SirviS MDR

MDR Description

SirviS MDR includes 24/7 coverage, threat insights, proactive notifications, consultations on handling threats and false positives. In addition, MDR includes threatresponse, meaning they will take action on all false positives and true positives.

We are a 100% in-house, non-outsourced Team of Tier-1, Tier-2, and Tier-3 cybersecurity experts monitoring thousands of endpoints. Our mission is to augment customer security organizations by providing a second set of eyes on the SentinelOne deployment and appropriate responses to contain threats. SirviS MDR empowers customers to focus only on the incidents that matter making it the perfect endpoint add-on solution for overstretched IT/SOC Teams.

Which events are analyzed by the service?

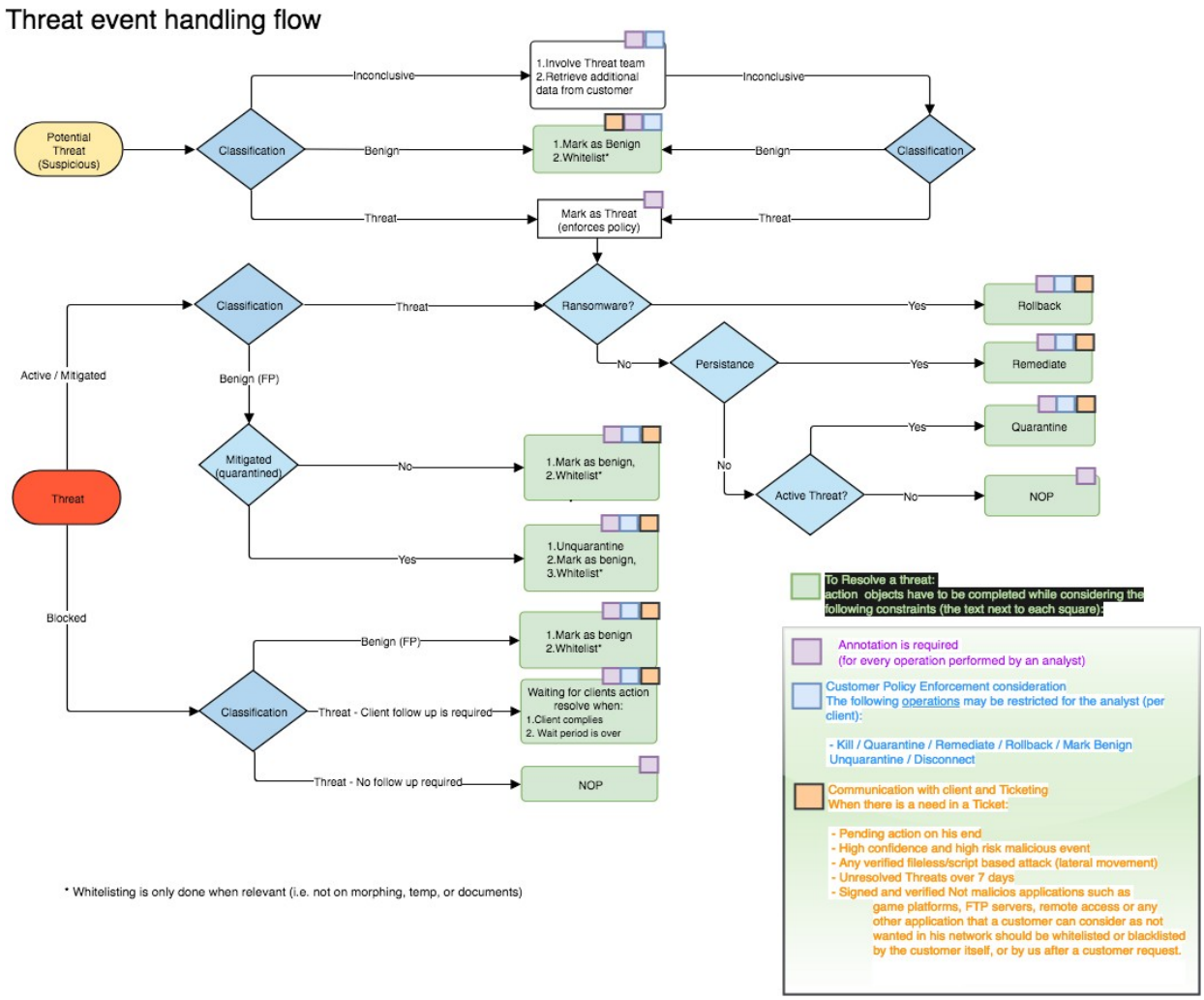
SirviS' security operations team analyzes and adds threat insights (annotation) to all unresolved events on the console. SirviS MDR customers have the added benefit of the analysts taking mitigation action and resolve action as required. If the customer resolves a threat before a SirviS analyst gets to it, the threat will not be analyzed or annotated, as it will be considered "Resolved" by all means.

What's Included?	
24X7 MDR	• Every console threat is, reviewed, acted upon, and documented • Full response capabilities • Proactive Notifications
HUMINT	• Intelligence-based hunting for attacker techniques, global APT campaigns, and emerging cybercrimes • Threat bulletins & alerting if/when threats are detected in your environment
Threat Response SLA	• 2-hour/4-hour own/investigate • The fastest MDR on the planet • Analyst triage, verdict, and initial actions
QUARTERLY SECURITY REVIEW	• Consultation guiding long-term remediation and security architecture • Agent version alignment & exclusions review • Threat / actor trends

SirviS MDR

What do the SOC analysts do when they see an event?

The following diagram illustrates a simplification of the process done by our analysts on an ongoing basis.



EXPERT STAFF	TRUSTED	VALUE	HUMINT
Never Outsourced	By the World's Largest Organizations	MDR & DFIR Reduce SOC Workload	Includes Intel-Based Threat Hunting

SirviS MDR

Which data points are used in the threat classification process?

There are multiple data points which are used in the classification process. Some are available in the console in plain sight and just need analysis experience and others, which are more low level or integrate other data sources. The main sources are listedbelow:

- Threat data
    - Process actions
    - File manipulation
    - Registry
    - Outbound IP connections
    - Filename / path
    - S1 Risk
    - Publisher (and cert validity)
    - Static indicators (DFI detections)
    - Dynamic indicators (DBT / Fileless detections)
- AV reputation (Virustotal and Reversing Labs)
- SHA1 reputation among S1 customers (over 2M agents)
- Raw data (OSevent information)
- Proactive agent log analysis
- Deep Visibility cross reference (in advanced attacks, when feature exists)

When will SirviS notify me via email?

Due to the proactive nature of the service (it initiates issue/requests to the customer), every onboarded customer is asked to an email address or contact so the SOC analysts don't need to guess who to send the note to. The analysts will create notifications in the following scenarios:

- Pending action on customer's end
- High confidence and high risk malicious event (Fileless, APT, Ransomware, etc)
- Any verified fileless/script based attack (lateral movement)
- Unresolved Threats over long duration of time (Monitoring tier)