IMPROVING AND MATURING YOUR SECURITY OPERATION CENTER (SOC)

Nipon Komomsuwan

NetWitness Product Director, SEA , Sri Lanka & Mongolia

SECURITY CHALLENGES:

INCOMPLETE VISIBILITY

Difficult to see any and all threats – wherever they reside in a modern IT infrastructure

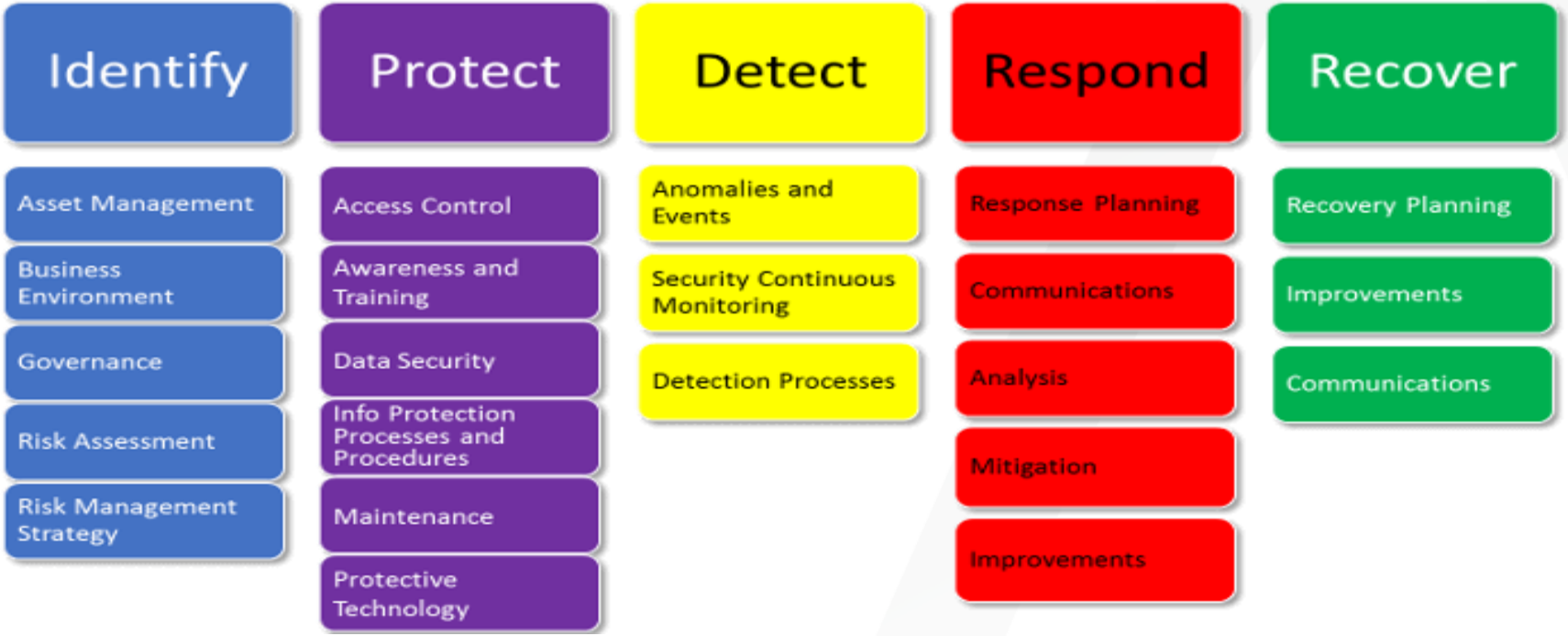
RESOURCE SHORTAGES

Skilled analysts are in short supply, and teams struggle to effectively combat threats

CONTEXT DRIVEN PRIORITIZATION

Difficulty linking security alerts with business context and risk, resulting in a lack of focus on the most important threats

NIST Cyber Security Framework



WHAT IS DETECTED?

- Initial Infection
- Command & Control
- Anomalous Outbound Connection
- Lateral Movement
- Data Exfiltration

ORGANIZATIONS NEED SOC TECHNOLOGY THAT PROVIDES….

