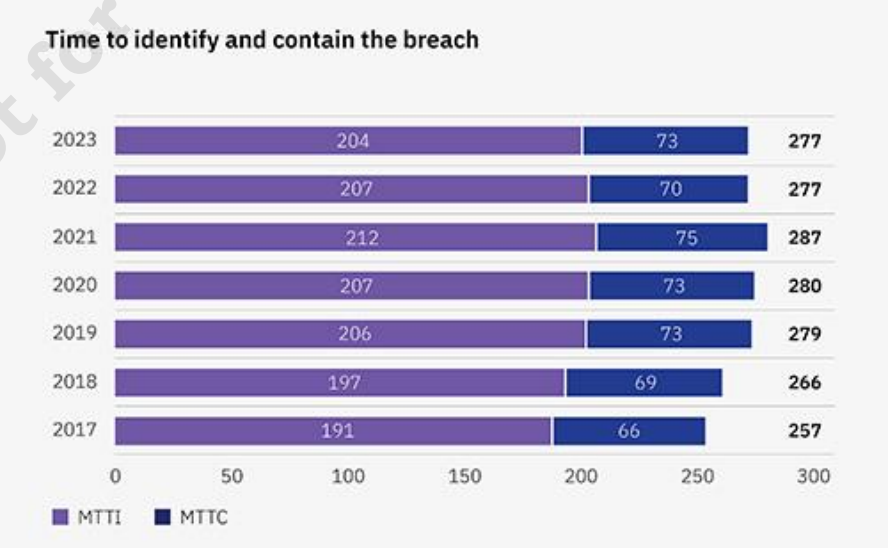

Figure 3: Time to identify and contain breaches.
Source: IBM Cost of Data Breach Report 2023

First, we have compliance audits. These audits are infrequent (annual, quarterly at best) and are basically paper checklists. They do not actually test if controls are working as needed. And because they are infrequent, they quickly become out of date due to the dynamic nature of IT environments. Security professionals have long known that compliance ≠ security.

The next set of tools for ensuring the effectiveness of security controls is penetration testing in various forms. These include manual or semi-automated pen tests, red team-blue team exercises, and fully automated breach and attack simulation (BAS). A primary impediment to effective testing, however, is the impact a pen test can have on a live production network. To avoid such impacts, the tests are often limited in scope and frequency. Some tests may be restricted to only lab environments. The other issue is the tests typically focus on a specific control (such as firewall, or endpoint security). This approach does not measure overall risk to the IT system. It tells you if something is not working but does not measure the potential impact (risk) of the exposure. Testing techniques in their various forms lack system-wide coverage, are scope-limited, and are often too infrequent to keep up with changing IT environments.

The final tool in the prevention tool bag is vulnerability management and prioritization. As you can see in (see figure 4) about 25,000 new vulnerabilities are found annually.

Organizations regularly scan their endpoints, servers, network gear, and applications to find which vulnerabilities are present in their environment, and there are almost always many more identified than can be addressed. The list must be prioritized down to a manageable workload without leaving exposures that pose a high risk to the organization. Unfortunately, an effective risk-based approach to prioritization has proven to be elusive. The risk of a given vulnerability is highly dependent on the particulars of the IT environment. It can be a significant risk in one environment but only a minimal risk in another. Prioritization systems have also not been very effective because they do not test or simulate how an attacker would exploit each open vulnerability and what damage they could do after the initial breach.

Simply put, many organizations currently lack the tools and methodologies needed for identifying, prioritizing, and remediating the cybersecurity risks in their infrastructure.

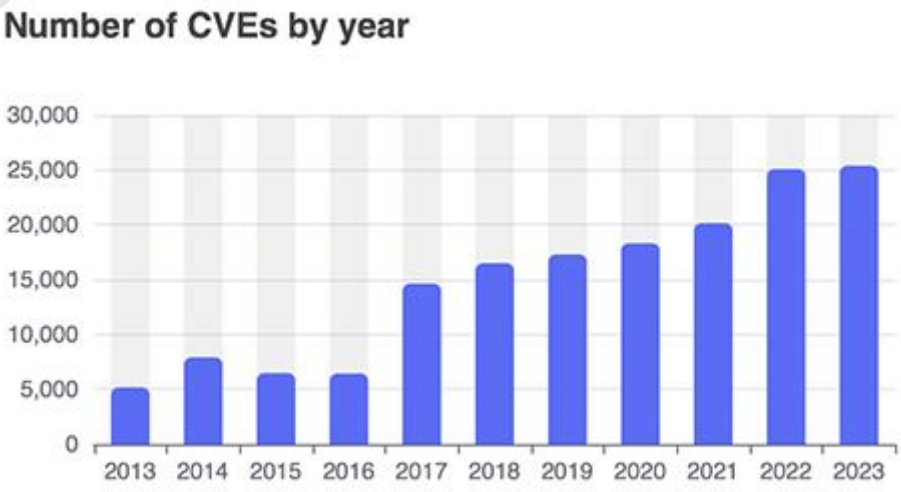

Figure 4: Number of new vulnerabilities (CVEs) reported annually.
Source: cvedetails.com

The CTEM Framework

In July 2022 security analysts at Gartner introduced a security approach or framework called Continuous Threat Exposure Management (CTEM). They identified the need for such an approach based on the issues outlined above – inadequate security testing regimes, lack of accurate risk-based prioritization, and lack of continuous assessment.

The CTEM process described by Gartner is a five-step cycle, which as the name suggests, should be carried out on a continuous basis so as to keep up with the dynamic nature of IT environments and threats. The steps to this process are:

***Scoping*:** Define the boundaries of the IT environment that will be subject to threat exposure management. This typically includes the IT estate (data centers, office environments, cloud services, remote workers), but can extend further.

***Discovery*:** Identify all the assets within scope. This includes device and software configurations, vulnerabilities, security controls, connectivity, and asset value. The process requires a system-wide approach as opposed to a collection of siloed results from vulnerability scans, audits, and pen tests.

***Prioritization*:** The goal of this phase is to identify the exposures most likely to be exploited and their potential impact on the organization. In short, the exposures must be measured in terms of likelihood and impact. This equates to risk-based prioritization.

***Validation*:** This is a testing phase where the exploitability of exposures is confirmed along with potential impact on assets. This goes beyond determining whether a given system or control can be compromised. It includes how the compromise could be leveraged (e.g., lateral movement) to gain access to high-value assets. An exploitable system may not pose a high risk if an attacker cannot leverage that system to do significant damage.

***Mobilization*:** This is the remediation phase. The previous four steps reveal a risk-prioritized list of exposures, including the details of what systems are involved and the specific attack paths an attacker would follow to leverage each exposure. This provides not only the information needed to determine what issues need to be addressed most urgently, but also the most efficient and effective ways to achieve remediation.

Like security frameworks we have seen before, this looks great on paper, but implementation is where things get difficult. CTEM is a framework/process and not a tool. However, without effective tools that address the shortcomings in how exposure management is done today, CTEM is unlikely to make a significant impact on reducing cyber risk.

In a previous Pipeline article we described the emerging use of reasoning-based AI and digital twinning technologies in cybersecurity. Reasoning-based AI attack path simulation applied holistically to a virtual cyber twin of the IT environment overcomes many of the barriers to implementing the CTEM framework. These technologies are not "CTEM in a box," but they do provide the means for organizations to implement the CTEM framework and achieve the 3X risk reduction that Gartner forecasts.