ConversationalGeek®

Conversational Continuous Threat Exposure Management

By Derek A. Smith (CCISO, CISSP) and **Dan DeCloss** (Founder, Plextrac)

In this book, you will learn:

- Why your security needs to get to a state of continuous validation
- What's missing from traditional security approaches
- How the CTEM approach works to continually secure your environment

Sponsored by PlexTrac

PlexTrac is the market leader in pentest reporting and management, empowering MSSPs and enterprises to automate and streamline their Continuous Threat Exposure Management (CTEM) lifecycle. Our platform enhances the entire risk management workflow—from identifying and prioritizing risks in a business context to tracking remediation progress and measuring security posture trends with real-time analytics.

Discover how PlexTrac can revolutionize your security operations at www.plextrac.com

Conversational
Continuous Threat Exposure Management

By Derek A. Smith

ConversationalGeek®

Conversational Continuous Threat Exposure Management

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Derek A. Smith
Project/Copy Editor:	Ian Whiteling
Content Reviewer(s):	Dan DeCloss
	Hope Goslin

Note from the Author

You've likely been tasked with *staying ahead* of cyberattacks. *That's no easy feat.* With the speed at which attack techniques are evolving, it's necessary for organizations to be as proactive in their security approach as possible. The use of pentesting and vulnerability assessments are necessary tools in an effort to mitigate an attack vector before it's used.

But it's necessary for organizations to reach beyond just being *proactive* in their security efforts and shift to a cybersecurity approach that places your organization ahead of the bad guys *every day*.

We'd typically use the term *continuous validation* to better define the efforts. This term, however, has been borrowed by industry vendors and tends to be thought of as only applying to efforts like breach and attack simulation or control validation. In reality, when applied practically using approaches like *Continuous Threat Exposure Management* (CTEM), you'll find that the practice of continuous validation applies to every aspect of your proactive security efforts as a lifecycle.

To help you get to a state of continuous validation via CTEM, this eBook will focus on the challenges with the traditional approaches to proactive security, why continuous validation enhances your organization's cybersecurity stance, and what defines CTEM and its practical application to get you there.

So, grab a cup of coffee (or something stronger) and let's dive in.

Derek A. Smith, CISSP

CTEM: Reaching a State of Continuous Validation

So, are we secure or not?

In today's rapidly evolving digital landscape, your cyber threats are more prevalent and sophisticated than ever before. The sheer volume and variety of these threats have turned your cybersecurity battlefield into a relentless game of cat and mouse, where the stakes couldn't be higher.

Reactive security continues to be the predominant focus by organizations but isn't comprehensive enough an approach to be a viable strategy in and of itself. Reactive security is the equivalent of plugging leaks in a dam with your fingers and toes, the leaks will continue to come and there are only so many fingers and toes to go around. Ultimately, the leaks will grow, and the dam will break.

Of course, the ability to detect threats and respond to them is a critical part of an organization's cyber defenses. But if that's your sole approach, you're going to need a *lot* more fingers and toes.

As an organization's understanding of cybersecurity matures, the focus begins to include *proactive* security measures, such as pentesting and vulnerability assessments. These measures shift the organization from simply responding to threats as they occur, to anticipating and preventing the potential for attack vectors before threat actors have a chance to utilize them and do any damage.

The concept of proactive security can be likened to a chess game, where the best players don't just respond to their opponent's moves — they *anticipate* them. By thinking several steps ahead, you can make strategic decisions that prevent your opponent from gaining the upper hand. In the same way, proactive security measures allow your organization to stay steps ahead of cybercriminals by identifying and addressing vulnerabilities before they can be exploited.

Since even cyberattacks involve a human element — intelligent, motivated individuals constantly seeking new ways to exploit vulnerabilities — using proactive security measures to outmaneuver cybercriminals before they act is a valid approach.

However, both reactive and proactive security measures still have a big problem.

In short, both of these traditional approaches to cybersecurity are only securing the environment *at a single point in time*. Think about it: reactive security measures are responding to something that's happening *now*; the response only continues to secure the environment in the future if a subsequent attack uses the same medium, techniques, etc.

Given the sophistication of modern cyber threats, it's clear that a reactive approach to security is woefully inadequate, requiring organizations with a mature security strategy to employ pentesting, vulnerability assessments, and other strategies as proactive measures.

For those of you already there, congratulations — you've taken the first step: shifting from *reactive* to *proactive*.