Pervasive Visibility

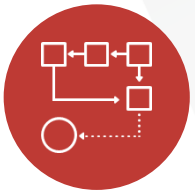
- Visibility across Endpoints (OS-level), Logs, Networks (Packets), VMs and the Cloud – Combined with threat intelligence and business context
- Visibility into Operational (OT) and IoT Networks and Devices
- Consumption and transformation of data into *usable* threat metadata

Detection of Advanced Attacks

- Multiple sets of analytic techniques: Data science modeling and machine learning; user & entity behavior analytics (UEBA) to fine unknown threats
- Library of known threat indicators
- 3rd party and Community derived Threat Intelligence
- Processing of large volumes of threat data for complete threat detection

Investigation and Response

- Validation of incidents with Endpoint and Cloud visibility and analysis
- Orchestration across your entire security arsenal to accelerate incident response and automation

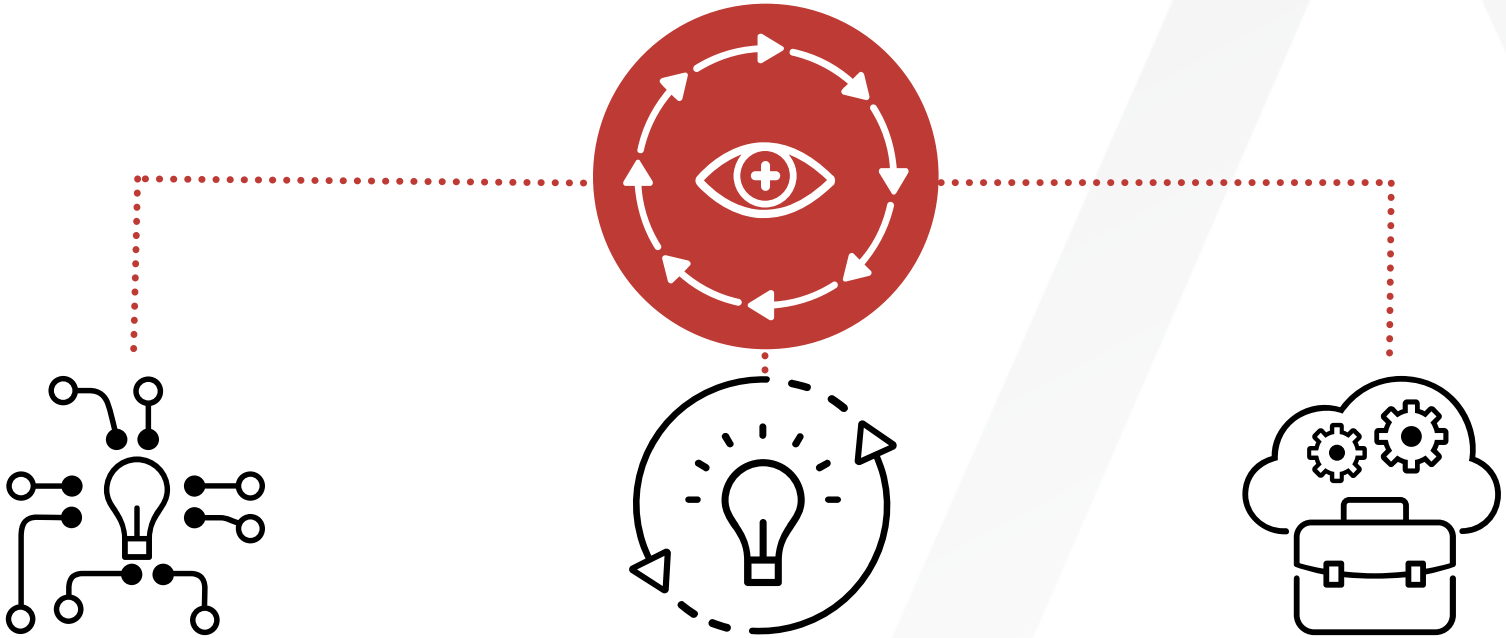


Connecting with the Business

- Enable security teams to act and mitigate the full attack before it can impact the business
- Automated response to drive efficiency
- Orchestration across entire SOC to speed response to the most impactful incidents

