LOGRHYTHM LABS EMBEDDED EXPERTISE

Security Analytics Suite - Honeypot

LogRhythm™

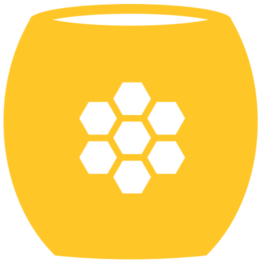
Cyber attacks are becoming increasingly targeted in nature, making it imperative for organizations to deploy security tools that enable the detection and prevention of targeted attacks. When deployed and analyzed correctly, honeypots provide organizations with an increased awareness of attack and breach activity generating dynamic threat research unique to the customer environment they are targeting.

Honeypots are isolated systems that are designed to look like part of the corporate network such as web servers running enterprise applications. These decoy systems are easy to exploit, making them an attractive target for opportunist attackers. All activity on the honeypot can be attributed to nefarious activity since there is no valid reason to access these systems. By monitoring honeypot activity, an organization can learn about targeted threats and leverage this information to understand who they are being targeted by, what information their adversaries are seeking, and how attack patterns will look within the network, allowing for proactive threat defense.

The Honeypot Security Analytics Suite delivers

- ☑ Real-time event contextualization across multiple dimensions
- ☑ Improved risk-based prioritization
- ☑ Forensic visibility into malware attack vectors and patterns
- ☑ Tight integration for consolidated threat management

LogRhythm's Honeypot Security Analytics Suite



LogRhythm's Honeypot Security Analytics Suite allows customers to centrally manage and continuously monitor honeypot event activity for adaptive threat defense. When an attacker begins to interact with the honeypot, LogRhythm's Security Intelligence Platform begins tracking the attacker's actions, analyzing the honeypot data to create profiles of behavioral patterns and attack methodologies based on the emerging threats. This automated and integrated approach to honeypots eliminates the need for the manual review and maintenance associated with traditional honeypot deployments.

The Honeypot Security Analytics Suite provides AI Engine rules that perform real-time, advanced analytics on all activity captured in the honeypot, including successful logins to the system, observed successful attacks, and attempted/successful malware activity on the host. As a result, the Honeypot suite allows AI Engine to also detect when similar activity captured from the honeypot is observed on the production network. For example, if an observed attacker interaction on the honeypot is followed by a subsequent interaction with legitimate hosts within the environment such as production web servers, LogRhythm can generate an alarm alerting IT and security personnel to the suspicious activity.

In addition to advanced analytics rules, the Honeypot Security Analytics Suite features prebuilt investigations, dashboard layouts, lists, and Smart**Response**™ plugins to automate actions based on observed activities. Investigations and layouts enable analysts to quickly view and understand data collected from the honeypot, providing details on top attacker IP addresses, usernames, passwords, payloads, impacted applications, etc. This information automatically updates lists that can be leveraged in the system and initiates Smart**Response**™ plugins that programmatically add attackers to integrated security tools such as firewalls and access control systems to prevent known bad actors for accessing the production environment.

LogRhythm's Honeypot Security Analytics Suite generates threat intelligence specific to the targeted environment, allowing organizations to identify their adversaries, recognize their attack patterns, and take the necessary steps to prevent attacks from infiltrating the corporate network. Research from the LogRhythm Labs team is continually embedded in the suite.

Honeypot Security Analytics Suite in Action

Prevent Compromised Credentials

Challenge The majority of attacks exploit valid user credentials to gain unrestricted access to the corporate network. Organizations need an effective means of monitoring for insecure accounts and passwords to prevent credentials from being compromised.

Solution LogRhythm's Honeypot Security Analytics Suite provides AI Engine rules that monitor for successful and unsuccessful logon attempts to honeypot servers, capturing details on the username and password. This allows analysts to see commonly attempted username and password combinations on the honeypot hosts.

