TIDAL CYBER®

THREAT-INFORMED DEFENSE

Tidal Cyber and BAS: Get More From Your Tests

Tidal Cyber Breach and Attack Simulation (BAS) Tool Integration

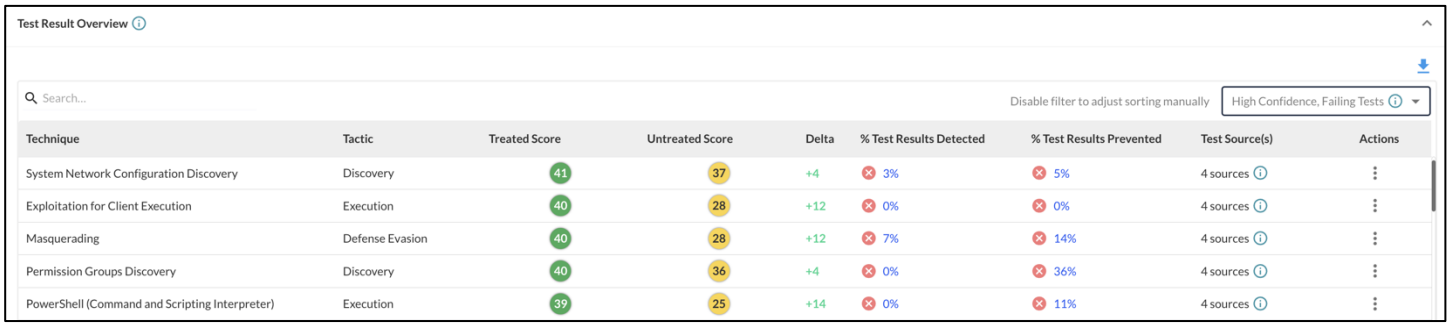
TIDAL CYBER

THREAT-INFORMED DEFENSE

Breach and Attack Simulation (BAS) Tool Integration

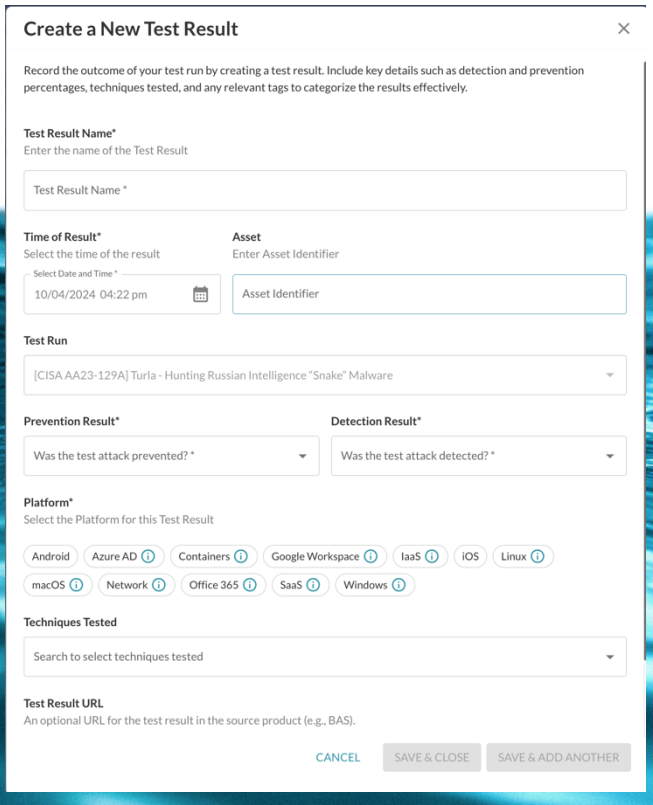
Tidal Cyber Enterprise Edition is the first and only CTEM / TID vendor to complete the Threat-Informed Defense cycle by adding the ability to integrate with Breach and Attack Simulation (BAS) tools to incorporate BAS testing and evaluation results, empowering visibility into the true state of defenses and where to target future tests with the most impact.

With these integrations, security teams gain increased confidence in knowing their threat intelligence and defensive measures align to provide the greatest possible protection for their enterprise assets, all while maximizing current security stack investments.



Test results can be supplied by:

- A BAS tool
- Manual data entry via the Tidal Cyber Enterprise Edition user interface
- Using the Tidal Cyber Enterprise Edition application programming interface (API)



Get More From Your Tests

Enterprise Edition provides empirical feedback and insights on your defensive capabilities and your Confidence Score not possible with any other product in the market today, allowing users to quickly and easily answer these critical questions:

- Where are my defensive capabilities not working as intended?
- Where can I improve the accuracy of my defensive stack model?
- Where are my defenses weakest?
- What should I test next?
- What defenses can my team confidently take credit for?

TIDAL CYBER®

THREAT-INFORMED DEFENSE

Tidal Cyber Enterprise Edition answers these questions with the Test Results Overview on the Coverage Map Dashboard:

Where are my defensive capabilities not working as intended?

Testing your defenses and reviewing the results in Tidal Cyber Enterprise Edition lets you identify and act on possible implementation failures and improvements in your defenses. The Tidal Cyber Test Results Overview shows behaviors where your security controls may not be working as intended and allows you to investigate why the test is failing.