But even proactive measures aren't without their own drawbacks — the biggest of which is that they only address the state of security *when an assessment is performed*; new vulnerabilities won't be addressed until the next time the organization decides to be "proactive."

In other words, while these measures are absolutely critical, your strategy needs to evolve and shift from truly a point-in-time perspective to a *continuous state of security*.

The Real Goal: Continuous Validation

The overly simplified goal of both reactive and proactive security strategies is to *reduce risk*. And in an organization that wants to maintain as secure an environment as possible — identifying, prioritizing, and mitigating that risk is certainly key.

But the goal isn't to just optimize those strategies and get better at detecting attacks or finding vulnerabilities; it's to shift to an approach that *continuously validates* the organization's state of security as an ongoing process using a rich set of security data from multiple sources — commonly referred to as *continuous validation*.

Practically speaking, this ongoing process includes regularly testing, assessing, and verifying the security of systems, applications, and networks using disparate sets of security data from pentest tools, vulnerability scanners, attack surface management platforms, and more. By doing so, organizations gain context and are better able to prioritize remediation to ensure established security standards, compliance requirements, and business objectives are met.

And, unlike the point-in-time nature of security and vulnerability assessments, continuous validation provides real-time or near-real-time insights into an organization's security posture, enabling the rapid identification and remediation of vulnerabilities and weaknesses before they can be exploited by malicious actors.

In other words, you need to evolve your cybersecurity efforts from *reactive* to *proactive* to *continuous*.

CTEM: The Path to Continuous Validation

Continuous Threat Exposure Management (CTEM) outlines a methodical, ongoing process for identifying, assessing, prioritizing, and mitigating security threats and vulnerabilities within an organization's environment. CTEM's approach focuses on *constant* improvement and adaptation to the evolving threat landscape, ensuring that organizations maintain a persistent proactive stance against cyber threats.

In other words, the outcome of embracing CTEM is *continuous validation*.

The rest of this eBook will focus on the shortcomings of traditional security approaches to maintain a continuous state of security, introduce CTEM in practical terms, and discuss the role of proactive security measures within CTEM — all in an effort to get your organization's cybersecurity efforts to a state of continuous validation.

Let's begin by taking a look at the traditional approaches you use today and discussing why they're falling short.

There's plenty wrong with traditional approaches

Assuming you buy into the premise that the goal should be continuous validation, it's necessary to first take a look at how to improve the efficiency and efficacy of your current efforts by acknowledging what's wrong with your approach.

The periodic approach used in traditional security methods today is only so effective because it faces a number of challenges:

- An Inability to Harness a Wide Range of Data Sources — There are abundant data sources to help gather information, assess vulnerabilities, and simulate attacks. But, if there's not a way to easily leverage, in essence, *all of them*, the result is inadequate coverage of all the potential attack vectors, leaving some vulnerabilities undiscovered. This can give your organization a false sense of security (because you don't know what you don't know), believing that your systems are secure when, in fact, there are still significant risks.

- No Repeatable Test Plans — A well-defined and repeatable test plan is essential for ensuring that your assessments are comprehensive and that the results are both meaningful and consistent. Without a test plan, there's a risk that critical vulnerabilities will be overlooked or that the findings will be unreliable. This can make it difficult to replicate the test or compare results across different environments.

  Running a pentest without a defined plan breeds inconsistent testing results which, in turn, generates unreliable reporting which yields ineffective remediation. The result is an inability to know whether your organization is truly improving its security stance.

- A Lack of Scheduling — Without proper scheduling, there is little to no visibility into when scans, pentests, mitigation actions, and other activities are taking place, resulting in a lack of collaboration between teams working to potentially address the totality of risks presented by a threat actor.

- Inconsistent Reporting — Without a standardized approach to reporting, the reports generated by different tests can vary widely in terms of format, content, and quality. This can make it difficult for your stakeholders to understand the findings, validate threat exposure, and make informed decisions.

- A Lack of Contextual Prioritization — The siloed nature of findings from pentesting versus other sources of risk creates a lack of centralized detail, making it difficult for those responsible for remediation to understand the actual impact, the degree of exploitability based on scanner data, likelihood of an attack, and the overall risk to the business. These elements are essential for quantifying risk and establishing priorities and timelines for remediation.

