EXPERT TIPS INSIDE

THREAT-INFORMED DEFENSE 101

Brought to you by ATTACKIQ

STUDY PLAN

OBJECTIVES

1. What is the definition of “threat-informed defense” (TID)?
2. How does an organization evolve from a reactive to proactive approach with TID?
3. How does the MITRE ATT&CK® framework work as part of a TID?
4. What is security optimization and what does it have to do with TID?

STUDY PLAN

STRUCTURE

1. Learn the basics of TID.
2. Examine how TID has evolved over time.
3. Identify the meaning of security optimization and its role in threat-informed defense.
4. Outline the steps to evolve to TID, as well as its benefits to cybersecurity teams.

PRIMER: WHAT IS THREAT-INFORMED DEFENSE?

> *"Threat-informed defense" applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks. It's a community-based approach to a worldwide challenge."* [1]
>
> - MITRE

[1] https://www.mitre.org/news/focal-points/threat-informed-defense

FUNCTION OF THREAT-INFORMED DEFENSE

A threat-informed defense strategy focuses security teams on preparing for the threats that matter most, and on developing granular visibility into their security program's effectiveness. Today private organizations lack visibility into their security teams' performances against known threats. A threat-informed defense strategy solves that problem by focusing the organization on known threats, and then testing the organization against known threat behaviors to generate real data about its security program's performance and maximize security effectiveness.

APPROACH

MITRE ATT&CK + PURPLE TEAMING + BREACH AND ATTACK SIMULATION = THREAT-INFORMED DEFENSE

Rather than a tool or tactic, threat-informed defense is a comprehensive strategy that is centered around three key objectives:

1. Understand the adversary's approach.
2. Identify your most valuable data and defense capabilities.
3. Build tight bonds between blue and red teams to focus on known threats and test defenses regularly, enabling a **“purple team”** construct.

INDUSTRY CHALLENGES CREATING THE NEED FOR THREAT-INFORMED DEFENSE

WHY IS THIS NEW APPROACH SO IMPORTANT?

- Traditionally, network defenders focused their defensive strategies on meeting baseline cybersecurity best practices: correcting misconfigurations, administering patches, and deploying best-in-class commercial products.
- Concurrently, defensive **“blue teams”** were focused on defending the home terrain.
- At the same time, organizations were spending money on building or employing **“red teams,”** or penetration teams, to adopt an adversarial approach and test the blue team's defenses.
- However, calling them red and blue teams portrays a picture of balanced opposing teams that is not remotely accurate.
    - Blue teams are vastly larger and spend much more than red teams.
    - Red team testing is episodic, and the coverage delivered is vastly smaller than the scale of the blue team's defenses.

INDUSTRY CHALLENGES CREATING THE NEED FOR THREAT-INFORMED DEFENSE (CONT.)

WHY IS THIS NEW APPROACH SO IMPORTANT?

- If the defenses are not oriented toward the most important threats, those resources are wasted. If they are not tested against the important threats, then they are likely to fail when challenged by the adversary, letting the adversary slip past.

- A purple team construct aligns red and blue to focus everyone in the security team on a process of continuous threat-informed defense analysis. It's not new team members, but an organizing process that aligns and brings out the best of red and blue together.

- Purple teams focus on the overarching threat landscape. They understand the security technologies as well as their organization and its operational attributes. With their combined knowledge, they test and improve their defense capabilities continuously in a collaborative manner to drive up effectiveness.

WHY THREAT-INFORMED DEFENSE IS IMPORTANT FOR CYBERSECURITY TEAMS: FROM TID TO SECURITY OPTIMIZATION

HOW CYBERSECURITY SPENDING INFORMS THREAT-INFORMED DEFENSE

When considering the importance of TID for cybersecurity professionals and teams alike, it makes sense to start by understanding typical security investment patterns.

Typically, cybersecurity teams invest in the necessary technologies and human resources one of two ways:

1. **Ad hoc:** Cybersecurity decision-makers approach the board for financial backing when a project arises (say, in response to a specific threat, or for an emerging solution).

2. **Benchmarks with peers:** The percentage of IT budget spent on cybersecurity technology is influenced by how others are spending.[2]

[2] https://attackiq.com/lp/from-reactive-to-proactive-security-optimization-and-threat-informed-defense/

WHY THREAT-INFORMED DEFENSE IS IMPORTANT FOR CYBERSECURITY TEAMS: FROM TID TO SECURITY OPTIMIZATION (CONT.)

These approaches don't lead to effective operational cybersecurity. However, security optimization — the ultimate result of threat-informed defense — does. Security optimization is a management practice that maximizes the effectiveness of your total security program (people, process, and technology) by ensuring that existing security controls are measured, monitored, and modified continuously from a threat-informed perspective.

