Hilco Global
AN ORIX COMPANY

SMARTER PERSPECTIVE: CYBERSECURITY

Thinking Like the Enemy: How Threat Actor TTPs Supercharge Cybersecurity Maturity

By Bob Olsen, MBA, MS, CISSP, CCSP

March 2026

Building a mature cybersecurity program around threat actor tactics, techniques, and procedures (TTPs) means designing security from the adversary's point of view rather than from a control checklist. When you start with how attackers actually work – how they gain access, move laterally, escalate privileges, and exfiltrate data – you anchor your program in real world behavior instead of theory. This orientation acknowledges that breaches are a matter of "when," not "if," and that resilience depends on understanding and disrupting an attacker's workflow at every stage.

Using TTPs as the backbone of a program gives security leaders a precise language for describing risk. Instead of saying "we have a monitoring tool," they can say "we can detect privilege escalation attempts and suspicious remote administrative activity." That shift from technologies to behaviors makes it easier to explain risk to executives and boards, because discussions focus on concrete attacker actions and the potential business impact. It also helps unite disparate teams – operations, engineering, legal and leadership – around a shared picture of how an intrusion unfolds and where defenses must intervene.

TTP driven programs also bring discipline to prioritization. No organization can defend perfectly against every possible attack path, and trying to do so leads to thinly spread resources and unfocused spending. By concentrating on the techniques most relevant to its industry, technology stack, and critical assets, an organization can make deliberate choices about where to invest. Identifying the TTPs of threat actors who commonly target specific industries can add even more refinement to this approach. Security roadmaps become collections of specific behavioral gaps to close, rather than shopping lists of products to buy. This approach typically yields fewer tools, better tuned controls, and clearer justification for every dollar spent.

Operationally, a focus on TTPs raises the quality of detection, hunting, and response. Detection engineers can design and track alerts around well defined attacker behaviors, then measure how well those behaviors are covered in different parts of the environment. Threat hunters can build hypotheses that mirror real adversary playbooks, which makes their searches more targeted and more likely to uncover subtle, "living off the land" activity. When incidents occur, responders can quickly infer likely next steps by mapping observed actions back to known tactics, allowing them to anticipate attacker moves instead of reacting blindly.

Finally, a program grounded in TTPs adapts more easily as the threat landscape changes. For example, threat actors have been shifting away from traditional malicious script-based hacking tools and focusing more on abusing trusted services such as Remote Monitoring and Management (RMM) tools. While specific tools, malware families, and infrastructure come and go, the underlying behaviors attackers rely on change far more slowly. By concentrating on those behaviors, organizations reduce their dependence on fragile indicators and one off signatures.

As new campaigns are observed, teams can ask a simple set of questions: which known behaviors are being reused, which new ones are appearing, and how well do our current controls perform against them? That continual loop – observe, map, test, improve – is what turns a basic security function into a genuinely mature, threat aligned capability.

Organizations that want to act on this approach do not need to overhaul everything at once; they can start with a focused, practical roadmap. First, establish a common catalog of attacker behaviors relevant to your environment and use it to map existing controls, detections, and response playbooks. The MITRE ATT&CK and ATLAS knowledge bases are a great source of TTP information. Next, identify the handful of high impact tactics and techniques that matter most to your business and prioritize engineering work, tabletop exercises, and threat hunting around those behaviors. From there, build a recurring cycle – quarterly or monthly – where you reassess emerging adversary tradecraft, update your behavioral coverage, and validate it through purple teaming or automated attack simulations. Over time, this rhythm of mapping, measuring, testing, and improving will embed threat informed thinking into everyday operations and steadily move the program toward true maturity.

BOB OLSEN, MBA, MS, CISSP, CCSP
MANAGING DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Bob can be reached directly at ROlsen@hilcoglobal.com.