  Remediation teams are already overwhelmed by the number of things they need to fix and are likely fixing things that don't matter (and not the things that do). Having the ability to harness *all* of your data sources would not only allow you to centralize the data, but also apply a contextual prioritization strategy to the data. This helps to augment the source-based subjective impact and risk scores with the organization's own objective criteria that aligns with the perceived business risk — key elements in creating actionable reporting.

- Ineffective Remediation — Most security teams don't own remediation. Without an ability to assign remediation ownership, it's difficult to track those activities and follow up to ensure the work was done — let alone effectively. Furthermore, it's difficult to escalate issues when the work isn't getting done.

- Difficulty in Measuring Progress — Every assessment is a point-in-time security snapshot, so they provide no visibility into measuring the effectiveness of your organization's security controls over time. Over time, each assessment's activities and findings play a role in establishing progress (e.g., is the remediation task from a test performed months ago still protecting the organization?). Without the ability to analyze findings and measure their progress over time, your organization will not be able to identify areas where improvements are needed and understand the long-term impact of your efforts.

- Little-to-No Automation — Consider all the challenges mentioned above, many of which arise because parts of the process and their outcomes are performed manually. This manual approach introduces human errors, inconsistencies, inaccuracies, and inefficiencies, which hinder the goal of gaining actionable insights to improve organizational security. As a result, remediation efforts become less impactful, creating a ripple effect that further weakens the overall security posture.

- Siloed Teams and Data — Teams across the organization are using threat intelligence (found in the forms of both security data sources and the outcomes of security assessments) to influence priorities and remediation efforts. But if each team has no idea what the others are working on, there is no concentrated effort to mitigate the risks associated with bigger threat actors like APT29, and the overall potential impact the teams have as a whole is diminished.

These challenges pose a significant threat to any organization aiming to achieve continuous validation of its environment's vulnerabilities, security controls, and defenses. They also hinder the establishment of a predictable approach to remediation, monitoring, and impact measurement.

It's time to change your approach

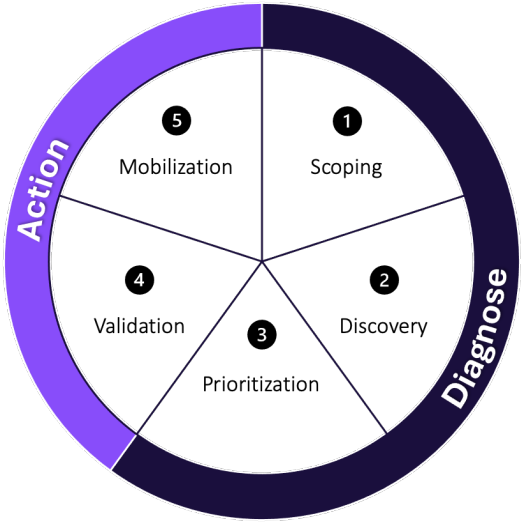
In addition to the challenges faced by proactive security measures, the periodic nature alone isn't enough to ensure an organization is secure against the latest exploits and attack techniques. What's needed is an approach that sees assessments as being a continuous process (rather than as a set of repeated one-off assessments) that takes advantage of the myriad of security data sources to identify risk, inform your test plans, prioritize across teams, and ensure timely remediation. By embracing a continuous approach, you will empower teams to quickly adapt to changes and also report on the real-time status effectively.

In other words, *it's time to adopt CTEM*.

Continuous Threat Exposure Management

CTEM is a cyclical approach that promotes continuous and proactive improvement to your security posture over time. While it's technically *not* a framework (as it lacks step-by-step guidance, policies, controls, etc.), it is a process that, when followed, creates a state of continuous validation of your organization's state of security by identifying and prioritizing vulnerabilities and exposures, providing context into the actions needed to remediate them, and reducing the organization's risk of a cyberattack.

As shown on the next page, CTEM separates the process down into two phases and five steps:



The Continuous Threat Exposure Management Cycle

CTEM's two phases separate the work of continuous validation:

1) Diagnose — This phase involves assessing and analyzing identified threats and vulnerabilities and potential risks to understand their implications within the environment. The purpose of this phase is to provide a clear, actionable overview of security gaps and exposure levels, enabling informed decision-making for targeted remediation.

2) Action — This phase focuses on implementing remediation and mitigation strategies to address the vulnerabilities and risks identified in earlier phases. The purpose of this phase is to take decisive steps to strengthen the security posture, which can include deploying security patches, updating configurations, enhancing security policies, executing targeted defensive measures, and performing analysis and reporting for visibility.

