



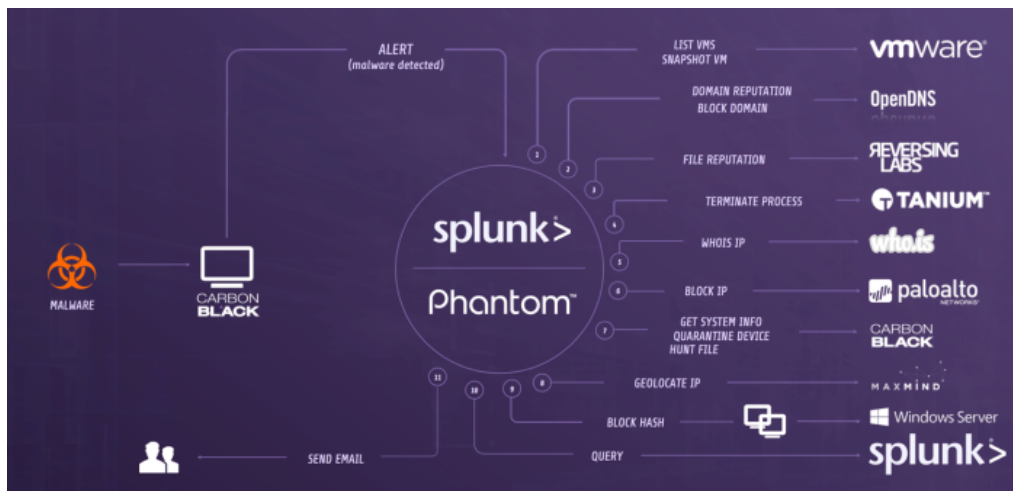
## Phantom Automation – Splunk Data Driven Response Action

Let your SIEM take automated action to the common security remediation

Spico is a leader in Splunk Enterprise Security deployments. With our customer battling Malware on a daily bases we realize how noisy security indicators can become. With a lot of exploits being common across an organization or organizations the remediation process is a repetitive task SOC analyst have to perform over and over. Leveraging Phantom with Splunk Enterprise Security can save time and money from common security incidents.

### Phantom + Splunk Enterprise Security Benefits:

- Playbook creation for common security tasks
- Sharable playbooks for a variety of common security investigations
- Allowing small SOC teams of 2 or 3 to act as 10 security analysts
- Complete automation of detection and remediation
- Data Driven Security Decision from Splunk ES to any remote device



Spico Solutions can help any organization get from point A to point B with regards to Splunk Enterprise Security and Phantom automated Security response.

For more information please reach out to [info@spicosolutions.com](mailto:info@spicosolutions.com) or call us at 760.510.6795

SPICO SOLUTIONS|SPICOSOLUTIONS.COM|2137 NEW CASTLE AVE, CARDIFF, CA 92007