



Threat-Informed Defense Managed Services

Summary

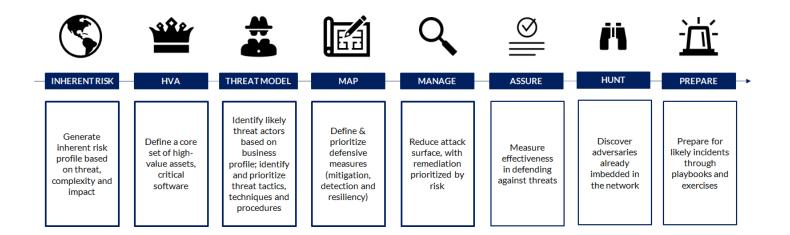
Security teams continually tune their cyber defenses against threat behaviors that are most likely to attack them. However, keeping pace with rapidly evolving threat groups and the hundreds of tactics, techniques and procedures (TTPs) they employ is difficult. Understanding whether currently-deployed security products can defend effectively against those TTPs is even harder. Accurately assessing which of the thousands of capabilities available from hundreds of vendors can best defend against those TTPs has also been a challenge for even the largest of security organizations.

Through its partnership with Tidal Cyber, The Chertoff Group is solving this problem. By leveraging the Enterprise Edition of Tidal Cyber's platform, The Chertoff Group can continually deliver threat-informed defense as a managed service to help its organizations:

- Understand which TTPs matter most as adversaries behaviors evolve;
- Rapidly assess whether existing security products and capabilities adequately cover those evolving TTPs; and
- Identify solutions that address critical coverage gaps as they emerge.

The Chertoff Group Approach

The Chertoff Group helps organizations develop comprehensive threat-informed defense strategies and operating models that provide direction and repeatability for safeguarding businesses and their customers from key cyber-related risks. The Chertoff Group's threat-informed defense operating model service incorporates these principles through the following elements:







The Chertoff Group's approach leverages its expertise combined with the MITRE Corporation's <u>ATT&CK</u> framework. ATT&CK is the most comprehensive, authoritative approach to mapping of threat actors to tactics, techniques and procedures (TTPs) openly available today.

The Chertoff Group's approach is anchored in core cyber resiliency strategic design principles like focusing on common critical assets; supporting agility and architecting for adaptability; reducing attack surfaces; assuming compromised resources and expecting adversaries to evolve. Taken together, these design principles are intended to reduce the occurrence of threat activity and the potential severity of impacts.

In doing so, The Chertoff Group helps clients isolate the following issues and answer these persistent questions:

- 1. What are we being asked to defend? The Chertoff Group ensure strategies and operating models are informed by a comprehensive understanding of inherent risk and the attack surface, with a particular focus on high-value assets.
- 2. What are we being asked to defend against? ATT&CK serves as the foundational framework and knowledge-base for mapping threats to attack-surface-specific defenses.
- 3. How do we go about it? We use a capability development framework to map capability needs to resources required to address those needs, and then build a program that can scale based on the scope of the organization.

Leveraging Tidal Cyber's Enterprise Edition to Keep Pace with Adversary Evolution

Tidal Cyber's Enterprise Edition enables security organizations to gain continuous visibility into their operational security posture relative to all key threats at scale through the implementation of:

Threat Profiling and Coverage Mapping

Threat Profiling enables security operators to add and automatically track the behavioral evolution of multiple important threat objects (groups, malware families, campaigns) that are likely to attack a given enterprise. Leveraging MITRE ATT&CK and other threat intelligence sources, Tidal Cyber maintains an updated perspective on the TTPs that are likely to be employed by that threat object. The platform gives security organizations the ability to weight each TTP based on the relative risk associated with the behavior.





