No.58
August 10th, 2022

HardenStance Briefing
Trusted research, analysis & insight in IT & telecom security

PUBLIC/UN-SPONSORED

Tidal Cyber’s Community Edition is GA

- Tidal Cyber has announced the General Availability (GA) of its Community Edition at BlackHat. The Enterprise edition is targeted for GA later this year.
- Tidal Cyber’s ‘Threat Informed Defence’ SaaS platform makes it a lot easier for security operations teams to adjust their organization’s security posture and defend against relevant threats based on TTPs featuring in the MITRE ATT&CK Framework.
- Other cyber security vendors should welcome Tidal Cyber as a valuable ecosystem partner that can help customers extract a lot more value from their own products.

If you’ve come across a more differentiated and potentially impactful cyber security start up than Tidal Cyber in the last six months, please let HardenStance know - because we haven’t. The data and tools the MITRE ATT&CK Framework provides for understanding the Tactics, Techniques and Procedures (TTPs) of the major cyber threat actors is respected, even revered, by the security operations ‘cognoscenti’. But that whole ‘cognoscenti’ thing is also ATT&CK’s biggest shortcoming. ATT&CK is undoubtedly brilliant but it’s complex. In fact it can be very difficult for many infosec professionals to get their heads around it – and especially to act effectively on it.

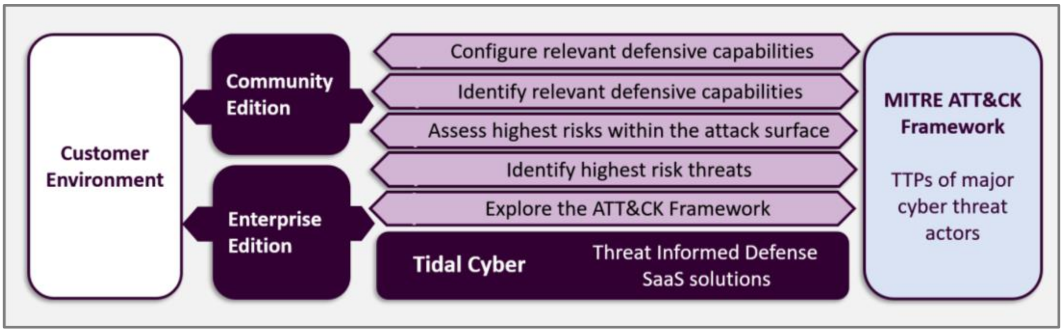
ATT&CK is brilliant but it’s complex. It can be very difficult for many information security professionals to get their heads around it – and especially to act on it.

Mapping Security Posture Dynamically to the ATT&CK Framework

It’s one thing to know that a specific threat actor or group of threat actors could be targeting your business and to understand their TTPs. It’s another thing altogether to extrapolate from that exactly what specific actions a security team can take within its unique environment to defend against that threat.

Tidal Cyber’s ‘Threat Informed Defence’ SaaS platform enables organizations to explore the threat intelligence from ATT&CK, identify the directly relevant behaviours, and identify security solutions and configurations that can protect against, detect, respond or test them. The free Community Edition becomes Generally Available (GA) with effect from Wednesday August 10th (during BlackHat). You can access the platform via this link here (see also "More Information" at the end of this Briefing). The Enterprise edition is planned to go GA later this year.

Figure 1: Threat-Informed Defence: Tidal Cyber’s Value Proposition


Customer Environment
Community Edition
Enterprise Edition
Configure relevant defensive capabilities
Identify relevant defensive capabilities
Assess highest risks within the attack surface
Identify highest risk threats
Explore the ATT&CK Framework
Tidal Cyber
Threat Informed Defense SaaS solutions
MITRE ATT&CK Framework
TTPs of major cyber threat actors

Source: HardenStance

Tidal's Founders are Uniquely Placed to Make ATT&CK Easier to Use

All three of Tidal Cyber's founders previously spent several years working for MITRE. **Rick Gordon**, CEO, was Managing Director of Programs; **Richard Struse**, CTO, was Co-Founder of MITRE's Centre for Threat Informed Defence (as well as father of the STIX and TAXII cyber threat intelligence standards); **Frank Duff**, Chief Innovation Officer, was founder of the MITRE ATT&CK Evaluations.

