DEFENSESTORM
THE BEST OFFENSE.

# DefenseStorm Vulnerability Management

Vulnerability scanning assesses your system by discovering the security weaknesses in a network an adversary may be able to exploit due to missing patches, uninstalled software updates, open ports, running services and misconfigurations. Regularly reviewing the environment, prioritizing and applying corrective actions and verifying that threats have been eliminated are necessarily to ensure consistent improvement. That is why ongoing scanning is vital for organizations to adopt as part of a robust vulnerability management and patching policy, thereby proactively shrinking the attack surface.

## Why DefenseStorm Vulnerability Management?

• DefenseStorm's partnership with CODA Footprint allows us to integrate their product with GRID.

• Integration with a scanning service enables us to provide a more comprehensive overview of risk, tie into reporting, dashboards, Active Compliance (tasks), etc.

• Partnering with CODA Footprint also provides continuous scanning capabilities. Vulnerabilities are more quickly discovered, resulting in a shorter patch time and overall reduction of risk.

• Additionally, integration enables automatic task ticket creation when new vulnerabilities are detected, replacing the hands-on ticket creation aspect with automation which leads to scalability and fewer resources spent on mundane work.

DEFENSESTORM
THE BEST OFFENSE.

# DefenseStorm Vulnerability Management

## Partnering with CODA we:

- Identify and assess network-connected devices with automated asset discovery and classification
- Prioritize remediation efforts by automated (and self-learning) groupings of assets (apps/devices) into technical and business contexts
- Assimilate evolving threat intelligence utilizing industry feeds and CODA Threat Intelligence (Cortex™) with AI-driven metadata processing to enhance the processing algorithms of the platform
- Focus on risk-based remediation with actionable mitigation suggestions – prioritization is based on threat intelligence, RLE (Real Life Exploitation) vectors, and weaponization along other calculated factors
- Reduce remediation planning using the CRSS (contextual risk scoring system) in order to provide the most effective patching plan to address the riskiest assets first
- Ensure continuous risk mitigation and posture improvement by combining advanced machine learning with the data collected across the ecosystem to provide the best remediations and identify the riskiest exposed assets tailored to each customer's environment
- Update automated, pre-generated CODA-based reports in real time including but not limited to the Customer Vulnerability Report, the Remediation Report and the Contextual Risk Scoring Report from both a snapshot and historical point of view