INVESTING IN THREAT HUNTING CAPABILITIES

Malware is more evasive than ever, and signature-based antivirus and traditional defenses are getting worse at stopping advanced threats. IT security teams are increasingly leveraging machine learning, threat intelligence and behavioral analytics to identify anomalies and eliminate threats.

PROACTIVE THREAT HUNTING IS INCREASING

YES Will be building a threat hunting program within three years

AUTOMATING THREAT HUNTING IMPROVES DEFENSE

64% Improving detection of advanced threats

63% Reducing investigation time

59% Saving time from manually correlating events

53% Reducing time wasted on chasing false leads

50% Discovering threats that could not be discovered otherwise

49% Creating new ways of finding threats

92% OF ORGANIZATIONS THAT ADOPT A THREAT HUNTING CAPABILITY ARE UNCOVERING THREATS MORE QUICKLY

2.5x speed improvement of threat detection and response **WITH a threat hunting platform**

92% with **75%** without

5% with **12%** without

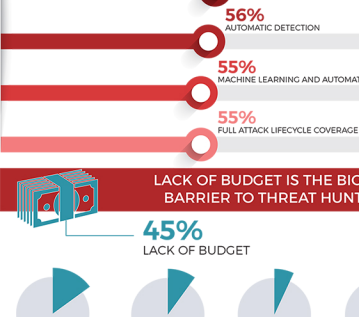
2% with **4%** without

1% with **3%** without

0% with **4%** without

1% with **2%** without

THREAT INTELLIGENCE MOST SOUGHT AFTER THREAT HUNTING CAPABILITY



LACK OF BUDGET IS THE BIGGEST BARRIER TO THREAT HUNTING

45% LACK OF BUDGET

BUDGET REMAINS THE MOST SIGNIFICANT BARRIER

SecureOps empowers IT security teams with leading edge threat hunting capabilities in order to identify threats, reduce response times and improve overall defense.

Over 84% of those surveyed feel that threat hunting should be a top security priority

But only 3 out of 4 surveyed feel they're spending enough time on it.

secure OPS