Cyber Threat Profile

HIGHLIGHTS

- Anticipate changes to your organizational risk profile based on changing threat factors

- Provide situational awareness to leadership teams, cyber defense and enterprise risk functions to guide security strategy and investments

- Proactively prepare operational teams through targeted training exercises against real threats

- Validate technology against the capabilities and tactics of adversaries

- Map organizational high-value targets to threat actors based on the vulnerabilities and malware leveraged

- Survey internal network telemetry to uncover active or past unauthorized access.

Understand the threats targeting you

Cyber threat actors and tactics are constantly changing and adapting to defensive measures, complicating the lives of security professionals. To properly understand the threats it faces, an organization must identify its specific security goals, business vertical, geography, high-value targets (critical assets), historical threat activity, and defensive posture. These efforts require regular maintenance and should combine both an internal and external point of view for holistic understanding and useful specificity.

The **Double Technology's** Cyber Threat Profile gives you a composite picture of the most important and relevant cyber threats to your organization and how those threats are likely to materialize and impact you and your partners, now and in the future. The Cyber Threat Profile is an essential part of an intelligence-led security strategy--one that creates a proactive defensive posture to reduce cyber risk.

Benefits of a Cyber Threat Profile

A cyber threat profile has strategic, operational and tactical benefits, including:

- Arm executives with a thorough understanding of cyber threats to guide security investments

- Bridge threat communication gaps between business and security operations teams

- Review security architecture decisions based on attacker motivation, capability, and intent

- Enhance threat modeling processes through incorporation of pertinent attacker profiles

- Reduce responder stress by effectively scoping investigations

- Go beyond CVE scoring by integrating threat intelligence into vulnerability management activities

Collectively, the benefits of a cyber threat profile enable you to make security decisions based on cyber risk rather than best practices or instinct.
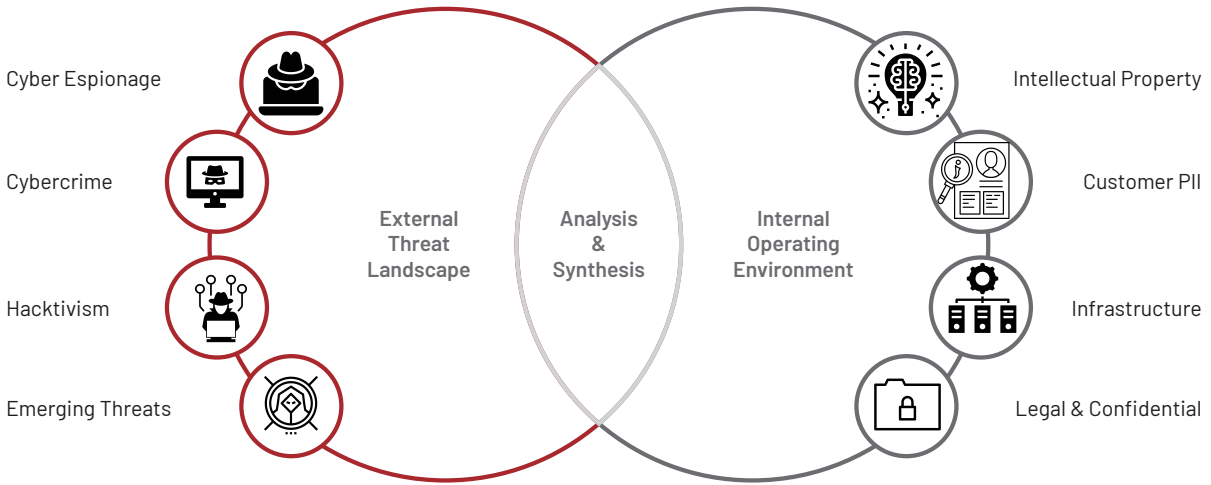
FIGURE 1. Elements of an effective Cyber Threat Profile.

A cyber threat profile is a critical component to a holistic cyber security strategy. It can serve multiple organizational personas and be a central input and driver for other threat management activities, such as threat modeling, security validation, threat hunting, red teaming, penetration testing and tabletop exercises. Before beginning, it is important to understand the desired

