There is no question that end-users have become a prime target for cyber criminals. However, the real tangible target is the end-user’s workstation, and organizations would be remiss not to regularly validate the security of their endpoints. In spite of organizations mandating employees to complete security awareness training and spending a significant portion of their security budgets on modern endpoint protection tools, assessing the security strength of their endpoints remains a major gap. In fact, the most common security gap on endpoint was out-of-date or unpatched software, according to 75% of respondents from “The Cost of Insecure Endpoints” report by Ponemon Institute.

To close the gap, Optiv has developed an endpoint assessment methodology that accounts for each step of the attack lifecycle from payload delivery to data exfiltration. This methodology is developed and performed by offensive security experts that specialize in enterprise exploitation. The identification of vulnerabilities and gaps in security controls that may have gone unnoticed will assist you in tuning detection or protective controls to handle user activities. Associated remediation efforts will enhance incident response capabilities and further strengthen your overall security posture.

How Do We Do It?

**THREAT MODELING**
Footprint the system to identify and prioritize potential attack vectors

**PAYLOAD DEVELOPMENT AND DELIVERY**
Tailor a variety of payloads to the system and test every viable delivery method

**LOCAL PRIVILEGE ESCALATION**
Assess system for any susceptibility to elevate privileges

**LATERAL NETWORK MOVEMENT**
Opportunities to expand beyond the initial foothold may be identified depending on the test environment

**CODE EXECUTION**
Each payload is tuned and tested against the system to identify exploitation methods to gain the coveted initial foothold

**COMMAND AND CONTROL**
Evaluate every method to establish a persistent connection to the system

**DATA EXFILTRATION**
Each file type will be tested over various communication channels in order to determine how data can leave the system
How We Do It Better

- **Increased Confidence in Security Controls:** Know for a fact which controls are functioning as promised and expected.

- **Prioritized Hardening Strategy:** Not all hardening activities are created equal. Prioritize the ones that matter so your time and resource allocations are optimized.

- **Improved Security from Proactive Planning:** Utilize objective, fact-based reporting to truly understand the “what if” and prepare accordingly.

- **Enhanced Defense Posture:** Your defenses will improve quicker than ever after an attack.

- **Attack Instrumentation:** AttackIQ and other industry leading tools are leveraged to rapidly validate your defensive controls against the MITRE ATT&CK framework.

Secure your security.

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2020 Optiv Security Inc. All Rights Reserved.