The phases break down into five distinct steps:

Diagnose

Scoping — This stage involves defining the scope of potential threats and identifying critical business assets that need protection. It helps to establish a focused approach for the rest of the CTEM process by prioritizing business risks and attack surfaces against known threat actors and their TTPs.

Discovery — In this stage, all assets and exposures, both known and hidden, are identified. The goal is to uncover vulnerabilities, misconfigurations, and security gaps — in essence, attack paths threat actors could take — across networks, applications, and systems to build a comprehensive risk profile.

Prioritizing — Not all vulnerabilities pose equal risk. This stage prioritizes exposure based on factors like exploitability, impact, and criticality to the organization. It ensures that the most severe risks are addressed first, optimizing resource allocation.

Action

Validation — This phase involves testing and validating whether the identified exposures can be exploited and how they may affect the organization. Techniques like red teaming and attack path simulations are used to refine the prioritization process and verify remediation strategies to determine which security controls or mitigation actions are working.

Mobilization — The final stage focuses on making the findings actionable by mobilizing teams to implement remediations and reduce vulnerabilities. This includes establishing ownership, cross-team collaboration, and accountability to ensure the job gets done as well as ensuring that business leaders are engaged in the process for continued security improvements.

This cyclical approach allows organizations to continuously refine their security posture and respond more effectively to emerging

threats in real time, making it a comprehensive and forward-thinking strategy for cybersecurity management.

CTEM was first introduced by Gartner in 2022 as a strategic approach designed as the foundation for companies aiming to minimize risks and significantly reduce the number of information security incidents.

So, What Needs to Change to Get to Continuous Validation?

Proactive security measures play a clear role within CTEM and continuous validation efforts, sitting firmly within the *Discovery* and *Validation* steps. But the remaining steps make it clear that the answer does not rest with the act of performing a pentest, building a report, and handing it off to someone in Security.

So, it's necessary to address any of the previously identified challenges associated with traditional pentesting methods that apply to your organization — but with a slightly larger focus. Most of those challenges actually apply to some degree to the steps within the CTEM approach, keeping organizations from reaching a state of continuous validation.

Practically speaking, you can start with improving what you already know:

- Leverage a wide range of data sources including vulnerability scans, risk assessments, pentests and more
- Use the gathered threat intelligence to inform test plans, assess new vulnerabilities, and simulate attacks
- Establish well-defined and repeatable test plans to create standardized testing

- Establish visibility into the scheduling of activities and engagements to ensure proper cross-team communication and collaboration

- Create consistent reporting with contextual risk scoring so reports become instantly valuable

- Find ways to make sure reports are delivered to those responsible for remediation to ensure a proportional response

- Be able to measure progress of the efforts to create a feedback loop for continuous improvement

Next, take a *step back and look at CTEM's larger process of reducing risk* and begin to approach risk in a far more comprehensive and continual way.

At some point, it will become evident that automation is needed to create the efficiencies and consistency necessary for the entirety of CTEM to be effective. So, the next step is to incorporate AI and automation into your efforts. AI-based automation can be used to address the challenges mentioned in a number of ways to move your organization toward continuous validation:

1. Performing the tasks you currently can't — Take the example of all those disparate security data sources previously mentioned that your pentesters don't necessarily have access to and, therefore, are never going to fully check, correlate, and let dictate assessment and remediation priority. Automation can first be used to ingest, correlate, and normalize the data, creating a richer and more useful data set. Secondly, automation can leverage external threat intelligence sources to support proper prioritization of efforts.

2. Automating the tasks you can (but probably shouldn't) — AI and automation can be used to perform, in essence, any repeated task, offloading routine tasks, such as vulnerability scanning and report generation, freeing up IT and security teams to focus on more assessment and remediation efforts. Automation also will ensure consistency and predictability in each task, resulting in overall improvements in vulnerability management efficacy.

3. Querying AI to make quick decisions — We're on the cusp of seeing interactive querying of your rich security data with AI becoming a mainstream feature of solutions that assist with continuous validation. Think of this as an iterative process with the security team member asking questions to help identify and prioritize risks, quickly providing insight into what action should be taken.

4. Improving prioritization — Assuming the AI in question has access to your comprehensive risk profile, it can likely do a much better job of risk scoring and establishing which issues to address first.

5. Connecting the tasks into a repeatable process — Each of these processes your team currently performs uses its own tools, data sets, applications, and platforms. Automation is the key to integrating all of this into a unified process.

