Core Security Assessment

Customers Spotlight:

Major Multinational Retailer

- Corporate office suspected access control issues with inactive and abandoned accounts
- Migrating to new IT infrastructure service provider
- Strong IAM operations ensured they passed all audits, but wanted additional security assurance

Assessment Findings

- Identified 1000+ abandoned contractor accounts to be terminated
- Found 130 terminated employee accounts that needed to be de-provisioned
- Discovered 14,000 inactive user groups
- Determined 25+ users with access in excess of role via hidden, nested entitlements

Customers Spotlight:

International Entertainment Company

- IT Leadership suspected variants of malware were going undetected
- Rising concerns over DDoS attacks
- Existing incident response vendor malware reports were not in-line with AV software findings
- Risk resulted in needing to perform bare metal restores at a cost of $2.0 million

Do You Have Insight into the Risks that are Present in your Environment Today?

Are you among the increasing number of organizations that have implemented solutions that look at access risk, existing vulnerabilities and advanced threats in your increasingly complex network and infrastructure, and are inundated with data that you cannot analyze and respond to in a timely fashion? Do you find yourself desperately trying to prioritize information and security tasks in order to stay ahead of potential threats? Are you struggling to correlate data from multiple sources quickly and do all of this with a shortage of dedicated resources on your team? Do you really want to wait until someone else finds these gaps first?

The reality is that the IT stack continues to get more complicated with new and emerging application. There will rarely ever be enough time nor will there ever be enough resources to fully combat the problems IT Security and Operations face as the adversaries are moving faster and often have more scale and resources than we do. This we cannot control.

What we can control, however, is how much visibility we have into our environment in order to help us prioritize and make better decisions about where to focus our security effort and response.

Gain Valuable Insight with a Core Security Assessment

The Core Security Assessment is a consultative engagement that leverages the industry leading and award-winning suite of actionable insight solutions to diagnose access risk, existing vulnerabilities and advanced threats in your organization and arms you with actionable information and insights.

The Core Security Assessment reduces the complexity of the information you need to understand, providing immediate visibility into the following:

- Access Risk
  - Abandoned accounts - accounts that have been inactive for a time period that exceeds policy
  - Privileged accounts - accounts with increased levels of permission that provide elevated access to critical networks, systems, applications or transactions
  - Hidden entitlements – entitlements that exist but are difficult to detect because of inheritance or indirect assignment
- Vulnerability Risk
  - Prioritization and validation of vulnerabilities based on exploitability, business need, and asset classification
  - Demonstration of how to eliminate false positives
- Network Risk
  - Advanced detection to observe egress, proxy and DNS traffic
  - Identification of suspicious behaviors and content
  - Prioritization based on risk scores

By correlating the risk data from these 3 different areas, we will help you understand what role an exploited vulnerability may have played to allow a resource to become compromised as well as emphasizing what other resources are still at risk.

Assessment Findings

- 100% of the machines identified as infected by Core were in fact infected
- Targeted remediation efforts reduced the chances of needing to perform future preventative restores

Large Regional Healthcare Provider

- HIPAA compliance goal, focused on CVSS 7 and higher vulnerabilities
- Found and patched 900,000 vulnerabilities
- Six person-months of effort

Assessment Findings

- Discovered 100,000 additional vulnerabilities, 526 of them exploitable
- Discovered 15 direct paths to critical database
- Total effort: < 1 minute

How It Works

The Core Security Assessment follows a proven methodology to assess three distinct risk components:

Access Risk: An Access Insight discovery tool is downloaded from the Core Security web site and run by you --- no software installation is required. This discovery tool automatically scans your Active Directory structure. Following the scan, a Core Security consultant will import the scan results into the Access Insight solution using a virtual image we provide (no software installation is required) and will use Access Insight to highlight areas of access risk.

Vulnerability Risk: A Core Security consultant will ask you a few questions about your network environment and the existing vulnerability scanners you have deployed. If you currently do not use a vulnerability scanner, we can provide one for the assessment process. Using this information, we will configure a virtual appliance for you to download and install in your environment. We will then assist with the import of vulnerability data as well as the configuration of how that data is prioritized. This will all be done through our on-premise, web-based management console.

Threat Detection: Similar to the Vulnerability Risk assessment process, a Core Security consultant will ask you several questions about your network configuration, including available SPAN port(s) or TAP(s), egress points, speed of internet pipe, etc. Using this information, we will configure a physical appliance and ship to you. Once attached to your network, this appliance will monitor network traffic for several days looking for abnormal behavior.

Using data from the three components above, Core Security will produce a detailed report of its findings to be used to help establish a baseline for remediation. We will also provide detailed demonstrations of the solution capabilities.

ABOUT CORE SECURITY

Core Security provides market-leading, threat-aware, identity, access and vulnerability management solutions that provide actionable intelligence and context needed to manage security risks across the enterprise. Solutions include multi-factor authentication, provisioning, Identity Governance and Administration (IGA), Identity and Access Intelligence (IAI), and Vulnerability Management (VM). The combination of these solutions provides context and shared intelligence through analytics, giving customers a more comprehensive view of their security posture so they can make better security remediation decisions and maintain compliance.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

CORE SECURITY

11/2016