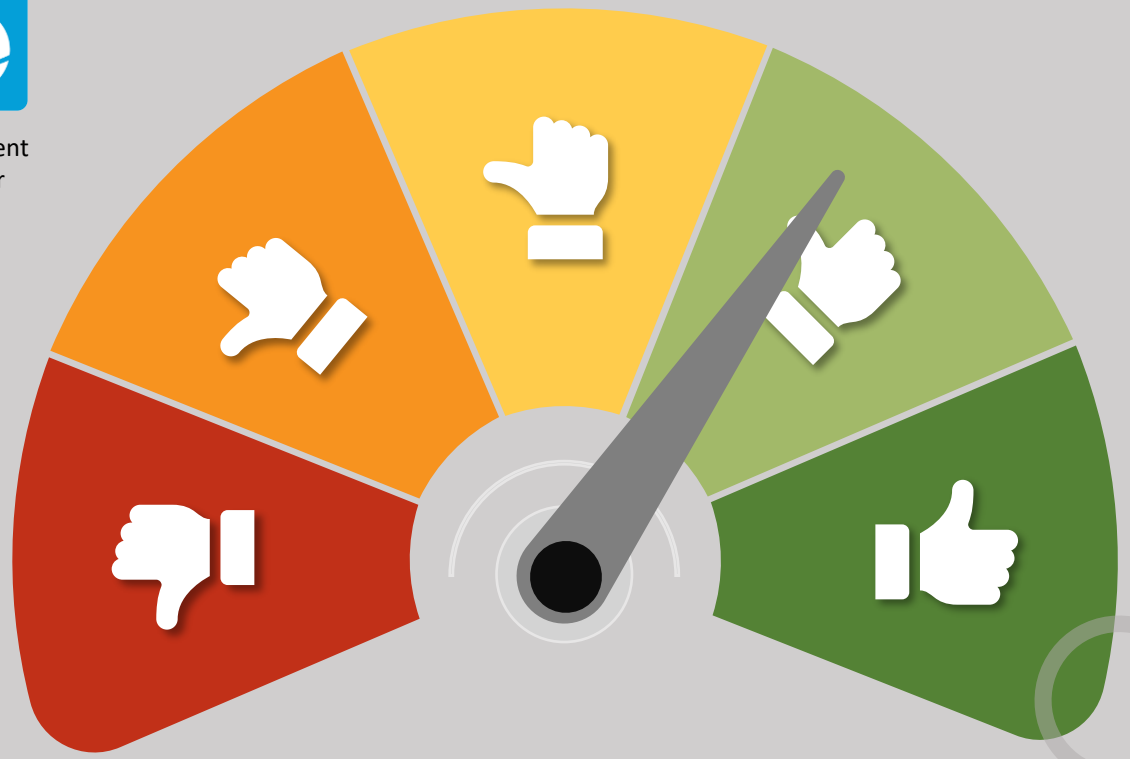
Naiden Nedelchev © 2024

# SOC Maturity Scale with Tools



## Not in place

## Only works on alerts

Windows Event Viewer

Linux Event Viewer

Cisco Event Viewer

## Holistically logs data and security events centrally

Nagios Log Server

KIWI Syslog Server

DATADOG

## Systematically adopts and applies best practices

THE CYBER KILL CHAIN®

MITRE ATT&CK

The Diamond Model of Intrusion Analysis

## Looks at trends and conducts threat hunts

splunk>

SWIMLANE

Azure Sentinel