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

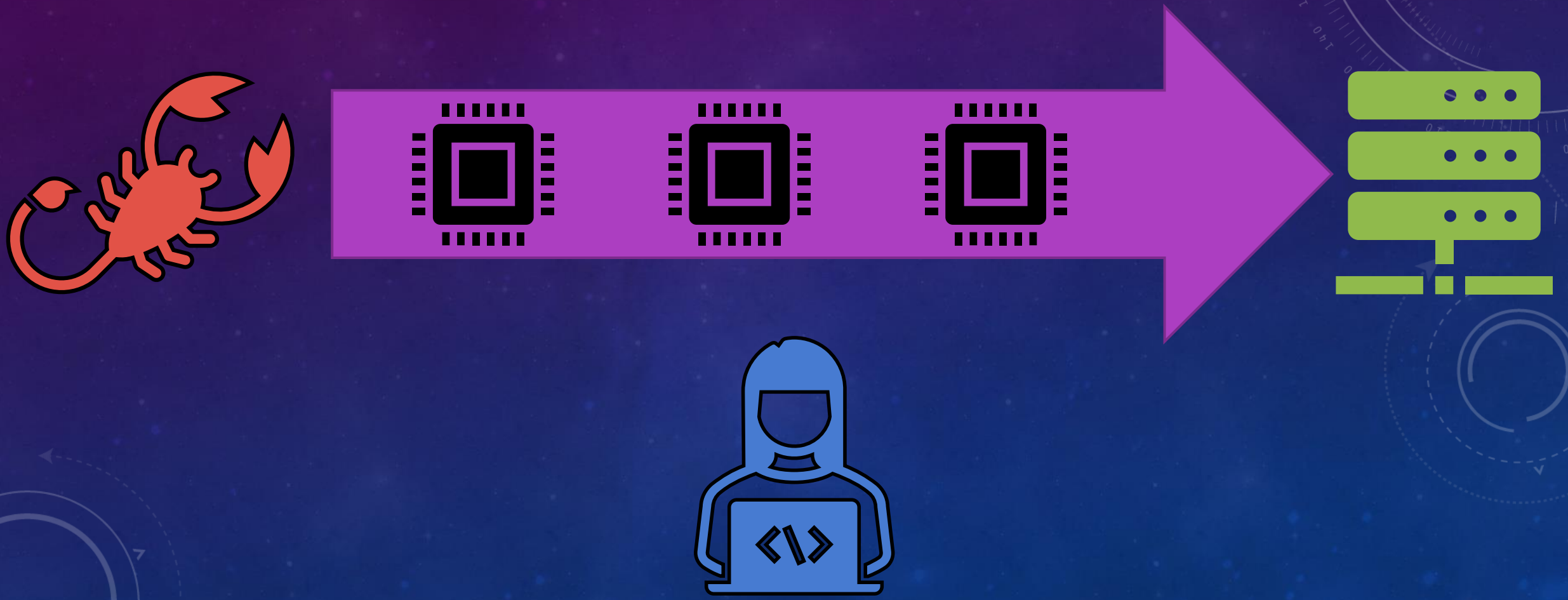
- The opinions expressed in this session are solely my own and do not express the views or opinions of my employer.

- 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

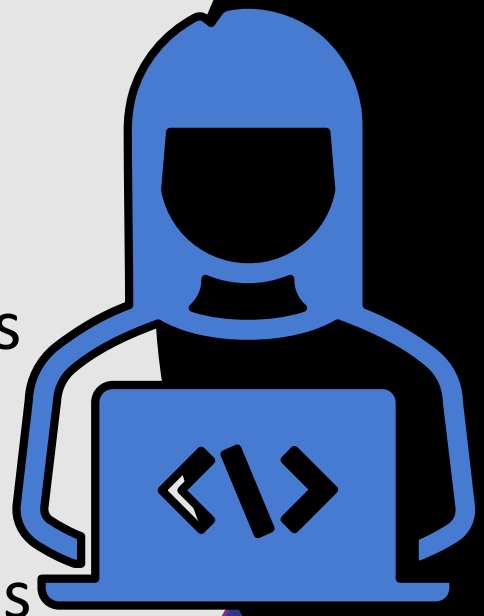
THE THREAT HUNTING EVOLUTION

- 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

THANK YOU

All the best!