CSO50 CONFERENCE+AWARDS

LEVERAGING World-Class SECURITY Strategies

PRODUCED BY

CSO FROM IDG

Modern Cyber Defense

Vivek Attri
Cyber Defense Center Leader
Genpact

About Genpact

…MANAGING DIVERSE COMPLEX CLIENT OUTCOMES

Pay **~7M** client invoices per month worth **~$20B**

Monitor an aviation engine taking off **every 2 mins**

Manage **~$200B** commercial lending assets

Manage F&A behind **every second beer sold**

Manage real time **~3M+** devices globally

Builder and co-owner of **largest KYC** utility platform in the world

Analyze **~2B** global consumer retail transactions annually

Manage **10,000+** drug licenses globally

Program Background

2015

One of earliest adopters of SIEM – Since 2005

- Capacity Challenges as we grew
- Limitations - Tool architecture, advanced capabilities and automation
- Vendor stability issues and technical support limitations
- Standard Incident response process

JANUARY 2016

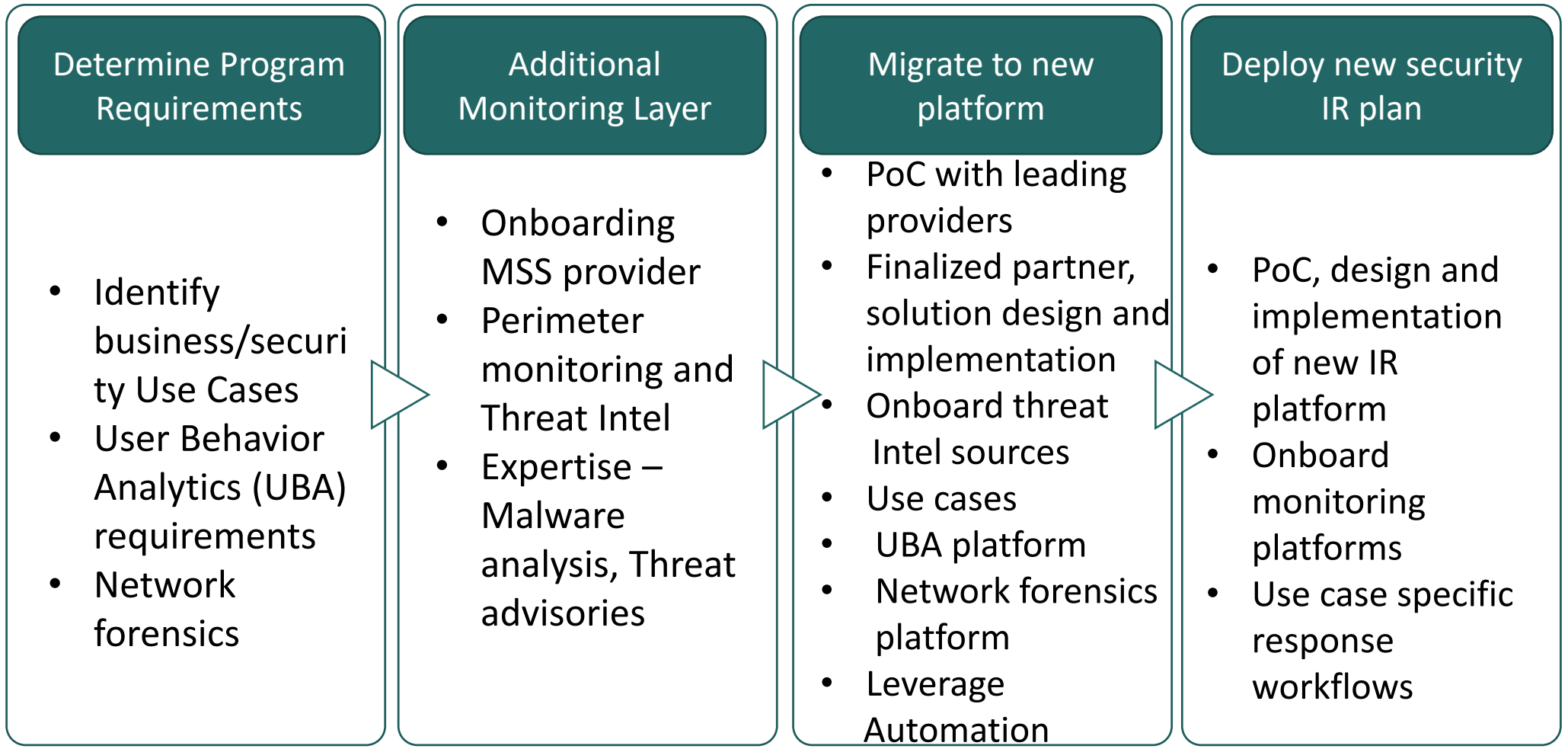
Vision for the new Cyber Defense Program

- Enhance situational awareness
- Enhance analytics and investigation capabilities
- Intelligence driven Cyber Defense functions
- Unify and Streamline security incident response processes
- Focused in-house expertise

Key Contributors to this new vision

- Address operational/business, security and compliance monitoring requirements
- Simplify the view of the organization’s security posture through a single pane of glass
- Robust and Intel driven incident response processes
- Effective reporting for Senior and mid-level management

2016 – Building the New Cyber Defense Program



What made our program different?

Context	Richer context for incident prioritization, investigation and reporting with insights
Use of Security Intelligence Platform to ingest hygiene data and automate Security risk metrics	Dynamic risk metrics
Response Orchestration	Response Automation for certain alerting scenarios
Inclusion of niche technologies under security intelligence umbrella	SIEM ++
Leverage Automation	Tailored applications built on top of SIEM platform
Outcome based procurement approach	Support Model

Business Impact

Significant increase in situational awareness and effectiveness of security incident investigation	Highly effective monitoring and prompt response against progressive threat vectors	Increased productivity allows security team additional time to focus on more value added activities
40+ Technologies 7k+ devices 80k+ assets 70k+ employees Cloud technologies	100+ Use cases UBA CASB Phishing IR process automation	90% reduction in reporting time Automation of complex processes

Business Impact

Avoidance of security attacks / incidents and resultant impact	Accurate and faster root cause analysis (RCA) of misconfigurations and unauthorized changes on IT infra	Address customer specific compliance requirements
Reduced cycle time for incident detection, response and mitigation	Advanced logging enabled on IT devices	Easier demonstration of IR processes for audits and certifications Customer contractual requirements factored in

2018 – Vision

- Intelligence ecosystem
- Threat hunting
- Intel driven CDC processes
- Result oriented Red/Blue team exercises
- Adaptive response orchestration
- Interactive automations and machine learning

Thank you