GuardiCore

Multi-Method Breach Detection Spotlight: Using Reputation Analysis for Data Center Breach Detection

Organizations spend millions on security measures to safeguard their networks and data centers against external threats. Yet breaches take place with stunning frequency and threats can dwell undetected for weeks or months before attacking their targets. The longer it takes to detect and contain a breach, the more damage it can inflict and the costlier it becomes to resolve. As noted in the Ponemon Institute's 2016 Cost of a Data Breach Study, "Time to identify and contain a data breach affects the cost… Our study shows the relationship between how quickly an organization can identify and contain data breach incidents and financial consequences." There's no question that strong perimeter defenses are essential, but it's clearly time to place at least equal emphasis on earlier breach detection and faster incident response within the data center.

When Something's Just Not Right

Modern data centers and clouds divide workloads by tasks and functions to increase speed and scale, which helps make more efficient use of compute power. Servers generally communicate on east-west pathways (laterally within the data center) with a select group of hosts, and occasionally on north-south (externally connected) pathways. Ideally, they are being monitored, patched and updated with the latest software.

Even though the functions and interactions of these servers are well defined, that alone does not make them secure. On the contrary, these servers are prime targets for attacks. Because they have the ability and permission to connect to sensitive data sources and pathways, attackers frequently try and use them as launching points to attack other parts of the data center. Malicious processes, which often have the same name and file attributes as an authentic process but don't have a certified file hash, will attempt communication actions, such as network scans or trying to connect with valid servers using non-standard protocols or ports.

Security teams need a way to recognize when servers are acting suspiciously. The root causes will not be obvious or transparent.

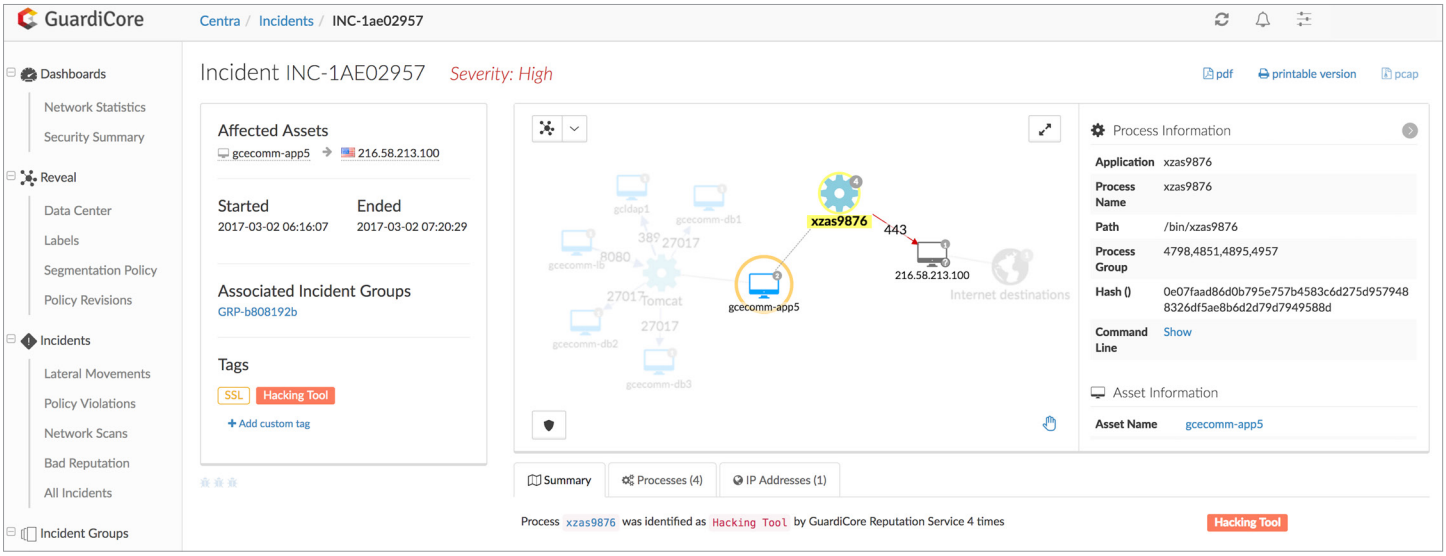
Multiple Detection Methods Detect Breaches Faster

- **Dynamic Deception**
  A redirection architecture and dynamically generated live environments engages attackers and identifies their methods without disrupting data center performance.
- **Policy-Based Detection**
  Security policies at the network and process levels enable instant recognition of unauthorized communications and non-compliant traffic.
- **Reputation Analysis**
  Detects suspicious domain names, IP addresses and file hashes within traffic flows providing comprehensive breach detection.

Accelerate Breach Detection With Reputation Analysis

The GuardiCore Centra™ Security Platform packs a full arsenal of breach detection methods, including robust reputation analysis capabilities. Reputation analysis is aimed at identifying threats based on suspicious domain names, IP addresses and file hashes associated with known malicious activity. Non-conforming or unauthorized communications are an indicator of compromise—for example, malware installed on a server and attempting to communicate with a known bad IP address or domain name.

Reputation analysis adds a valuable early-warning dimension to your breach detection capabilities. It leverages GuardiCore's vast network of attack sensors and deception engines, combined with regular threat intelligence feeds and the insights of our security analysts. The platform also has the ability to distinguish "negative processes" indicating the presence of an untrusted asset that warrants investigation.



GuardiCore Reputation Services *identifies a malicious process using reputation-based analysis.*

Corner Your Adversaries with Multiple Detection Methods

Reputation analysis is just one of several methods the GuardiCore Centra Security Platform uses to improve real-time breach detection and response. Working in conjunction with each other, these complementary methods also include:

- Dynamic deception, which employs real data center servers, IP addresses, operating systems and services as decoys that actively seek out suspicious activity at the first indication, engage with it and redirect it to a containment area for threat confirmation and investigation.
- Policy-based detection, which uses segmentation policies to implement security controls around individual or groups of applications within the data center. Any policy violation, such as an unauthorized communication attempt, automatically triggers an alert to initiate an investigation.

Deploying these three methods simultaneously forms a strong security net, virtually ensuring that any live breach in the data center is caught, mitigated and contained for in-depth investigation.

Learn more about GuardiCore's comprehensive data center breach detection capabilities at **www.guardicore.com**

About GuardiCore

GuardiCore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to stop advanced threats through real-time breach detection and response. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers.