Threat Hunting Checklist *for* CYBER WARRIORS

Arm yourself with the knowledge and experience to hunt down unknown threats

To get in the hunt, you need certain skills, an optimized threat hunting process and the right tools and data. Here's our abbreviated checklist of what you need to be ready for your first/next hunt.

THREAT HUNTER SKILLS

- Understanding of both network and operating systems (OS) in an infrastructure
- Understanding of analytic tradecraft, including the ability to create hypotheses and test those against assumptions (including biases)
- Understanding of attacker TTPs from both a process and tool perspective

OPTIMIZED THREAT HUNTING PROCESS

- Form a hypothesis and prepare for a prospective hunt
- Operationalize a framework to assist in the identification of threat vectors
- Leverage external intelligence (Fidelis Threat Research)
- Collect internal intelligence
- Pivot macro to micro focus

TECHNOLOGY PLATFORM

- Unified platform that integrates Network Traffic Analysis (NTA) and Digital Forensics and Incident Response (DFIR) to ensure faster detection, empower threat hunting and automate response (Fidelis Elevate)

Get the Threat Hunter's Toolkit **DOWNLOAD NOW**

Fidelis Cybersecurity