SECUREAUTH + CORE SECURITY

Case Study

Energy Infrastructure Company

Core Vulnerability Insight & Core Impact

Background

This organization is the most complete energy infrastructure-focused company in the world and a major provider of government services. They chose the Core Attack Intelligence Platform to consolidate, normalize and prioritize vulnerabilities for remediation—ensuring the security of their intellectual property

The Core Attack Intelligence Platform helped this energy infrastructure organization:

+ Evolve their vulnerability management program and improve their overall security posture.
+ To better understand their network, assets, configurations, and related vulnerabilities. Core Insight helped them fully discover their network while providing a single pane of glass view of consolidated and prioritized vulnerabilities, and critical asset risk.

The Challenge

A comprehensive vulnerability and risk management solution was a requirement for this organization. In addition, a recent acquisition and stringent compliance regulations left them in need of a more strict security program.

Very often, vulnerability management practices involve simple “patch Tuesday” remediation, and don’t account for the many critical assets prone to attack throughout a typical infrastructure. Remediation efforts are performed on a large volume of CVSS “high-priority” vulnerabilities without consideration of business risk or downstream effects. This not only greatly increases the risk of a security breach, but leaves these organizations challenged to understand how they will be attacked and exploited, making it harder to respond effectively.

> *“Without Core Impact it would have been impossible to integrate penetration testing into our security process. other tools require too much expertise, aren’t safe to run on live networks, and deliver questionable results.”*

Core Impact:

Easy to Use

Safe

Reliable

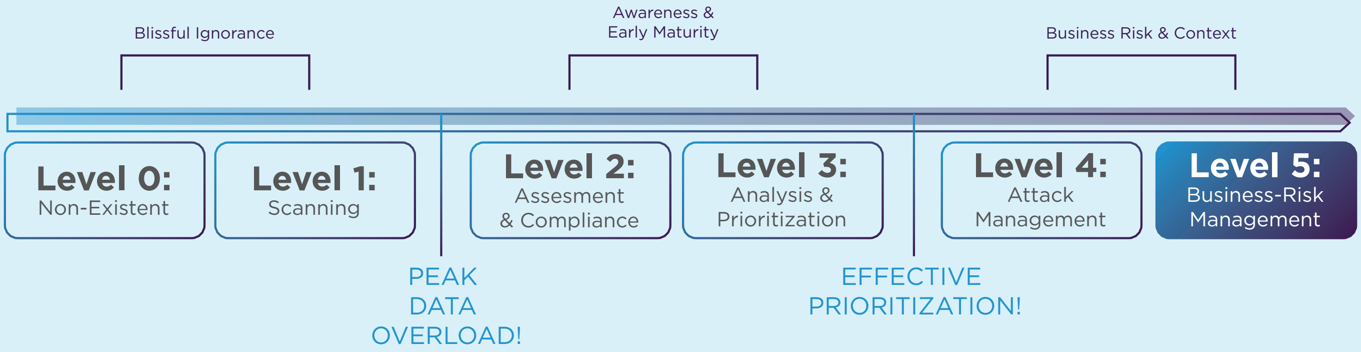
The Approach

This Energy Infrastructure Company needed to evolve their vulnerability management program, starting early in the vulnerability management maturity model. However, their strategic vision will take them well past the initial stages of scanning, into advanced prioritization and attack planning.

As a first “discovery” step, with Core Insight and vulnerability scanners in place, they began executing campaigns to identify assets and prioritize vulnerabilities throughout their network. To further prioritize these vulnerabilities, they were validated with Core Impact to confirm any potential threats before remediation efforts.

Focused on protecting intellectual property and various endpoints such as industrial control systems, the organization continuously monitors risk through attack planning and threat modeling campaigns in Core Insight. These efforts produce attack paths across networks, business units, and geographical locations, even into suppliers and contractors, to ensure there are no exploitable points between locations. This is not only important for the security of each partner, but many regulations require strict monitoring of vulnerability risk throughout the supply chain. Executive level reporting helps summarize risk, vulnerability, and remediation details to the various IT users, line-of-business owners, and management.

Threat Vulnerability Management Model


Blissful Ignorance
Awareness & Early Maturity
Business Risk & Context
Level 0: Non-Existent
Level 1: Scanning
Level 2: Assesment & Compliance
Level 3: Analysis & Prioritization
Level 4: Attack Management
Level 5: Business-Risk Management
PEAK DATA OVERLOAD!
EFFECTIVE PRIORITIZATION!

Benefits

With limited resources, strict regulation, and a large global environment, this organization recognized the need to firm up their security program. Acquiring point solutions was not an option. Instead, they pursued a holistic security program to form internal policies, governance, and processes to strengthen their position and protect critical assets. One of the most influential elements of this program is aggressive vulnerability management, consisting of prioritization and consolidation of vulnerability data along with attack path simulation to identify breach points for remediation.

This new approach to vulnerability management not only gave them visibility into their network that wasn’t possible before, but also gave them control over potential threats across their network. The result is a manageable, prioritized list of vulnerabilities for remediation, greatly reducing the risk of a breach of intellectual property