Key Strategies for Running a World-Class Security Operations Center

Dr. Eric Cole
The Challenge
The Changing Landscape
Navigating the SOC Battle Field
Consolidation / Authority

Navigating the SOC Battle Field
Navigating the SOC Battlefield

Consolidation / Authority

Metrics / Value
Navigating the SOC Battlefield

Consolidation/Authority

Metrics/Value

Technology
Navigating the SOC Battlefield

- Consolidation/Authority
- Metrics/Value
- Technology
- Staff
Navigating the SOC Battle Field

- Value of Data
- Technology
- Staff
- Metrics/Value
- Consolidation /Authority
Navigating the SOC Battle Field

- Value of Data
- Communicate
- consolidation/authority
- Metrics/Value
- Technology
- Staff
Truths & Lies
SOC Checklist

- Clearly define the objectives and what constitutes success - Plan “long term”, execute “short term”
- Determine metrics to identify what is working and what is not
- Learn, configure and become one with your tools
- Utilize experts/outsourcing to increase effectiveness
- Determine storage capabilities and critical data sources
Thank you for your time

Dr. Eric Cole

Twitter: @drericcole

ecole@secureanchor.com
eric@sans.org
www.securityhaven.com