It is about programmatically aligning security and risk services with the business to empower decision-making, and it helps you drive up your security team's effectiveness in meeting compliance and regulatory standards. But before we jump into how security optimization helps with risk and compliance management, let's lay out some of the technical steps that come first.

> ***"The unification of threat and risk management through continuous security control testing gives organizations a way to report on security and compliance effectiveness simultaneously — something that's never been done until now."***
>
> - Jonathan Reiber, Senior Director, Cybersecurity Strategy and Policy, AttackIQ

THE PATH TO ALIGNING THREAT AND RISK MANAGEMENT

STEP 1

THREAT-INFORMED DEFENSE

1. Identify the probable threats the organization will encounter.
2. Select technologies that will offer adequate, purposeful protection.

A threat-informed defense is a critical element in cybersecurity strategy, key to gaining the necessary insight for prioritizing and optimizing security decisions. Its value extends beyond garnering knowledge and into effecting change. To determine which actions to take in a timely and resource efficient manner, security optimization is a necessary next step.

STEP 2

SECURITY OPTIMIZATION

1. Identify and quantify cybersecurity risks through the collection of accurate data on the performance of existing security controls against actual threats.
2. Prioritize security investments based on a quantified understanding of the potential risk on business outcomes.
3. Continuously assess and calibrate staff skills, processes, and technology to maintain the desired security posture.

STEP 2 (CONT.)

SECURITY OPTIMIZATION

One of the goals of a security team is to balance the need for protecting the business against the need to run it. Security optimization focuses on the priorities and investments required to achieve that balance.

STEP 3

ALIGNING THREAT AND RISK MANAGEMENT

Security optimization aligns threat and risk management, which, in turn, increases compliance effectiveness.

- Over the last decade, the cybersecurity compliance landscape has grown increasingly complex. Some frameworks have become the de facto standards that drive other regulatory and compliance frameworks, to include the National Institute for Standards and Technology (NIST) 800-53 family of security controls.

- Simply following the steps outlined in a compliance framework does not guarantee success if cyberdefenses are not tested against known threats. To solve this problem, in 2020 MITRE Engenuity's Center for Threat-Informed Defense mapped the security controls in the NIST 800-53 framework to adversary behaviors in MITRE ATT&CK.

- With that threat and risk framework alignment, organizations can then use a breach and attack simulation platform to test and validate that the security controls mandated by a specific compliance framework are working effectively. Teams can then report out with granular data about their regulatory and compliance effectiveness.

STEP 3 (CONT.)

ALIGNING THREAT AND RISK MANAGEMENT

- Organizations can benefit in several ways from this data-driven alignment of threat and risk management. They can:

- ☑ Close the loop in the cybersecurity ecosystem, achieving a more comprehensive cybersecurity strategy for their stakeholders.
- ☑ Determine the degree to which specific people, processes, and technologies comply with regulatory frameworks such as NIST, DoD's CMMC, PCI DSS, etc.
- ☑ Ensure compliance validation happens routinely rather than through occasional audits or internal security reviews.
- ☑ Improve the organization's overall security posture.

Ultimately, businesses and government agencies can move beyond simple compliance to measuring the true effectiveness of their approach to security.

"MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."

- MITRE[3]

[3] https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf

THE ROLE OF THE MITRE ATT&CK FRAMEWORK IN THREAT-INFORMED DEFENSE

- The foundation of TID is MITRE ATT&CK, a framework of adversary tactics, techniques, and procedures (TTPs).[4]
- The release of ATT&CK in 2015 has given organizations a framework against which they can design defenses. By understanding how adversaries target your data, you are in a better position to secure yourself.
- Cybersecurity teams use the ATT&CK framework to enable threat-informed defense across all aspects of their security organization.
- With ATT&CK as a foundation, organizations are in a better position to establish a shared understanding of threats and threat behaviors.

Combining threat intelligence and MITRE ATT&CK delivers the following benefits to cybersecurity teams:

- Identify key hostile actors using a globally vetted framework.
- Gain insight into adversaries' operational behavior to analyze how that impacts your cyberdefenses.
- Deepen your approach by comparing your results to other analysts.
- Strengthen your defense teams.

[4] https://attack.mitre.org/

DID YOU KNOW?

AttackIQ's close alignment with MITRE ATT&CK is why the company became a founding member of MITRE Engenuity's Center for Threat-Informed Defense (CTID). The CTID is an organization within MITRE that conducts applied research and advanced development to improve cyberdefense at scale for the global community. It brings together the best cybersecurity researchers from across the globe.