If the test is misconfigured, you can fix the test configuration and re-run the test in the BAS product. If the test has correctly identified a control failure in your environment, fix the control and re-run the test.

TEST RUNS   TEST RESULTS

Process Injection

Test Result Name	Test Run	Asset	Source	Platform	Prevention	Detection	Techniques Tested
Code Injection via Load Library and Create Remote Thread	Red Canary 2022 Threat Detection Report - Top Techniques	EC2AMAZ-2F8DLJE	INTEGRATION-ATTACKIQ	Windows	FAIL	OTHER	Process Injection,
Code Injection via Load Library and Create Remote Thread	Red Canary 2022 Threat Detection Report - Top Techniques	EC2AMAZ-2F8DLJE	INTEGRATION-ATTACKIQ	Windows	FAIL	OTHER	Process Injection,
Code Injection via Load Library and Create Remote Thread	Red Canary 2022 Threat Detection Report - Top Techniques	EC2AMAZ-2F8DLJE	INTEGRATION-ATTACKIQ	Windows	FAIL	OTHER	Process Injection,

Where can I improve the accuracy of my defensive stack model?

Unexpectedly successful tests can help you build and improve the model of your defenses in Tidal Cyber Enterprise Edition. The defenses can be reviewed for each behavior that detected or prevented the simulated attack.

Test Result Overview

Search...   Disable filter to adjust sorting manually   Low Confidence, Passing Tests

Technique	Tactic	Treated Score	Untreated Score	Delta	% Test Results Detected	% Test Results Prevented	Test Source(s)	Actions
Steal or Forge Kerberos Tickets	Credential Access	24	14	+10	0%	100%	4 sources	⋮
Phishing	Initial Access	26	18	+8	0%	100%	4 sources	⋮
Kerberoasting (Steal or Forge Kerberos Tickets)	Credential Access	27	17	+10	0%	100%	4 sources	⋮
LSA Secrets (OS Credential Dumping)	Credential Access	28	19	+9	0%	100%	4 sources	⋮

TIDAL CYBER

THREAT-INFORMED DEFENSE

Where are my defenses weakest?

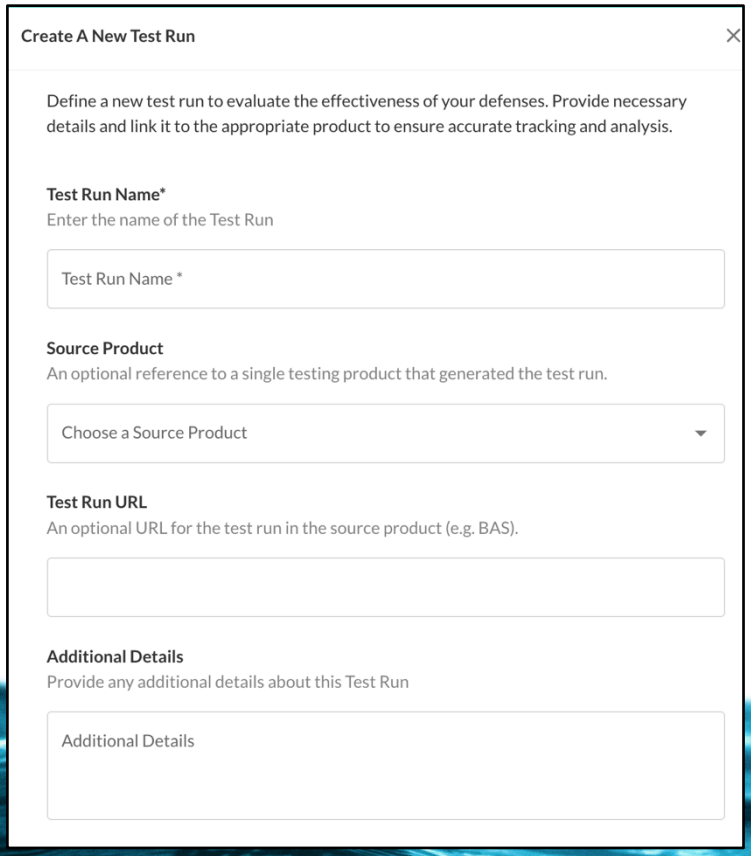
When the analytical analysis and the empirical results from testing agree you have a real problem, Tidal Cyber Enterprise Edition identifies these situations, builds support internally for addressing them, and confirms they are fixed.

What should I test next?

With thousands of scenarios you can run and more you can build, most organizations have limited staff time to run BAS tests and triage the results. Tidal Cyber Enterprise Edition helps you prioritize testing the behaviors where you have the weakest defenses before attackers find out for you.

What defenses can my team confidently take credit for?

It's easy to focus on the gaps and risks, but you also need the ability to report on what you've achieved. Tidal Cyber Enterprise Edition gives you a list of behaviors where the analysis and the empirical tests agree that you are well defended and where your defenses have improved over time.



Better Together- Getting Started with Enterprise Edition

Tidal Cyber Enterprise Edition and BAS have always been better together, and with this integration, users of both can gain the effective defenses and efficient operations provided by the Threat-Informed Defense continuous feedback loop.

Contact Tidal Cyber at tryenterprise@tidalcyber.com or tidalcyber.com to learn how to get started or to take a demo and see the integration in action.