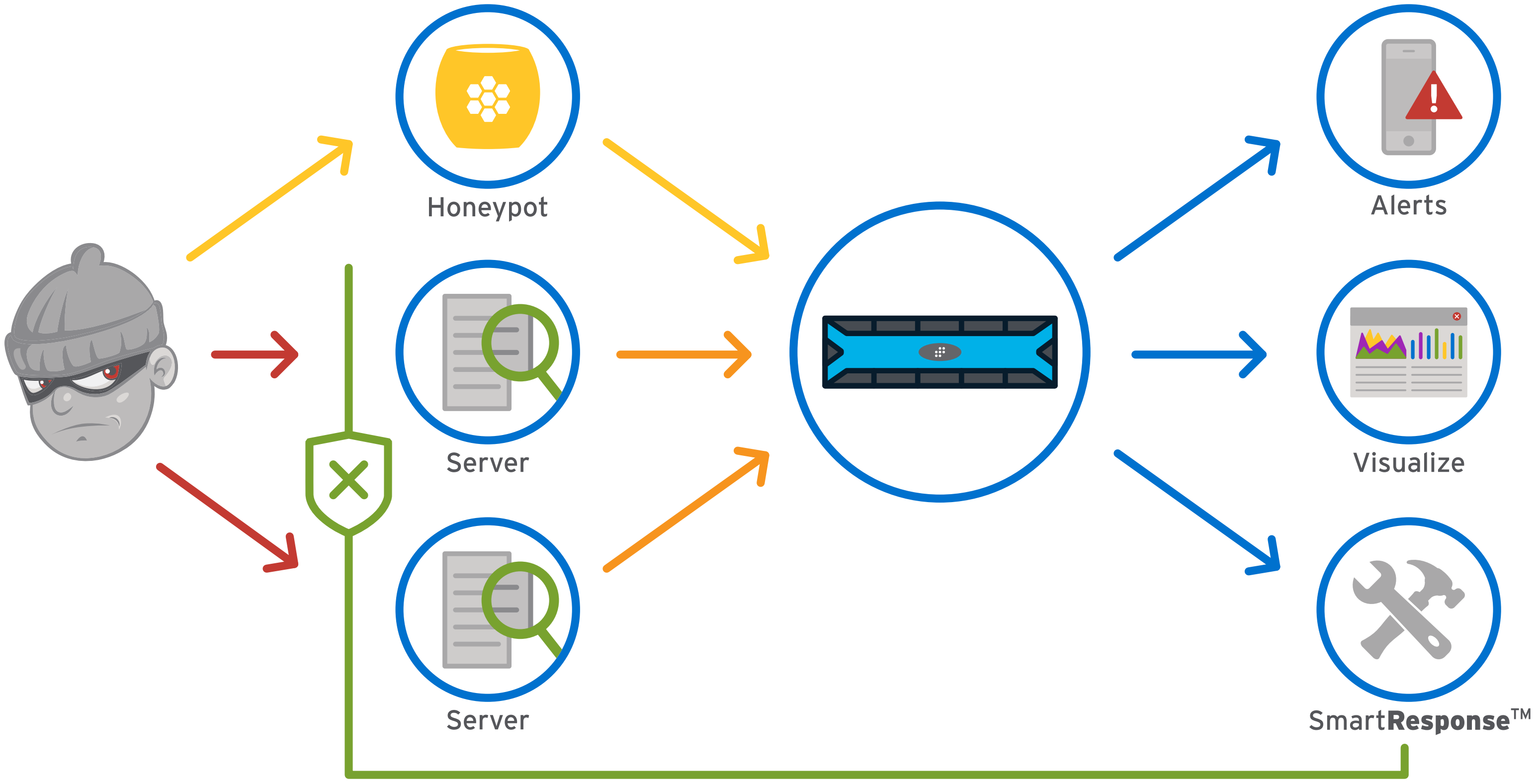
Additional Benefit By knowing which accounts are being targeted by hackers and which passwords are vulnerable to exploit in the honeypot, organizations are able to strategically increase defense measures within their network by monitoring at-risk user accounts and enforcing stricter password policies. A Smart**Response**™ plugin can automatically add the IP address observed in the honeypot to a firewall list to prevent interaction with the corporate network.

Detect Zero Day Malware

Challenge With the evolving sophistication and rapid propagation of new cyber attack campaigns, it is difficult for organizations to detect zero day exploits using traditional security tools because they lack the signatures and behavioral profiles needed to spot targeted malware.

Solution LogRhythm's Honeypot Security Analytics Suites attracts attackers to a honeypot server configured for optimal surveillance. When a honeypot host is successfully compromised, LogRhythm captures the full details about how attackers gained access along with the subsequent host interactions. Additionally, LogRhythm AI Engine rules capture and parse out all attempted malware and exploit downloads including communication with Command and Control servers.

Additional Benefit This data allows the security team to perform detailed threat analysis, giving them new insight into upcoming malware payloads and attack methodologies employed by adversaries. LogRhythm also captures additional environment data, such as user-agent strings, which highlight the tools that attackers or bots are using to breach networks. Smart**Response**™ plugin can automatically add the attackers to an internal threat list to block access to the corporate network.


Honeypot
Server
Server
Alerts
Visualize
SmartResponse™