Initial Access	30 Execution	22 Persistence	30 Privilege Escalation	80 Defense Evasion	5 Credential Access	33 Discovery	20 Lateral Movement	39 Collection	27 Command and Control	29 Exfiltration	29 Impact
Drive-by Compromise 34	Command and Scripting Interpreter 46 (5)	Account Manipulation	Abuse Elevation Control 23 Mechanism (2)	Abuse Elevation Control Mechanism (2)	Brute Force (2) 34	Account Discovery 36 (2)	Exploitation of 26 Remote Services	Archive Collected 27 Data (1)	Application Layer 27 Protocol (3) 27	Data Transfer Size 32 Limits 32	Account Access 13 Removal
Exploit Public- Facing Application	JavaScript 36	BITS Jobs 47 Boot or Logon Autostart	Bypass User Account @ Control	Bypass User Account Control	Password 32 Cracking	Domain Account 36	Remote Services (5)	Archive via Utility 20	DNS 29	Exfiltration Over Alternative Protocol (1) 36	Data Destruction 34
External Remote 24 Services	PowerShell 49 Python 23	Execution (1)	Sudo and Sudo Caching 28	Sudo and Sudo Caching 30	Guessing 29	Email Account 25	Distributed Component Object Model	Automated 24	File Transfer Protocols 20	Exfiltration Over Symmetric	Data Encrypted for 30 Impact
Phishing (2) 34	Visual Basic 34	Registry Run Keys / Startup Folder	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (2)	Application Window 26 Discovery	Remote Desktop 39 Protocol	Collection Session	Data Encodine (1)	Encrypted Non-C2 36 Protocol	Defacement (1) 36
Spearphishing 31	Command Shell	Create Account (1) 31	Make and	Make and	Credentials from 1	Debugger Evasion 20	SMB/Windows 40	Hijacking Data from	Standard 🚗	Exfiltration Over C2 00 Channel	Internal Defacement 34
Spearphishing 31 Link	Exploitation for Client Execution 32	Local Account 31	Impersonate Token 28 Parent PID Spoofing 28	Parent PID	Password 19	Discovery 33	SSH 4	Information 33 Repositories (1)	Encoding	Exfiltration Over Other 31 Network Medium (1)	Endpoint Denial of Service
Replication Through 18 Removable Media	Inter-Process Communication (1)	Create or Modify System 35 Process (1)	Token Impersonation/Theft	Spoofing Token Impersonation/Th (1)	Input Capture (2) 18	Discovery 35	Remote 39 Management	Sharepoint 31	Data Obfuscation (1)	Exfiltration Over 31	Inhibit System 35 Recovery
Supply Chain 10	Component Object Model 36	Windows Service 🛛 🚳	Boot or Logon Autostart Execution (1)	eft	Credential API Hooking	Network Service 30 Discovery 30	Remote Service Session Hijacking (2)	Data from Local 35 System	Protocol Impersonation 32	Bluetooth .	Network Denial of 38
Valid Accounts (3) 35	Native API 12	Event Triggered 23 Execution (1)	A Registry Run Keys/	BITS Jobs 4	Keylogging 28	Network Share 20 Discovery	RDP Hijacking 23	Data from Network 26 Shared Drive	Dynamic Resolution (1)	Physical Medium (1) 31	Service Stop
Default Accounts	Scheduled Task/Job 49	Windows Management	Startup Folder	Deobfuscate/Decode 19	Network Sniffing 35	Network Sniffing 29 Peripheral Device	SSH Hijacking 27	Data Staged (2) 36	Domain Generation Algorithms	Exfiltration over 27 USB	System Shutdown/Reboot
Domain Accounts 26	Scheduled Task 15	Instrumentation Event Subscription	Process (1)	Domain Policy	OS Credential Dumping (3)	Discovery 30 Permission Groups	Replication Through Removable Media	Local Data 27 Staging	Encrypted Channel (2)	Exfiltration Over Web 28 Service (1)	
Local Accounts 20	Software 30	External Remote 20	Windows Service 🚳	Modification (1)	LSASS Memory 13 NTDS 13	Discovery (2)	Software Deployment Tools 35	Remote Data 26 Staging	Asymmetric	Exfiltration to Cloud	
	Deployment Tools	Hijack Execution Flow (2)	Domain Policy Modification (1)	Modification 15	Security Account 31 Manager	Domain Groups 31 Local Groups 32	Taint Shared 13	Email Collection (1) 33	Cryptography 4	Scheduled Transfer 32	
	Service	DLL Search Order 10 Hijacking	Group Policy Modification	Execution Guardrails (1)	Steal or Forge Kerberos	Process Discovery	Use Alternate Authentication Material	Local Email Collection 25	Cryptography		
	Execution 49	DLL Side-Loading 40	Event Triggered 23	Environmental Keying	Tickets (1)	Query Registry 30	Pass the Hash 23	Input Capture (2) 24	Non-Application		
	Vser Execution (2) 33	Office Application Startup (1)	Windows	File and Directory Permissions Modification (1)	Kerberoasting 13 Steal Web Session 32	Remote System 4		Credential API 💿	Layer Protocol		
	Malicious Link 15	Office Template 41 Macros	Management Instrumentation Event Subscription	Windows File and	Cookie 32	Software Discovery 35 (1)		Keylogging 30	Protocol Tunneling (23)		
	Windows Management 49	Pre-OS Boot	Exploitation for Privilege n	Directory Permissions Modification	(1)	Security		Screen Capture 34	Praxy (4)		

Tidal Cyber Coverage Map

Coverage Mapping automatically assesses risk to an asset or group of assets by a Threat Profile on a TTP-by-TTP basis. This scalable approach compares the risks associated with a given TTP in a Threat Profile against the risk reductions offered by a **Defensive Stack**. A Defensive Stack is an inventory of security capabilities, as deployed and configured within a client's environment, to protect an asset or group of assets. The platform gives security organizations the ability to weigh each defensive capability based on its expected efficacy.

Tidal compares the risk presented by a TTP against the combined efficacy of the capabilities that comprise a Defensive Stack using a Behavioral Score. The Behavioral Score is an index between 0 and 50 that reflects the confidence that the risk presented by a TTP can be adequately offset by the capabilities in a Defensive Stack. The average of all Behavioral Scores is the overall Confidence Score of a Coverage Map.

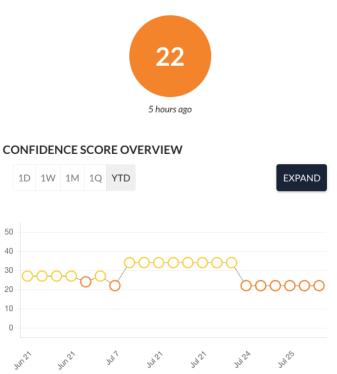
Confidence Scoring gives Coverage Mappings depth and value that evolves contemporaneously as adversaries and defensive capabilities evolve. With Confidence Scoring, security decision-makers have the ability to:

- Quickly and easily understand their operational security posture across the enterprise and see how it evolves over time.
- Identify key gaps in defensive posture and make data-driven decisions around which defensive capabilities are most important to add immediately.
- Optimize defensive coverage to ensure defense-in-depth where it is needed most.



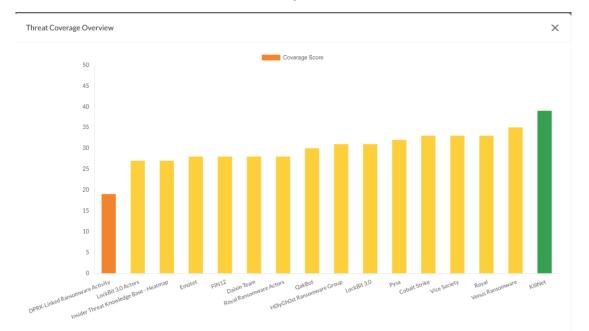


- Save significant money by eliminating unnecessary redundancies or migrating to more efficient platforms that offer the same or more risk reduction at a lower price.
- Understand the risk-reducing impact of security controls.



Confidence Score Over Time

Threat Coverage Overview







With Tidal Cyber's approach, security organizations have the ability to understand their updated security posture against TTPs as they evolve, how well the risk presented by a given TTPs has been resolved, and the relative residual risk that remains on an adversary-by-adversary basis.

