ALERT LOGIC™

Battlecard: Secureworks

Secureworks

	SOC Capabilities	Cloud Services	Price Analysis
Characteristics:	• 15-minute SLA for MSSP • Taegis XDR 1 hour SLA • Secureworks Threat Intel team in house	• Deployment across AWS and Azure only • Container support for Kubernetes through Redcloak	• Will collect from network-based nodes w/out charging additional • Push to primarily sell Taegis platform over Secureworks MSSP
Weakness:	• Integrations only for US1 Region • 1 hour SLA for Taegis • Not living up to SLAs	• Delve based vuln scan not integrated with console, not PCI compliant • Additional charge for IDS in cloud	• Not profitable and a much older company than AL • Vulnerable to change in Dell vision and company churn
Considerations:	• Taegis does not include IDS, built primarily for endpoints • Redcloak rebrand support only Windows and Linux (Red Hat & CentOS) • Taegis console is designed as a monitoring UI only, showing what work has been done.	• Multiple integration points • Limited AWS integrations (GuardDuty, ALB, WAF, VPC, Cloudtrail) • US2 and EU regions lack integration support • Deployment in AWS is tedious and requires multiple steps	• Minimum of 500 endpoints for purchase at $85,000 • Anything below 500 endpoint must go directly through Dell • Deployment surcharge or $30k • Under 500 endpoint does not come with the 40 hours of IR

Secureworks Quick Facts Battlecard

What they do:

- 24/7 SOC support through Taegis with a 60-minute SLA
- Leverages telemetry through persistent mechanisms, anomalous user activity, threat actor tactics, network communication and anomalous app usage.
- Offers up to 40 hours of IR per quarter, forfeiture of excess hours at end of quarter
- Provides internal Secureworks Threat Intel team

Questions to ask:

- What built in reports do you need for your day to day?
- Do you need the ability to create playbooks in the console?
- Is it within budget to forgo any unbilled retainer hours?
- Are you comfortable with the new Taegis software transition?
- Is there a need for a faster response time than a 60-minute SLA?
- Businesses outside of the supported US1 region are limited in integrations, are you comfortable with that?
- Are you a cloud-based customer, if so, are you ok with limited visibility inside the cloud?

Secureworks Disadvantages:

- Marketed as a next gen SIEM but does not actually run correlation or playbooks
- Forced to create playbooks with SOC, unresponsive due to limited SOC personnel
- Deployment is considered fulfilled after 40% of agents have been deployed for Red Cloak agents and the Taegis XDR collector
- Lack of full support for US2 and EU regions. Full integrations offered are not supported in US2 and EU.
- Taegis is primarily a Red Cloak rebrand with a heavy focus on telemetry from deployed Red Cloak agents.
- Deployment process in the cloud is cumbersome, requires in house technical expertise to deploy

Secureworks Advantages:

- Offer compliance-based assessments as Pro Services
- Capable of performing digital forensics through IR team
- Multiple integrations within the US1 region
- Red Cloak agent collects, command line parameters, thread injection events, binaries, executables, DLLs, registry modifications, network connections, DNS requests, Windows logs and Disk/Memory artifacts.
- Provides customers with a TEM (Threat Engagement Manager and CSM for recommendations, teleconferences and quarterly SPR (Security Protection Reviews).