Embracing Threat Informed Defense helps defenders sharpen their focus and improve cybersecurity risk posture.

Technology leaders today, more than ever, are facing increased budgetary pressure to reduce costs while continuing to provide the same or even better service to the business. The need to drive such efficiency is especially true even in business cost centers such as providing cyber security, which is historically well-suited for significant growth due to its critical importance to the business.

At least three things need to happen to improve an organization's cyber risk posture while reducing operational expenses.

1. Be laser-focused, prioritizing investment in the most severe business risks and associated threats.
2. Embrace and implement, or enhance automation wherever possible.
3. Remove complexity, even if this requires a higher short-term capital expense.

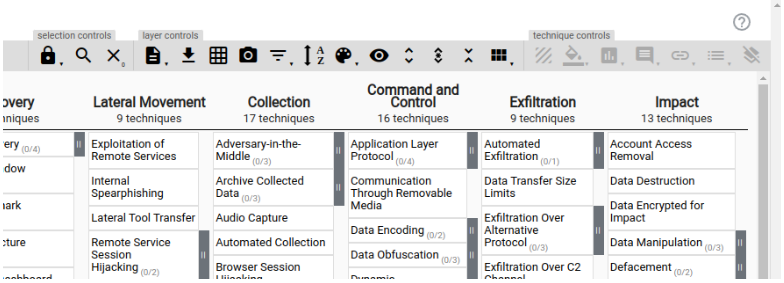
Threat Informed Defense helps technology teams and business leaders achieve the above by using observable threat intelligence data to understand which threats are related to the identified business risk and help inform and automate decision-making. Having risk, threat, and control data in a structured format enables the business to answer frequently asked questions such as;

- What are the detective and preventative control coverage/effectiveness related to our most critical business threats?
- How confident are we that we could catch actor x in our environment in a reasonable amount of time?
- What value are we providing to our customers?

The above questions take time to answer in a repeatable and data-based manner. Thankfully Mitre and other cybersecurity community members have developed tools and frameworks to help implement and automate elements of a Threat Informed Defense program.

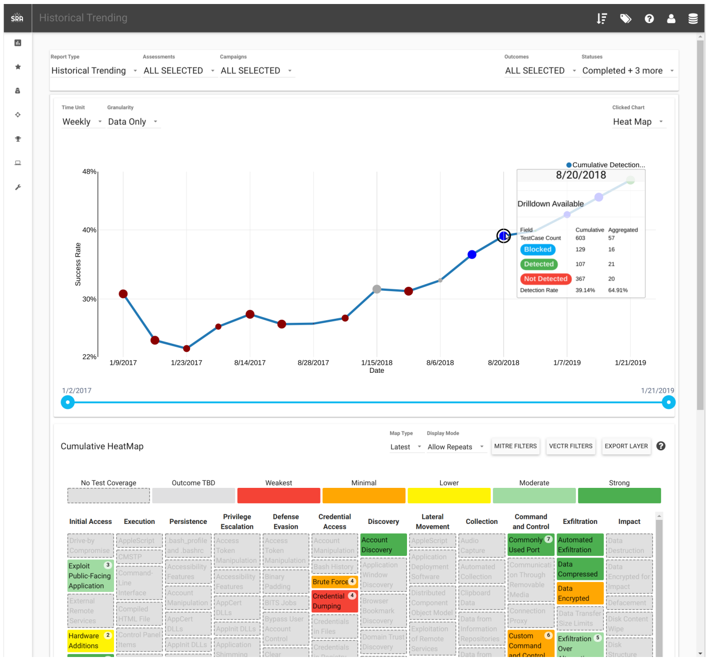
Frameworks such as Mitre Attack™ are now well established and embraced by the cybersecurity industry, enabling a standard nomenclature to describe badness, rank and model threats, and measure coverage and effectiveness.

Mitre's Attack Navigator can provide a visual representation of coverage or specific examples of threat actor campaigns.



overy niques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
ery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
dow	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
ark	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
cture	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
ashboard		Browser Session Hijacking	Dynamic		Defacement (0/2)

Projects such as VECR can facilitate tracking purple team exercises, measuring detection and prevention capabilities across different attack scenarios from each offensive security exercise.



Report Type: Historical Trending
Assessments: ALL SELECTED
Campaigns: ALL SELECTED
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Time Unit: Weekly
Granularity: Data Only
Clicked Chart: Heat Map

8/20/2018

Drilldown Available

Field	Cumulative	Aggregated
TestCase Count	603	57
Blocked	129	16
Detected	107	21
Not Detected	367	20
Detection Rate	39.14%	64.91%

Cumulative HeatMap

Map Type: Latest
Display Mode: Allow Repeats

No Test Coverage	Outcome TBD	Weakest	Minimal	Lower	Moderate	Strong
▭	⬜	🟥	🟧	🟨	🟩	🟩

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port 7	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application 3	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force 4	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions 2	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping 4	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control 6	Data Transfer Size Limits	Disk Content Wipe
	Control Panel Items	AppInit DLLs	Application Shimming	Clear	Credentials in Files			Data from		Exfiltration Over 5	Disk Structure
					Credentials in Registry						

Understanding specific cybersecurity Threat Scenarios is only one part of understanding the cybersecurity posture of the business. Linking threats to business risks enables a direct value measurement.

Documenting business risk including associated mission-critical business processes and mapping to cyber threats, allow companies to understand overall cybersecurity posture.

Frameworks such as the Rapid Risk Assessment (RRA) have existing taxonomy and tools for conducting such a risk assessment.

The above tools and frameworks are especially helpful in performing risk analysis, determining engineering investment in new and existing controls, aiding in the planning and execution of offensive security exercises, and reporting to leadership on the organization's overall cybersecurity risk posture.