SOLUTION BRIEF

Guardicore

Threat Detection Spotlight: Using Reputation Analysis for Breach Detection

Organizations invest heavily in security measures to safeguard their on-premises and cloud infrastructure from external threats. Yet breaches continue to take place with stunning frequency, and attackers can dwell undetected for weeks or months before initiating attacks against specific 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 2018 Cost of a Data Breach Study, "The faster the data breach can be identified and contained, the lower the costs. ...our study reports on the relationship between how quickly an organization can identify and contain data breach incidents and the financial consequences." There's no question that proactive security measures are essential, but it's clearly time to place at least equal emphasis on earlier breach detection and faster incident response across data center and cloud environments.

Lateral Movement: A Growing Threat

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 to use them as launching points to attack other parts of the infrastructure. Malicious processes, which often have the same name and file attributes as an authentic process but lack a certified file hash, will attempt communication actions, such as network scans or connection attempts with valid servers using non-standard protocols or ports.

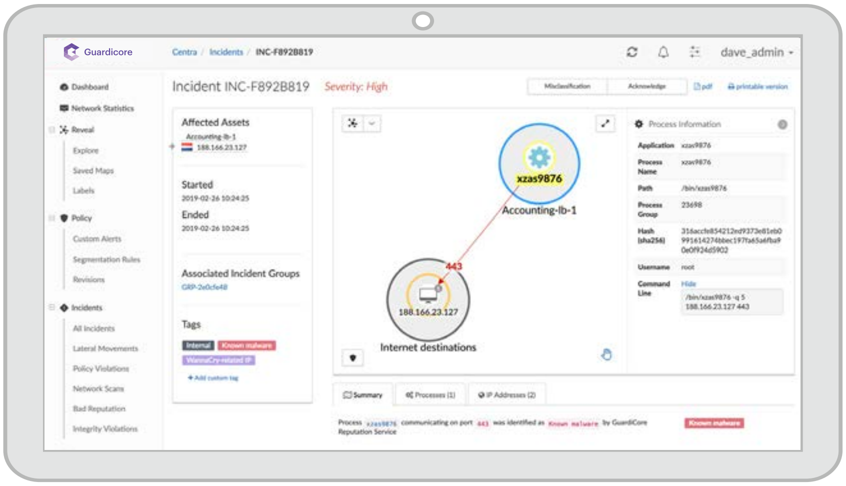
Security teams need a way to recognize when servers are acting suspiciously. The existence and root causes of these activities are generally not clearly visible.

Multiple Detection Methods for Faster Breach Detection

- **Policy-Based Detection**
  Security policies at the network and process levels enable instant recognition of unauthorized communications and non-compliant traffic.
- **Dynamic Deception**
  A redirection architecture with dynamically generated live environments engages attackers and identifies their methods without disrupting application performance.
- **File Integrity Monitoring**
  Discovers, profiles, and monitors key files and alerts the security team of unsanctioned modification or deletion of system files, configuration files, or content.
- **Reputation Analysis**
  Detects suspicious domain names, IP addresses and process/file hashes within traffic flows, drawing from both the Guardicore Global Sensor Network and customer-provided feeds.

Accelerate Breach Detection with Reputation Analysis

Guardicore Centra™ features an integrated set of breach detection capabilities, including robust reputation analysis and detection. Reputation analysis identifies 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.



Incident INC-F892B819 Severity: High

Affected Assets
Accounting-lb-1
188.166.23.127

Started
2019-02-26 10:24:25
Ended
2019-02-26 10:24:25

Associated Incident Groups
GRP-2e0cfe48

Tags
Internal Known malware WannaCry-related IP

Process Information
Application xzas9876
Process Name xzas9876
Path /bin/xzas9876
Process Group 23698
Hash (sha256) 316accfe854212ed9373e81eb0991614274bbec197fa65a6fba90e0f924d5902
Username root
Command Line Hide /bin/xzas9876 -q 5 188.166.23.127 443

Process xzas9876 communicating on port 443 was identified as Known malware by GuardiCore Reputation Service Known malware

Guardicore reputation services identifies a malicious process using reputation-based analysis.

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, third-party and customer-provided threat intelligence feeds, and the insights of our security analysts. Centra also has the ability to distinguish "negative processes" indicating the presence of an untrusted asset that warrants investigation.

Corner Your Adversaries with Multiple Detection Methods

Reputation analysis is just one of several methods Guardicore Centra uses to improve real-time breach detection and response. Additional complementary methods include:

- Policy-based detection, which uses segmentation policies to implement security controls around individual or groups of applications within data center and cloud environments. Any policy violation, such as an unauthorized communication attempt, automatically triggers an alert to initiate an investigation.
- Dynamic deception, which employs real servers, IP addresses, operating systems and services as decoys that actively seek out suspicious activity, engage with it, and redirect it to a containment area for threat confirmation and investigation.
- File integrity monitoring, which discovers key application files, profiles them, and monitors for unauthorized changes or deletions. Successful scans are logged for attestation purposes and exceptions generate timely alerts.

Deploying these techniques simultaneously forms a strong security net, virtually ensuring that any live breach in the data center is detected, contained, and recorded in detail for in-depth investigation.

About Guardicore

Guardicore is a data center and cloud security company that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security — for any application, in any IT environment.

More information is available at www.guardicore.com