TEVORA

Cyber Warfare Playbook:

PROACTIVE STRATEGIES FOR RESILIENT ORGANIZATIONS

While traditional cybersecurity approaches often focus heavily on defensive measures such as firewalls, antivirus software, and intrusion detection systems, there is a growing recognition of the important of a more holistic strategy to build resilient organizations. This includes both defensive and offensive measures to enhance an organization's security posture. Offensive strategies play a crucial role by proactively identifying and addressing vulnerabilities, simulating attacks to test defenses, and gathering intelligence on potential threats. By integrating these proactive measures with robust defensive mechanisms, organizations can better protect themselves against the most pernicious attacks and adapt to the evolving threat landscape.

Proactive Threat Identification

There's no question that every digitally empowered organization today needs to consider both sides of the cybersecurity equation, defensive and offensive, but the former is often the less complex task. "When you're being reactive you can look at just the systems and events in your organization. The scope is smaller, and things are mostly in your control," explained Ben Dimick, Tevora's Director of Security Implementation Services. "But when you are proactive, you're trying to intercept signals out in the wild that are more open to ambiguity. There's a lot more opportunity for interpretation." Threat hunting is actively searching for hidden threats that have evaded traditional security controls and monitoring tools. Security threat hunters use a combination of advanced analytics, machine learning, and human expertise to identify suspicious activities, anomalies, and behavioral patterns that may indicate areas of concern.

In the experience of Kash Izadseta, Tevora Senior Information Security Associate, one tool that is particularly useful in both proactively finding threats and in preparing an organization for live incidents is time-tested tabletop exercises, simulated scenarios that allow organizations to walk through their incident response procedures, identify gaps, and make necessary improvements. "These simulations help teams familiarize themselves with their roles and responsibilities during an actual incident, which leads to a more coordinated response," Izadseta said.

User Awareness Training

Educate employees about common cyber threats, such as phishing emails and social engineering tactics, empowering them to serve as the first line of defense.

- **Ransomware Readiness Assessments:** Help organizations evaluate their ability to prevent, detect, and recover from sophisticated ransomware attacks

- **Gap Assessments:** Identify weaknesses in an organization's cybersecurity posture, allowing them to prioritize remediation efforts

- **Reviews of System Configurations, Network Architectures, and Security Tools:** Ensure that all components are properly deployed and optimized to detect and respond to threats

Additionally, he recommends that every organization develops and maintains a comprehensive runbook, which is a step-by-step guide that outlines the procedures for handling specific incident scenarios. It includes instructions for a rapid response, contact information for key personnel, and guidelines for communicating with stakeholders.

Deception Technology

In addition to traditional threat hunting, new issues can be actively exposed by crafting a false environment within an organization's network to lure, detect, and deceive attackers — so that they can be safely observed and studied without risking actual systems and data. Honeypots, for example, are a type of decoy system that can be configured to mimic different types of systems, such as databases, web servers, or industrial control systems. By monitoring attacker activity within the honeypot, organizations can gain insight into their methods and motives.

That said, active defense measures are an especially delicate area in cybersecurity. "We absolutely discourage hacking back or otherwise antagonizing attackers," said Kevin Dick, Tevora's Director of Threat Services. "The risk to reward ratio just doesn't justify it. But in certain situations, methods like honeypots can be good tripwires or useful in slowing down attackers."

"The most important thing is keeping the right perspective with active defense measures," added Ben Dimick. "We advocate a careful and judicious approach. Honeypots can be useful for an additional layer of identification, but we would never put one just anywhere. It has to be a controlled environment for maximum safety, and it has to be tuned to avoid false positives because when an alarm goes off too frequently, people learn to ignore it."

Evolving Threat Intelligence

Threat intelligence gathering involves collecting, analyzing, and interpreting information about potential threats and vulnerabilities. As is so often the case across industries, knowledge is power in cybersecurity. “We subscribe to several feeds and utilize tools that monitor the dark web. We also track many websites, chat channels, and forums that monitor hacking activity,” said Kash Izadseta. “It’s a cat and mouse game, and we have to be up to the challenge and stay on top of very elusive adversaries.”

TTPs

Tactics, Techniques, and Procedures (TTPs) are the patterns of activities and methods used by cyber adversaries to achieve their goals. Understanding TTPs is critical because it provides a structured approach to analyzing and responding to adversary behavior.