HOW TO EVOLVE FROM A REACTIVE TO PROACTIVE CYBERSECURITY PROGRAM

FROM REACTIVE TO PROACTIVE IN THREE STEPS

1. Use a single threat framework like MITRE ATT&CK and prioritize a set of specific threats to the organization (i.e., hospitals should consider focusing on ransomware given their industry-specific risk profile).
2. Develop threat-based performance data and achieve real effectiveness from a management, planning, and outcomes perspective vs. focusing exclusively on meeting standards and compliance.
3. Adopt a **“purple team”** mindset that brings teams together to fight threats comprehensively.

HOW TO EVOLVE FROM A REACTIVE TO PROACTIVE CYBERSECURITY PROGRAM (CONT.)

FROM A THREAT-INFORMED DEFENSE PERSPECTIVE, A PROACTIVE ORGANIZATION IS CHARACTERIZED BY:

- Understanding which assets will be procured within the planning horizon across all areas — not just the assets that currently exist.
- An architecture team focused on identifying and understanding future risks, as well as the business impact of those risks.
- A cybersecurity strategy and roadmap that's informed by knowledge of existing threats and optimizes the planned actions for addressing them.
- A dynamic library of existing threats with a process in place for curation and management.

PRIMARY BENEFITS OF THREAT-INFORMED DEFENSE

- Achieve a pervasive, continuous testing program with the means to find and close security gaps.
- Develop more granular performance data, and drive improvements in your organization's security and technology governance processes.
- Successfully evaluate the performance of your people, processes, and technologies.
- Maximize the efficiency and effectiveness of your total security program to ensure existing security investments are measured, monitored, and modified continuously from a threat-informed perspective.

CONCLUSION

- Threat-informed defense applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyberattacks.
- Historically, cyberdefenses have not always been oriented toward the most important threats, resulting in wasted resources. If they are not tested against the important threats, adversaries are likely to slip past.
- Cybersecurity teams using the threat-informed defense approach can identify threats the organization is likely to encounter and choose the right security technologies as a result.
- Combining threat intelligence and MITRE ATT&CK allows organizations to evolve from a reactive to proactive cybersecurity program.

TEST YOUR KNOWLEDGE!

1. Which of the following is not a functionality of TID?

a. Delivers performance data which provides granular visibility into cybersecurity effectiveness against known threats
b. Monitors incoming and outgoing network traffic
c. Helps establish bonds between teams to focus on known threats and test defenses regularly
d. Allows you to compare your results to other analysts

2. Which methods comprise threat-informed defense?

a. MITRE ATT&CK, red teaming, penetration testing
b. NIST Cybersecurity Framework, blue teaming, vulnerability scanning
c. COBIT, blue teaming, data loss prevention
d. MITRE ATT&CK, purple teaming, breach and attack simulation

3. The labels "red teams" and "blue teams" are an accurate reflection of two balanced opposing teams.

☐ TRUE
☐ FALSE

4. Which approaches do most cybersecurity teams take in investing in technologies and human resources?

a. Ad hoc or benchmark with peers
b. Benchmark with peers or risk-based
c. Risk-based or ad hoc
d. In-house research or virtual CIO

TEST YOUR KNOWLEDGE!

5. Which three objectives does security optimization focus on?

a. Reduce risk; Align with NIST; Achieve cybersecurity operational success
b. Protecting assets; Identifying risks; Finding vulnerabilities
c. Identify cybersecurity risk; Prioritize security investments; Continuously calibrate staff skills, processes, and technology
d. Build inventory of IT assets; Develop risk profile; Determine budget

6. Which of the following is not a recommendation for moving from a proactive to a reactive approach to cybersecurity? Select all that apply.

a. Use at least three threat frameworks like MITRE ATT&CK, NIST, and COBIT
b. Develop threat-based performance data
c. Adopt a **"blue team"** mindset that focused on identifying threats in the operating environment
d. Adopt a **"purple team"** mindset that brings teams together to fight threats comprehensively

7. Fill in the blank: MITRE ATT&CK is a framework of _____ (TTPs).

a. Adversary tokens, tickets, and plans
b. Adversary tactics, techniques, and procedures
c. Adversary temperament, transactions, and prescriptions
d. Adversary tips, taxonomy, and patterns

TEST YOUR KNOWLEDGE!

8. One difficult side effect of TID is the fact that it makes it difficult to evaluate the performance of your people, processes, and technologies.

- ☐ TRUE
- ☐ FALSE

9. Which is a key benefit of TID?

a. Better fault isolation for more resilient applications

b. Prevents unapproved users from accessing information and records

c. Enhanced insights; more security certifications; single-pane-of-glass

d. Maximizes the efficiency and effectiveness of the total security program

PAGE LEFT BLANK INTENTIONALLY

Test answers on next page.

ANSWER KEY

1. Answer: B
2. Answer: D
3. Answer: False
4. Answer: A
5. Answer: C
6. Answer: A & C
7. Answer: B
8. Answer: False
9. Answer: D

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com.
Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.