# Threat & Vulnerability Management Program A STEP-BY-STEP JOURNEY TO SUCCESS

The majority of breaches start with the exploitation of a known vulnerability. Organizations don't have the people, resources, or time to patch the tens of thousands of vulnerabilities that will likely make their systems targets of attackers.

This 5-Level journey will provide the critical steps to a risk-based, proven vulnerability management program.

00

# LEVEL 1: Now We're Scanning

- » Asset inventory
- » Ticketing process, rudimentary metrics
- » More manual assessments
- » Shorter time-based patching
- » Unsystematic scanning

Set reasonable goals: start with areas of attack like surface hardening, asset inventory, and patch auditing. Understanding which systems are exposed and what % of systems have been patched are examples of good fundamental metrics.

### 3 LEVEL 3: Critical Assets and Risk

- » Risk-focused Assets prioritized
- » VM reporting and audit
- » Automated assessments
- » Patching by risk and criticality
- » Real-time vulnerability scanning

Leverage compliance standards like NIST, ICO, or CSC 20 to measure effectiveness and path towards security maturity.

# LEVEL 5: Reducing Business Risk

» Risk aligned with business

- » VM reporting integrated into risk assessment
- » Improvement in compliance categories
- » Continuous patching
- » Scanning is the foundation to real-time risk assessment

#### **START HERE**

- » No understanding of asset value
- » No metrics or processes
- » Manual assessments
- » Time-based patching
- » No scanning

Determine what data is important to your organization, on which systems that data lives, who accesses the data, and which applications are used.

# LEVEL 2: The VM Process is Starting

- » Asset criticality score
- » VM Lifecycle Process
- » Systematic assessments
- » Patching by risk
- » Scheduled scanning

Generate accurate, concise reports that don't overwhelm with low priority vulnerabilities, but identify high priority issues and remediation plans and timelines.

# LEVEL 4:

### **Risk-based Patching**

- » Asset scores consistently monitored
- » Real-time VM reporting
- » Assessment scores by compliance standard
- » Patching to reduce enterprise risk
- » Vectors scanned and prioritized

Business goals dictate security goals. Gaps in compliance are closed by priority, thus effectively lowering overall risk.