- **Tactics:** High-level goals or objectives that an adversary is trying to achieve, such as gaining initial access to a network, establishing persistence, or exfiltrating sensitive data. Tactics answer the question of “why” an adversary is performing an action.
- **Techniques:** Specific methods or actions that an adversary employs to achieve their tactical goals. Techniques answer the question of “how” an adversary is performing an action. Examples of techniques include phishing, exploiting vulnerabilities, or using stolen credentials.
- **Procedures:** Detailed, step-by-step instructions for executing a particular technique. Procedures answer the question of “what” actions an adversary is taking. For example, a procedure might involve the specific commands used to perform a particular exploit or the specific tools used to exfiltrate data.

By understanding TTPs, organizations can gain valuable insights into adversary behavior, such as the specific tools and methods they use, their preferred targets and attack vectors, and their ultimate goals and objectives. This knowledge can help organizations anticipate and prepare for potential attacks, prioritize their defenses, and respond more effectively to security incidents.

Dynamic Attack Simulations

A well-architected defensive posture might seem impenetrable at first glance, but, according to Kevin Dick, the goal of all simulated exercises is to put the theory into practice. “We can’t assume. We have to know with a high degree of certainty: Is this system secure? Are we going to have accurate detection? Practices like penetration testing prove the system functions as intended. It validates the controls and the investment.”

► Penetration Testing

Penetration testing, also known as pen testing or ethical hacking, is a foundational offensive cybersecurity exercise. Pen testers use the same tools, techniques, and methodologies as malicious hackers but with the permission of the organization being tested. They attempt to breach the organization’s defenses, gain unauthorized access to sensitive data or systems, and demonstrate the potential impact of a successful attack.

Penetration testers employ a wide range of strategies and techniques to identify and exploit vulnerabilities, including:

- Social Engineering
- Network Scanning
- Vulnerability Exploitation
- Password Cracking
- Privilege Escalation
- Wireless Testing

In addition to exposing risks, an ancillary benefit to penetration testing is that it can serve as a wake-up call to firms that might be underestimating the need for more extensive cybersecurity investments. “On paper, risk can be nebulous. Real world pen testing makes it tangible,” said Kevin Dick.

► Adversary Simulation

Going beyond traditional penetration testing, adversary simulations consider the broader context of an attack, including the attacker's motivations, objectives, and the specific Tactics, Techniques, and Procedures (TTP) they might employ. "We devote a lot of energy to understanding the human component to attacks and breaches because with real adversaries there's always a social engineering component," said Kevin Dick. "Even the most advanced defensive technologies are useless if a criminal can simply convince an employee to do something they shouldn't. And it only takes one domino to fall for the whole network to be compromised."

Adversary simulation can take various forms, each with its own specific objectives and methodologies:

Red Teaming

A Red Team operates as an independent, simulated adversary, and engagements are often broader in scope and more open-ended than traditional penetration tests, with the Red Team having minimal or no prior knowledge of the target environment.

"The challenge of red teaming is that every environment is different," explained Kevin Dick. "We spend a lot of time probing controls and working stealthily. Just dropping a malicious payload will set off alarm bells in most systems, so we're more careful than that. Real adversaries are crafty, patient, skilled, and have access to unique tools and exploits. So we put a lot of thought into how we can create an experience as close to the real thing as possible."

Purple Teaming

In a Purple Team exercise, Red Team attackers share their TTPs and findings with Blue Team defenders in real-time, allowing the defenders to adapt and improve their detection and response capabilities. This approach fosters knowledge sharing, communication, and continuous improvement between offensive and defensive teams.

Tevora's Kevin Dick explained why both Red and Purple team exercises have their place: "We often recommend our clients start with purple team exercises first; it gets everyone on the same page. The organization we're working with gets to experience the threat model right alongside us. We can guide them as they learn. Something as simple as saying 'Hey, did you see that? No, then let's tweak this and check it again' can lower the fog of war and help us jointly develop a baseline that we can calibrate from."

TEVORA™

Overall, the key to effective penetration testing and adversary simulation is to act tactically and methodically. “We ask ourselves how do we get in, what tools or tactics will help us get there, then we test our approach, report our findings, and analyze the outcome with an eye towards remediating risks. And, because cybersecurity is always a moving target, we reassess annually,” said Kevin Dick. “It’s always gratifying to see the improvement and excitement when we find out just how much more difficult our job is now that their security gaps have narrowed,” he said. “For one thing, we like the challenge, but more importantly, it means our guidance is having the desired effect.”

Tevora is your **comprehensive cybersecurity resource.**

Contact us today to learn more about the benefits of offensive security strategies and how they can protect your organization.