Their backgrounds render the Tidal Cyber leadership team uniquely well placed to understand the challenges that most security teams face in extracting value from the ATT&CK Framework and applying that intelligence to harden their security posture. On the all-important human side, their backgrounds have given the founders very high profiles among leading CISOs and other infosec practitioners as well as leading vendors. Their rich pedigree with MITRE tends to make the founders highly trusted in many of those key user and vendor circles – a valuable commodity in cyber security circles.

Towards 'Threat Informed Defence'

Drawing on a term first used within MITRE, Tidal Cyber has positioned its SaaS solutions as a "Threat Informed Defence" platform and hopes to see the term adopted as a new cyber security product category. The tailoring or customizing of Threat Informed Defence to an organization's unique environment makes it complementary to traditional vulnerability management-driven approaches which tend to be more generic. Because of the endless daily cycle of vulnerabilities that crop up – as well as the sheer volume of them – the case for Threat Informed Defence is that, on its own, vulnerability management does nowhere near enough to prioritize fixes relative to the degree of risk a vulnerability poses to an organization's unique threat surface. The pretty compelling rationale is that combining the two drives much better cyber security outcomes.

As can be seen from viewing the Community Edition, Tidal Cyber brings together the TTPs from the ATT&CK Framework with objects such as threat groups and software associated with specific malicious behaviours as well as open source and commercial tools that are capable of detecting or mitigating those threats. The platform also shows whether that defensive capability is on default or must be configured.

Check Point, Cybereason, and SentinelOne have also committed to joining the Product Registry. Their data will be integrated into the Community Edition shortly.

Sub-Optimal Configurations are All Too Common

The value can hardly be overstated. It's not just that it takes a lot of pretty rarefied expertise to stay on top of the latest, most relevant, threat behaviours. Or that it takes more knowledge to be up to speed on which specific vendor products can protect against them. Beyond that, at the point of wanting to actually implement a fix, it takes still more expertise to know exactly how a given vendor's product should be configured to ensure the most critical features are switched on. Ask customers. Ask vendors. A lot of security products in live production are running configurations that are sub-optimal relative to the user organization's own risk profile.

Vendors serving several product categories should welcome collaborating with Tidal Cyber. By ingesting and integrating the latest capabilities and configurations of multiple vendors, Tidal can become a single source of truth that's trusted by users as well as vendors because the platform helps customers extract more value from their products.

Solution providers whose product capabilities are available in Tidal's Community Edition at launch include: Atomic Red Team, AttackIQ, BreachBits, BluVector, Picus, Remediant, SCYTHE, Sysmon Modular, and Trinity Cyber. A number of other solution providers, including Check Point, Cybereason, and SentinelOne have also committed to joining the Product Registry. Their data will be integrated into the Community Edition shortly. Vendors are not charged anything for featuring on the platform.

Tidal Cyber wants the Community edition to be a high value tool through which users can more easily engage with the detailed knowledge in the MITRE ATT&CK Framework, derive actions from it, and then deploy them in their environment. With a free account, users can explore Tidal Cyber, label and save their work, come back to it and extend it. They can exploit the analytics within the tool - all for free. Users can also explore the platform without an account if they prefer.

The paid enterprise edition, due out later this year, will charge customers for more advanced features. Charges will be triggered at the point where customers start wanting to put significant effort into encoding information about their environment into the platform to arrive at more granular, real-time, custom mapping of pain points, solutions and configurations. Where users want to extend the picture they build up of their environment with their own proprietary data, these capabilities will also be exclusive to the enterprise edition. Examples might include data on observations of localized threats, threats not covered by ATT&CK, or records of red team investigations. ■

More Information

- Tidal Cyber's Community Edition: www.tidalcyber.com/communityedition
- HardenStance Briefing: "Threat Intel in Telecoms (TTIS2022)" (July 2022)
- HardenStance Briefing: "MITRE's ATT&CK Evals are out: Cheers!" (May 2020)
- HardenStance Briefing: "New STIX and TAXII Releases Approved" (April 2020)
- HardenStance received no payment - whether direct or in-kind - for publishing this Briefing.
- Register for **free email notifications** when HardenStance publishes new content.
- www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.