6. Report on trends over time — AI can be used to track and analyze testing failures and successes over time, providing visibility into improvement trends

The end result is an intelligent and automation-driven continuous validation process that works to ensure the organization remains in a *constant state* of the highest degree of security possible.

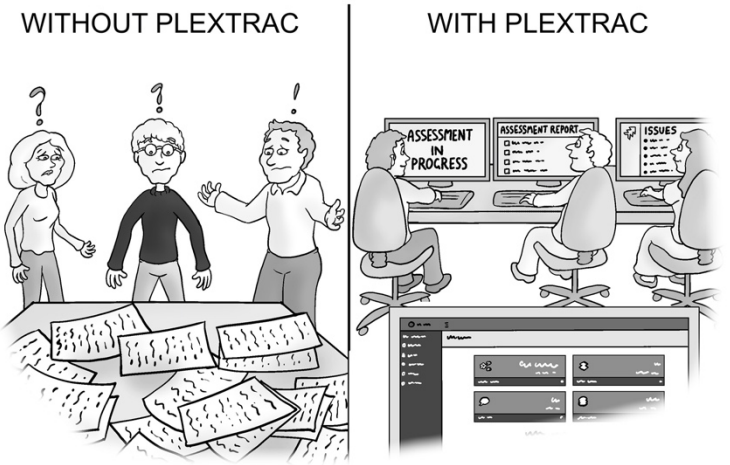
The Big Takeaways

Cybersecurity is a journey, not a destination. Your threats are ever-evolving, and so must your defenses. The days of waiting for an attack before taking action are long gone. In today's fast-evolving threat landscape, your proactive security measures are essential. Pentesting has historically been one of the key components that allows your organization to simulate cyberattacks on your systems, identify vulnerabilities, and take corrective action before an actual attack occurs.

However, to be truly effective, security assessment and remediation must evolve into a continuous validation process that generates actionable and understandable insights on a continuous basis to reflect the threat landscape in real-time.

By addressing the challenges found within proactive security processes while embracing frameworks like CTEM and the use of AI and automation, those responsible for the organization’s state of security will better understand how effective their efforts are in real-time, as well as how secure the organization *really* is against actual attacks.

PlexTrac: Empowering Continuous Threat Exposure Management



As cybersecurity threats continue to grow in volume and sophistication, organizations face constant pressure to stay ahead of potential vulnerabilities. Manual pentesting and traditional security assessments, while essential, often fail to keep pace with the continuous barrage of emerging threats. Cybersecurity teams are left with fragmented data from multiple sources, delayed response times, and a lack of strategic prioritization for remediation efforts. In today's landscape, achieving a Continuous Threat Exposure Management (CTEM) lifecycle is more important than ever, providing organizations with the ability to proactively manage and mitigate risks over time.

This is where PlexTrac, a leading cybersecurity platform, steps in. PlexTrac was born out of a desire to address the specific pain points experienced by security teams, particularly those performing pentests and vulnerability assessments and other proactive efforts.

PlexTrac not only streamlines the reporting and remediation process but also automates key workflows, allowing organizations to move toward a true CTEM framework.

This chapter will explore how PlexTrac's platform solves the challenges of manual testing and vulnerability management while providing security teams with the tools they need to continuously improve their security posture.

Improving the Process of Security with PlexTrac

PlexTrac is a comprehensive platform designed to automate and streamline the lifecycle of cybersecurity assessments, enabling organizations to achieve continuous threat exposure management. With a focus on reporting, collaboration, and risk management, PlexTrac facilitates the work of pentesters, red teams, and security directors by centralizing and automating the entire process. Below are the key features that make PlexTrac a standout solution:

- Automated Reporting and Collaboration — PlexTrac reduces the manual labor involved in creating reports for security assessments, including pentests, red teaming, and vulnerability scans. The platform allows security professionals to generate detailed, dynamic reports that integrate findings from multiple sources.

- Centralized Vulnerability Management — By bringing together data from various tools such as vulnerability scanners, pentest automation suites, and more, PlexTrac offers a unified view of security risks, enabling teams to prioritize remediation efforts more effectively.

- Contextual Risk Scoring — PlexTrac's flexible risk scoring system helps produce accurate risk prioritization by allowing organizations to customize how vulnerabilities are assessed

based on the context of their business, using both subjective and objective criteria.