The Chertoff Group Threat-Informed Defense Managed Service

The Threat-Informed Defense managed service will enable companies to keep pace with adversary TTPs as they rapidly evolve. Key elements include:

- Inherent Risk Profile. A strategic design principle for cyber resilience is supporting agility and architecting for adaptability. A starting point for doing so is understanding the inherent risk facing an organization that is, the risk before mitigations are put in place and how that risk is changing, for example based on new business initiatives, mergers & acquisitions or changes in technology architecture. This starts with business profile. From our experience, three foundational factors define inherent risk: (1) threat, (2) complexity and (3) impact, and we work to build and update profiles anchored in these elements.
- **High Value Assets.** Key operating constraints to defending an environment include both (a) a universe of threat actors that are adaptive and well-funded, and (b) limited resources with which to defend the attack surface. A secondary objective is to focus defenses on assets that represent heightened risks. The Chertoff Group helps define and evolve High Value Asset categorizations.
- Threat Model. Based on cyber threat intelligence sources, The Chertoff Group leverages the Tidal Cyber platform to continually update Threat Profiles that are relevant to the organization's business profile, including high-priority threat objects (adversary groups, malware families and emerging campaigns). The Chertoff Group tailors the weights for each threat object as it evolves based on specific requirements.
- Map. As The Chertoff Group updates Threat Profiles and Defensive Capabilities, the **Tidal Cyber** platform will recalculate Coverage Maps and Confidence Score automatically, providing an always current view of the organization's security posture against the TTPs that matter most.
- Manage. Leveraging Tidal Cyber, Chertoff Group will provide ongoing recommendations for adding new capabilities that fill new and existing coverage gaps, prioritized by the greatest impact to risk reduction.
- Assure. The Chertoff Group identifies and prioritizes critical defensive capabilities for periodic adversary emulation testing, providing the assurance that key defensive capabilities are as effective as expected. As important capabilities pass or fail these tests, The Chertoff Group adjusts the expected efficacy of the respective capability accordingly.





- Threat Hunt. Threat hunting complements existing detection capabilities, which are basically reactive, by proactively focusing on "identifying new adversaries or previously undiscovered malicious actors already entrenched in the enterprise." (MITRE World Class SOC Framework). Chertoff Group insights help prioritize these threat hunt operations.
- **Prepare for Incidents.** In a world where there is no such thing as risk elimination, incident preparedness is critical to minimizing impact from a successful intrusion. The Chertoff Group works with clients to develop plans, playbooks and exercises critical to sustaining a baseline of good practice and muscle memory on how to respond to high-severity incidents.

About The Chertoff Group

The Chertoff Group is an advisory firm of highly qualified experts that uses proven frameworks to help organizations achieve their business and security objectives in a complex risk environment. Our team helps organizations manage cyber, physical and geopolitical risks; navigate evolving regulatory and compliance requirements; and discover opportunities to win business and create value. Through our investment banking subsidiary Chertoff Capital, the firm provides M&A advisory services to companies in the defense technology, national security and cybersecurity markets. Together, we enable a more secure world. For more information, visit www.chertoffgroup.com.

About Tidal Cyber

Founded in January 2022 by a team of threat intelligence veterans with experience at MITRE, the U.S. Department of Homeland Security, and a wide range of innovative security providers, Tidal Cyber enables businesses to implement a threat-informed defense more easily and efficiently. Through both the Tidal Platform and our expert services, Tidal helps its customers map the security requirements and capabilities of their unique environment against the industry's most complete knowledgebase of adversary tactics and techniques, including the MITRE ATT&CK® knowledge base, additional open-source threat intelligence sources, and a Tidal-curated registry of security products mapped to specific adversary techniques. The result is actionable insight to track and improve their defensive coverage, gaps, and overlaps while also empowering cybersecurity teams to work more efficiently. For more information please contact: info@tidalcyber.com