SMOKESCREEN

5 Ways The Most Successful CISOs Stop Attacks

Leading companies are changing their approach to cyber-security*.
Here are the top 5 ways they've adapted:

1. **Focusing on detection and response**
   Preventive controls are ineffective against modern attacks that always find a foot in the door. Modern practitioners assume compromise has occurred, and build detection & response capabilities, instead of trying to plug every single loop-hole.

2. **Making security alerts actionable**
   In an average week, companies face 17,000 security alerts, most of which are false alarms that lead to real problems not being dealt with in time. CISOs are opting for technologies with very low false positives (less than 1% of alerts), freeing security teams to act on real threats instead of false positives.

3. **Increasing internal network visibility**
   'Dwell time' (how long an attacker is in the internal network) is usually measured in months or years long. Top security leaders are focusing on internal network visibility to reduce the dwell time to minutes and prevent business damage.

4. **Removing the human element in monitoring**
   Analysts monitoring screens in shifts has proved ineffective as people can't find suspicious patterns in huge volumes of security data. CISOs of leading companies now favour automated attack detection which reduces dependence on human analysts and lowers operational costs.

5. **Catching attacks early with threat intelligence**
   Detecting an attack during the planning stage is incredibly powerful as it can be mitigated before it begins. CISOs are setting up early warning systems to detect when they are targeted and give the security team the time advantage.

** Sources: Analysis of targeted attacks in the last 3 years, surveys of leading C-level executives tasked with security, and 2014 - 2015 industry research reports.*

Smokescreen detects targeted attacks
while saving millions wasted on false positives.

Click Here To Learn More