- Bi-Directional Ticketing System Integration — PlexTrac integrates seamlessly with ticketing systems such as JIRA and ServiceNow, enabling bi-directional data synchronization. This feature allows security teams to track remediation efforts in real time, ensuring issues are addressed and verified before closure.

- Continuous Threat Exposure Management (CTEM) Enablement — PlexTrac supports the implementation of a CTEM lifecycle by automating key workflows and providing continuous visibility into security posture over time. Security teams can track progress, identify priority items, and benchmark performance against industry standards.

- Customizable Reporting Templates — PlexTrac offers the ability to export custom-branded reports, allowing security providers and internal teams to maintain their established documentation formats while benefiting from the platform's automation capabilities.

- Analytics and SLA Monitoring — PlexTrac provides insights into an organization's progress over time, tracking the status of open vulnerabilities, adherence to SLAs, and remediation trends. This ensures teams can focus on the most critical issues and measure improvement over time.

Addressing Security Challenges

PlexTrac addresses the specific challenges that security teams face in traditional pentesting, vulnerability management, and exposure management, offering clear outcomes that improve efficiency, accuracy, and collaboration.

Reduced Time in Reporting and Collaboration

One of the most significant pain points for cybersecurity professionals is the time-consuming process of writing and updating reports. Manual report writing often results in wasted hours, duplicated efforts, and outdated data that doesn't provide actionable insights. PlexTrac solves this by automating much of the reporting process. Teams can quickly generate comprehensive reports that consolidate findings from various sources, making the collaboration between security and IT teams smoother and faster. The platform also allows for the direct assignment of issues to the responsible team members, creating a more dynamic and efficient workflow.

Improved Remediation Tracking and Workflow Efficiency

A common frustration is the inability to track and prioritize the remediation process effectively. PlexTrac addresses this via an ability to track issues within the platform or across multiple ticketing systems using its bi-directional integration to ensure that when an issue is assigned to a team member, the issues' status is continuously updated within PlexTrac real-time. This integration allows security teams to monitor the progress of each finding, ensuring that nothing slips through the cracks. Additionally, the platform's SLA monitoring feature helps organizations ensure that vulnerabilities are addressed within required timeframes. PlexTrac facilitates the validation of fixes before issues are closed, providing an extra layer of assurance.

Prioritization of High-Risk Vulnerabilities

Security teams are often overwhelmed with data from multiple sources, making it difficult to determine which issues should be prioritized. PlexTrac's contextual risk scoring system enables organizations to tailor and standardize their prioritization based on their specific risk landscape. By providing an objective framework that incorporates subjective business context, PlexTrac ensures that high-priority issues — such as vulnerabilities affecting critical business systems or regulatory compliance — are addressed first.

This targeted approach helps improve the overall security posture while optimizing resource allocation.

Facilitation of a Continuous Threat Exposure Management (CTEM) Lifecycle

The ultimate goal of any security team is to create a continuous security improvement loop. PlexTrac's comprehensive features enable organizations to move beyond annual pentests and static reports, pushing them toward a CTEM model. By integrating data from multiple assessment tools and automating remediation workflows, PlexTrac allows organizations to continuously monitor their security posture and make informed decisions in real time. Over time, this leads to a measurable improvement in risk mitigation and a proactive rather than reactive security strategy.

Enhanced Analytics for Strategic Decision Making

Security leaders often struggle to demonstrate their team's progress to executives or stakeholders. PlexTrac's robust analytics and reporting tools provide a clear, quantifiable view of an organization's security posture. The platform's dashboards and trend analysis tools allow security directors to track key metrics such as mean time to remediation and SLA compliance. This level of insight helps organizations measure the effectiveness of their security programs, identify areas for improvement, and benchmark their performance against industry peers.

Seamless Integration Across Tools and Teams

PlexTrac's ability to bring together data from a variety of cybersecurity tools — including vulnerability scanners, automation suites, and ticketing systems — ensures that organizations have a holistic view of their security risks. This centralization not only streamlines workflows but also enhances collaboration between teams, breaking down the traditional silos between security and IT operations. By fostering real-time communication and shared

responsibility, PlexTrac improves both the speed and effectiveness of remediation efforts.