RSA

VISIBILITY FOR ACCELERATED THREAT DETECTION



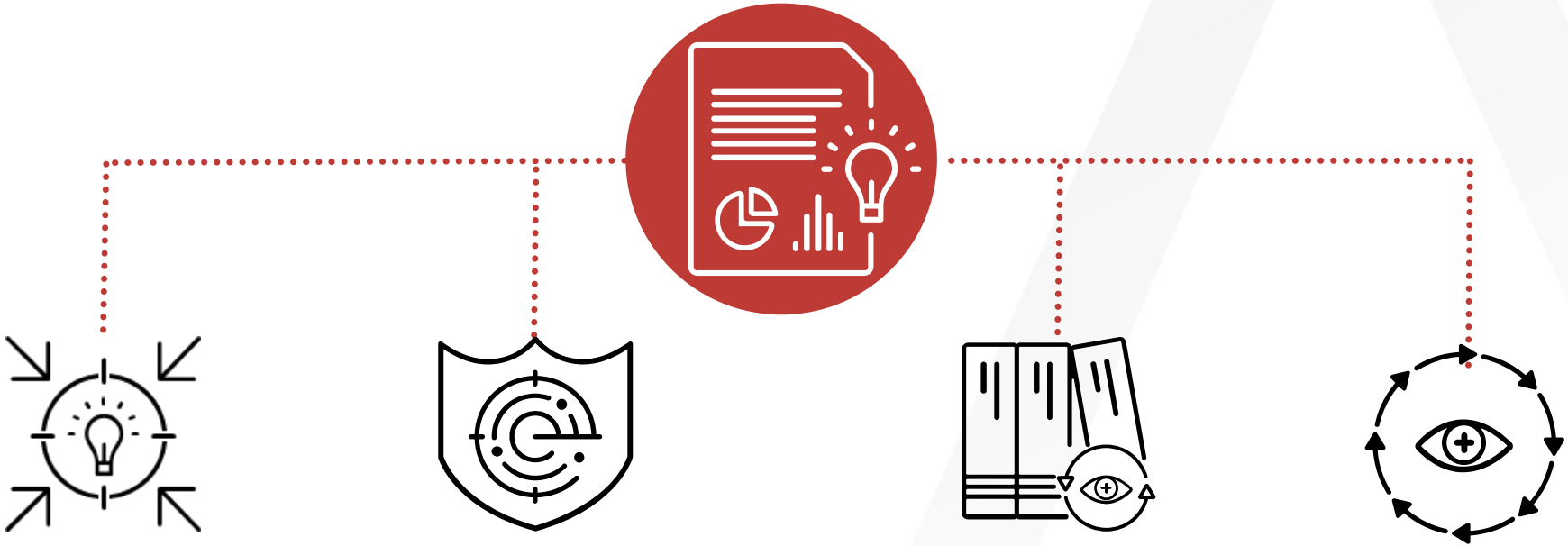
Logs, Packets, Endpoints, NetFlow, Cloud

Capture-Time Data Enriched and Transformed into Powerful Metadata

Threat Intelligence

RSA

FORCE MULTIPLIER – ANALYTICS AND ORCHESTRATION (HELPING RESOURCE SHORTAGE)



