The Value of SOCAutomation

HONEYCOMB

socautomation™

Automated Security Operations

ROI and Automation Metrics

This is how SOCAutomation drastically reduces costs, whilst at the same time, increases coverage and visibility

*Comparing Traditional SOC Incident Response to **SOCAutomation SOC Incident Response***

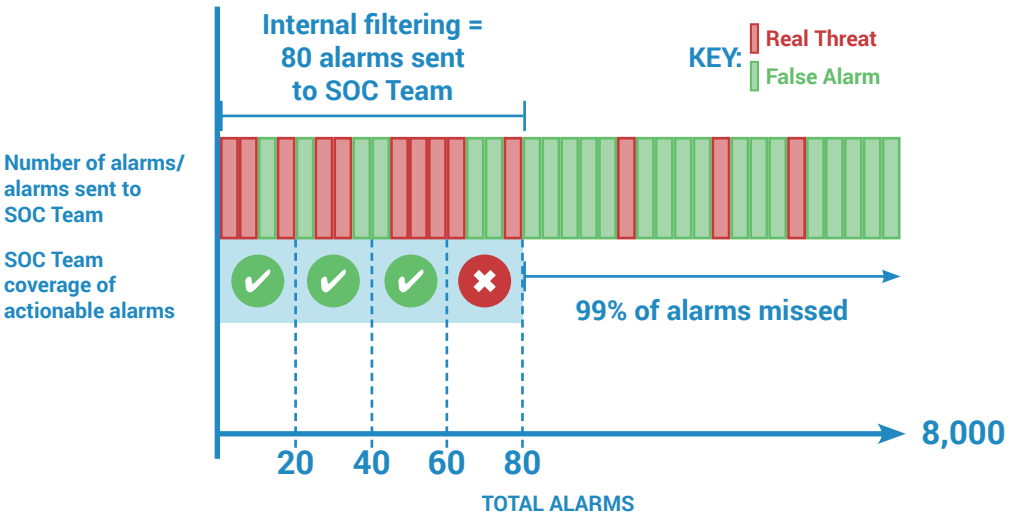
Traditional SOC Incident Response – NO AUTOMATION

Scenario – an organisation with:

- 60,000 devices
- 15 business units
- 5 MIS teams
- 3 locations
- 3 outsourcers
- SOC Team of 20 analysts

	ALARM TYPES				
	Virus/phishing	Recon/scanning/ DDoS	Access control	Compliance/ regulatory	Other
8,000 unfiltered alarms per day, of which, 80 (1%) are 'tuned'	41.6 (52%)	23.2 (29%)	7.2 (9%)	4.8 (6%)	3.2 (4%)
Total time spent per tuned alarm, per analyst	265 Minutes	310 Minutes	60 Minutes	80 Minutes	120 Minutes

An average of 3 alarms can be covered per analyst. Out of the 80 alarms sent to the SOC Team, 20 are still left unchecked and unresolved



- Some of the actionable alarms sent to SOC Team turn out to be false positives
- 60/80 of the actionable alarms are covered by the SOC Team daily incident overrun of +20 alarms
- 99% of all alarms are unchecked from the offset - some of these could be real threats ignored
- The SOC Team are constantly firefighting against an unmanageable level of alarms

The Value of SOCAutomation

HONEYCOMB

socautomation™

Automated Security Operations

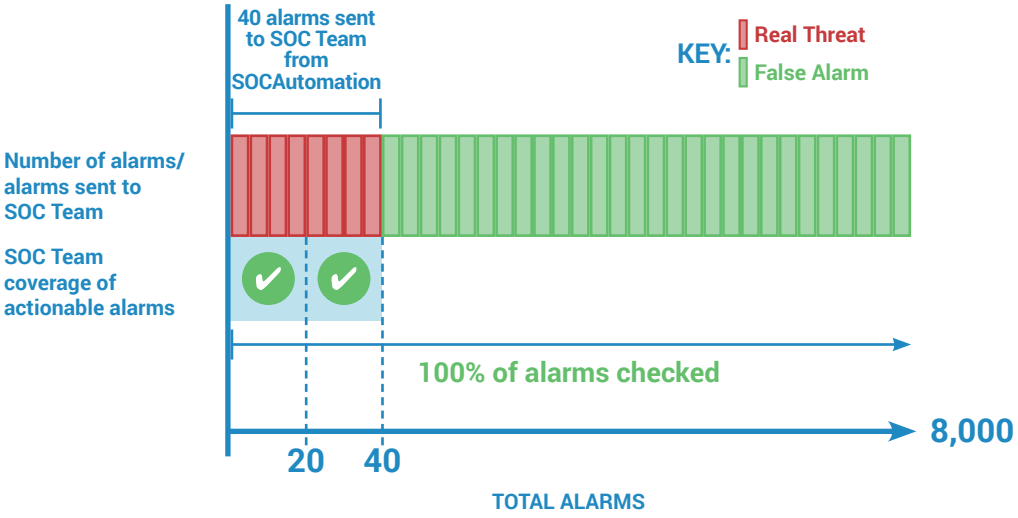
SOC Incident Response – WITH SOCAUTOMATION

Scenario – an organisation with:

- 60,000 devices
- 15 business units
- 5 MIS teams
- 3 locations
- 3 outsourcers
- SOC Team of 20 analysts

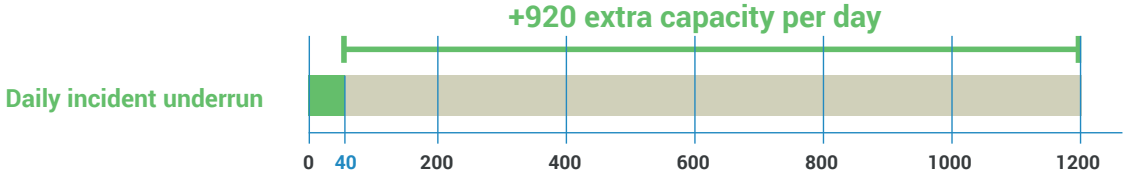
	ALARM TYPES				
	Virus/phishing	Recon/scanning/ DDoS	Access control	Compliance/ regulatory	Other
8,000 unfiltered alarms per day, of which, 8,000 (100%) are 'tuned'	3,120 (52%)	1,740 (29%)	540 (9%)	360 (6%)	240 (4%)
Total time spent per tuned alarm, per analyst	12 Minutes	12 Minutes	8 Minutes	9 Minutes	9 Minutes

SOCAutomation creates the ability of 48 alarms to be covered per day, per analyst. This allows 1 analyst, out of your 20-strong team, to cover all actionable alarms



- The actionable alarms sent to the SOC Team have been halved from 80 to 40
- With SOCAutomation, 1analyst has the ability to cover all actionable alarms
- SOCAutomation's Automated Feedback Service (AFS) and machine learning engine depicts the real from the false alarms
- 100% of alarms are checked and verified by SOCAutomation

Net-Gain with SOCAutomation



A net-time of 920 alarms has been gained per day - this means that the majority of the SOC Team can be reallocated to conduct more beneficial security tasks for the organisation

www.socautomation.co.uk