outcome. Double Technology's intelligence experts build cyber threat profiles at three different levels. Based on Double Technologies experience developing these profiles over many years, not every customer will require the same approach, which generally corresponds to the threat fidelity desired. Each level builds upon the previous levels threat fidelity and includes all prior deliverables.
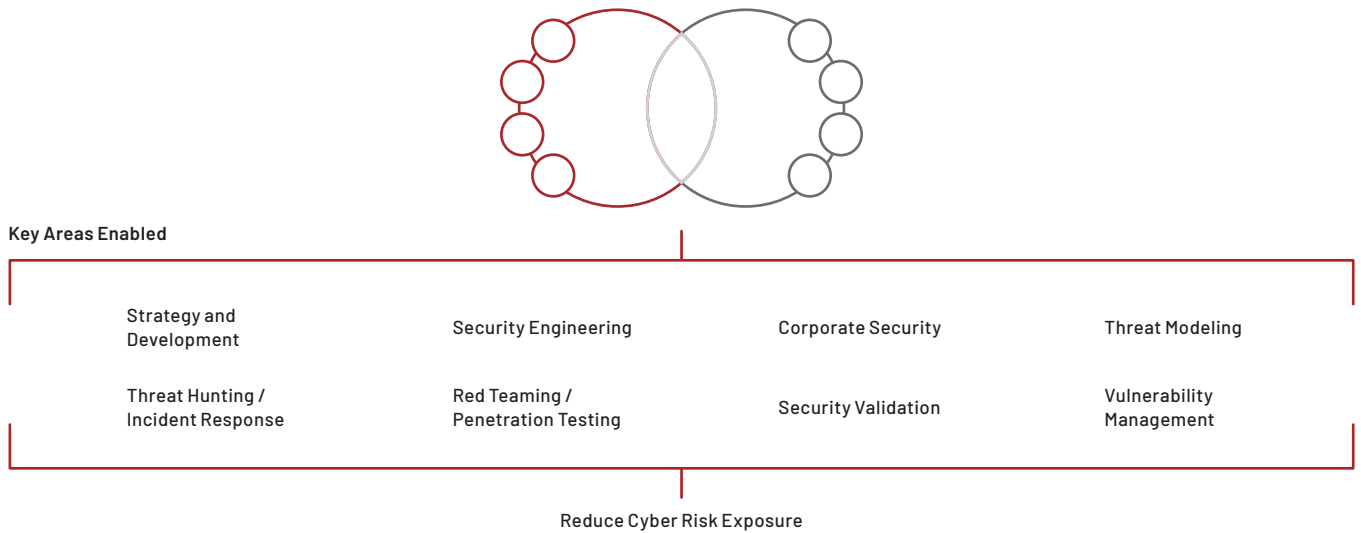

Key Areas Enabled

| Strategy and Development | Security Engineering | Corporate Security | Threat Modeling |
| Threat Hunting / Incident Response | Red Teaming / Penetration Testing | Security Validation | Vulnerability Management |

Reduce Cyber Risk Exposure

FIGURE 2. Applying your Cyber Threat Profile.

TABLE 1. Cyber Threat Profile levels.		
Level 1 **Which threats should I focus on?**	**Level 2** **How do we ready operational teams?**	**Level 3** **What threat activity have we seen in our environment?**
Level 1 outcomes are focused on **strategic** stakeholders. At this level threats are outlined at an organizational level: those that have targeted or are likely to target organizational users and operations. It informs security leaders of attacker motivation and intent. Outcomes will help explain who is behind an attack, why the organization may be a target, and what adversaries are interested in.	Level 2 outcomes build on Level 1 and are focused on **operational** stakeholders while enabling strategic program decisions. At this level, external threats are linked to internal high-value targets (critical assets) so organizations can prioritize defenses based on threat capability. Level 2 helps show how and where various threat scenarios are likely to cause severe impact within the operating environment.	Level 3 outcomes includes all Level 2 outcomes and are focused on **tactical** stakeholders while providing operational visibility into the effectiveness of current defenses and giving the organization cyber risk clarity. Double Technology's experts analyze internal security telemetry to deliver a fact-based assessment of present and past adversary targeting, which allows precise threat prioritization and allocation of resources.
Level 1 output: Comprehensive threat report (PDF format) detailing impactful cyber threats that are relevant to your geography, business sector, key infrastructure, and operations.	**Level 2 output:** All level 1 deliverables plus a customized threat register utility (Microsoft Excel format) that maps identified threats, including known vulnerability usage and associated malware to your high-value targets. The utility also includes a MITRE ATT&CK overlay.	**Level 3 output:** All level 1 and level 2 deliverables enriched by customer security telemetry and Double Technology's threat analysis, including a cyber risk heat map with countermeasure recommendations linked to environmental findings. A technical addendum (Microsoft Excel format) incorporates discovered malware families and related indicators, exploitation vectors, and any implicated internal hosts.

Threat Preparedness

Cyber Threat Intelligence functions must take a leading role in managing organizational threats. Business and cyber defenders need up-to-date intelligence to inform their specific decision-making processes. Those that fail to do so will have trouble consistently realizing value from intelligence and may ultimately decrease operational efficiency. The Cyber Threat Profile is your first step to becoming an intelligence-led organization.