

The background features a dark blue gradient with faint, light blue concentric circles and degree markings (40, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) scattered across the left side, suggesting a technical or analytical theme.

THREAT DETECTION AND RESPONSE

*Strategies for Success
by Varun Acharya*

ABOUT ME

- CISO at Healthscope
- 12 years professional Cyber Security experience
- Industries – Higher Education, Banking and Finance, Manufacturing, Healthcare
- Specialisations – Identity and Access Management, Security Operations, Cyber Threat and Vulnerability Response

DISCLAIMER

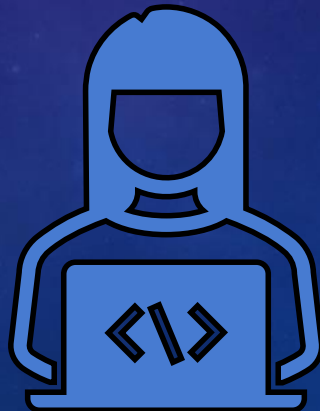
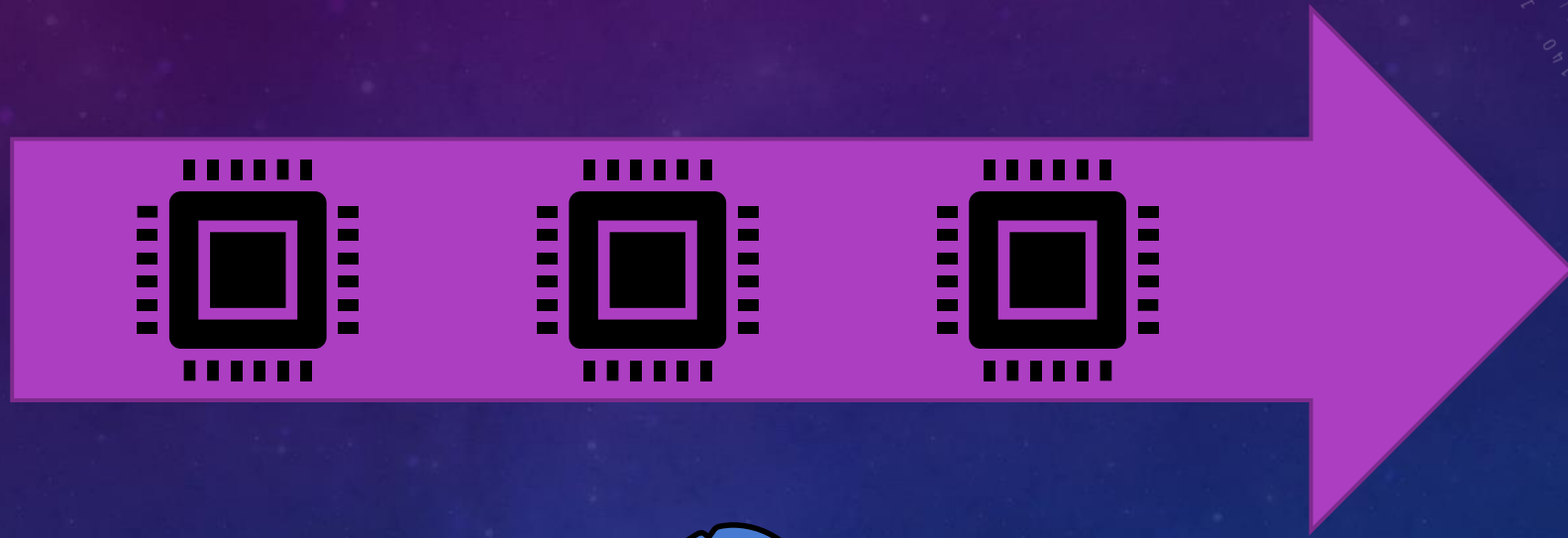
- The opinions expressed in this session are solely my own and do not express the views or opinions of my employer.
- This is not meant to be an exhaustive coverage of the topic. You may already know these things, or you may learn something new today. In either case, I welcome your feedback.



SECURITY RESILIENCE

*Technology & Capability
– a match made in
heaven*

THE ATTACK RACETRACK





BEYOND THE SIEM ALERT

*A mindset of continuous
Threat Hunting*

THE THREAT HUNTING EVOLUTION

- Unstructured
- Structured
- Automated





THE INTELLIGENT ANALYST

*Empowerment through
Threat Intelligence*

Bleeping Computer

ThreatPost

Twitter

Reddit

LinkedIn

Slack

Professional Associations

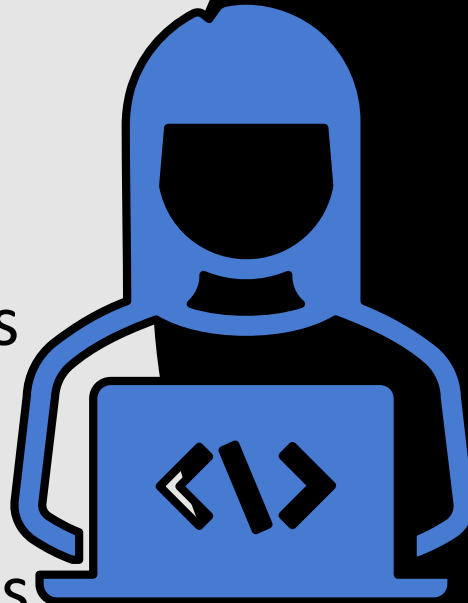
Vendor Publications

Paid Subscriptions

Current Affairs Magazines

Political Science Journals

Podcasts



SIEM

UEBA

NDR

Identity and Access

Endpoint Security

Third Party Access

VPN

Firewalls

Applications

Cloud

The background is a gradient of dark blue and purple, speckled with small white dots. Overlaid on this are several concentric circles and arcs in a lighter blue/purple hue. A prominent circular scale with tick marks and numbers (40, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) is visible on the left side. Other smaller circular elements with arrows are scattered across the frame.

THANK YOU

All the best!