Putting You on the Path to CTEM

In an era of escalating cyber threats, cybersecurity teams need more than just tools for manual pentesting and vulnerability management—they need a comprehensive solution that supports a Continuous Threat Exposure Management (CTEM) lifecycle. PlexTrac provides exactly that, enabling organizations to automate reporting, streamline remediation, and prioritize risks in a way that aligns with their business context. Through its innovative features and a focus on collaboration and efficiency, PlexTrac helps security teams not only keep up with today's threats but also build a proactive, continuously improving security posture for the future.

The Big Takeaways

PlexTrac offers cybersecurity teams a powerful platform to address the critical challenges of manual pentesting, security assessments, and vulnerability management. Founded by Dan DeCloss to solve the inefficiencies and frustrations he experienced firsthand in the security industry, PlexTrac automates reporting, integrates data from multiple tools, and streamlines remediation workflows. Its key features include automated reporting, centralized vulnerability management, contextual risk scoring for more accurate prioritization, and bi-directional ticketing integration, all of which facilitate collaboration and drive efficiency. The platform enables organizations to adopt a Continuous Threat Exposure Management (CTEM) lifecycle, moving from a reactive to a proactive security approach.

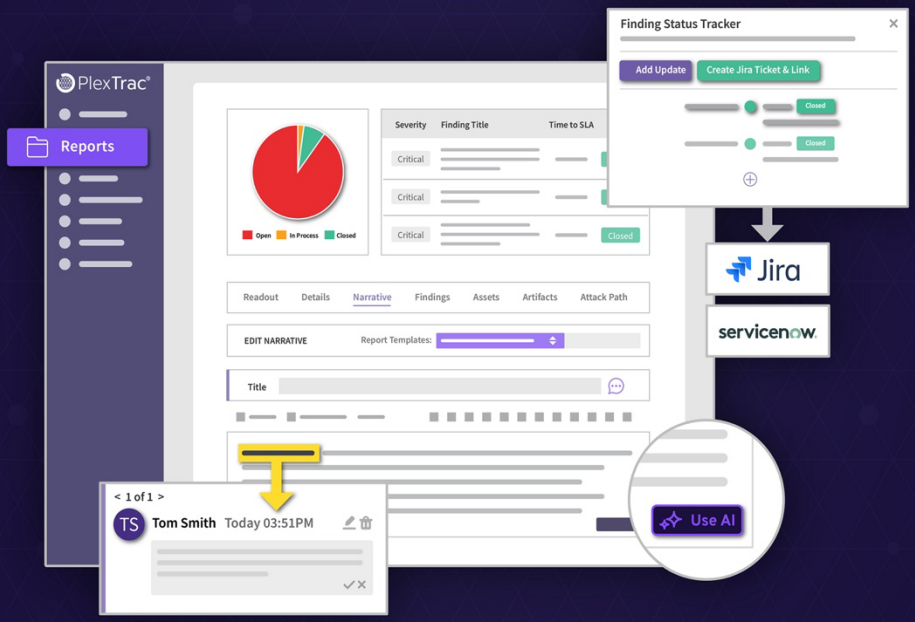
By centralizing and automating processes, PlexTrac reduces the time spent on manual reporting and offers enhanced analytics for strategic decision-making. Teams are empowered to prioritize high-risk vulnerabilities, track remediation progress, and maintain compliance with SLAs. PlexTrac integrates seamlessly with existing tools, ensuring continuous visibility and coordination between security and IT operations. Ultimately, PlexTrac supports organizations in improving their security posture over time, making it a vital tool for managing today's complex cybersecurity landscape.

Visit Plextrac's website at plextrac.com to learn more about their platform, designed to automate security assessments and streamline remediation efforts—empowering organizations to adopt a proactive approach to cybersecurity.

PlexTrac®

The #1 AI-Powered Pentest Management and Reporting Platform

PlexTrac automates pentest and vulnerability reporting, integrates data from multiple tools, and streamlines remediation workflows.



Book a Demo

Contact Us

Quickly become conversational about Continuous Threat Exposure Management (CTEM).

As the threat landscape continually evolves, organizations need to do the same with their threat management, shifting from point-in-time assessments to a state of continuous validation. In this eBook, we'll cover why traditional approaches to security validation no longer are sufficient and introduce CTEM as the best approach to ensuring the organization remains continually secure.

About Derek A. Smith

With over 30 years in the security industry, Derek A. Smith is a former government agent, cybersecurity SME, holds a variety of certifications (CISSP, CEH, CCISO, Security+, etc.), eight college degrees, is a published author, conference speaker, cybersecurity analyst for several international and local television news stations, government program manager, and more.