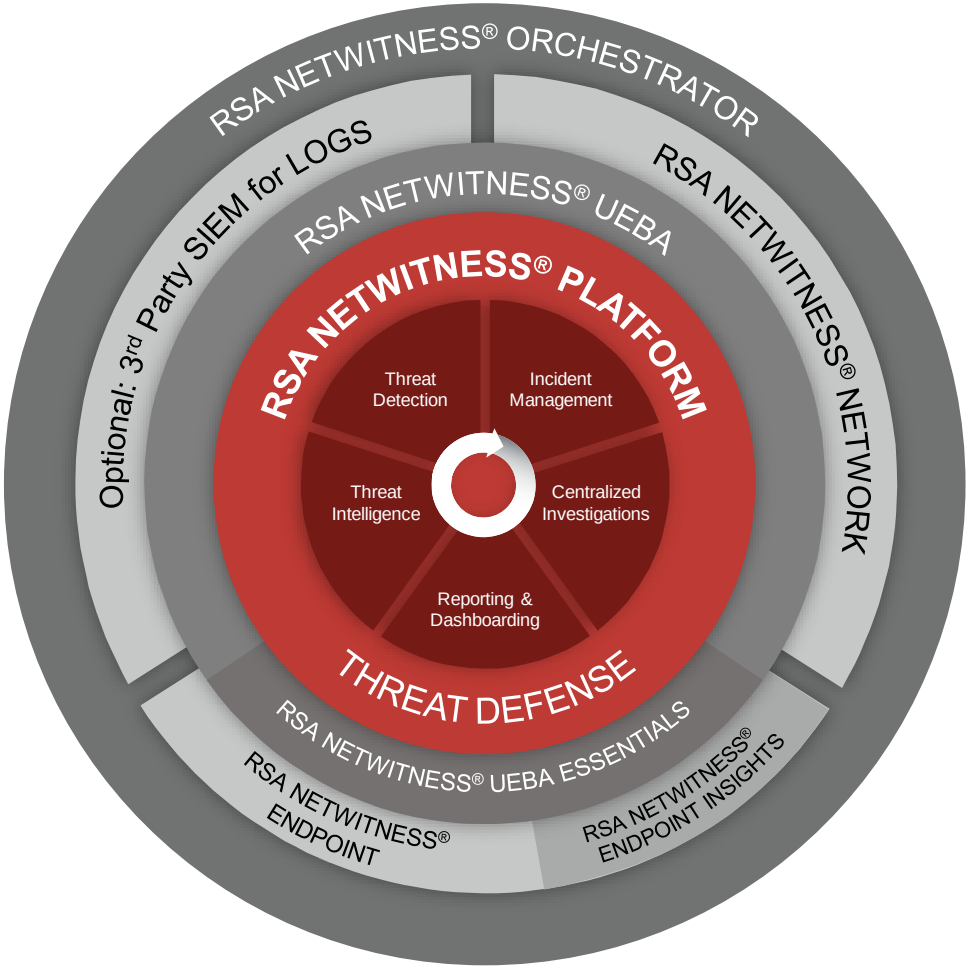
Correlate Multiple Data Sources

Behavioral Threat Detection

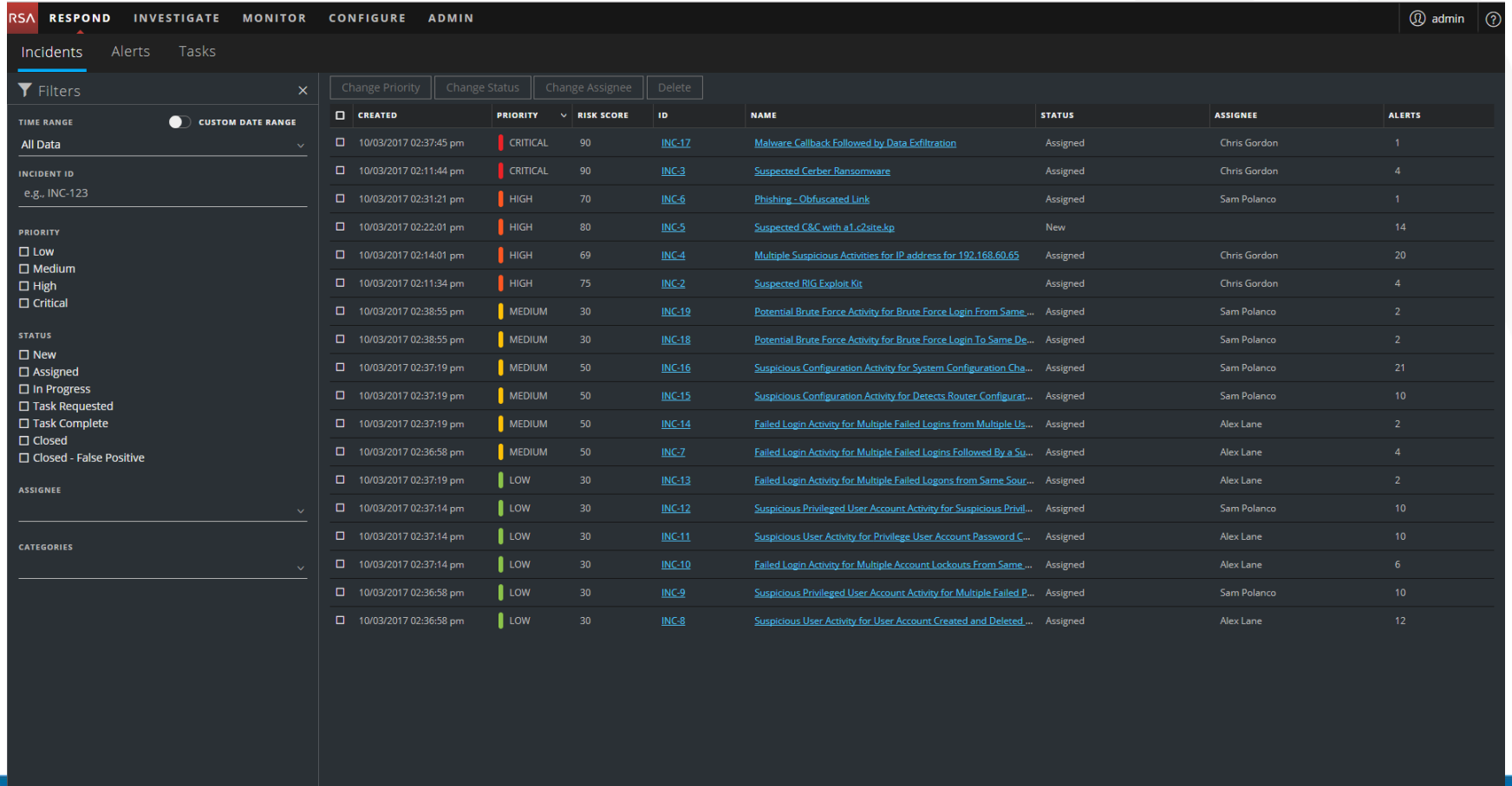
Out-of-the-Box Threat Intelligence from Experts & Community

Visualization

Security Platform

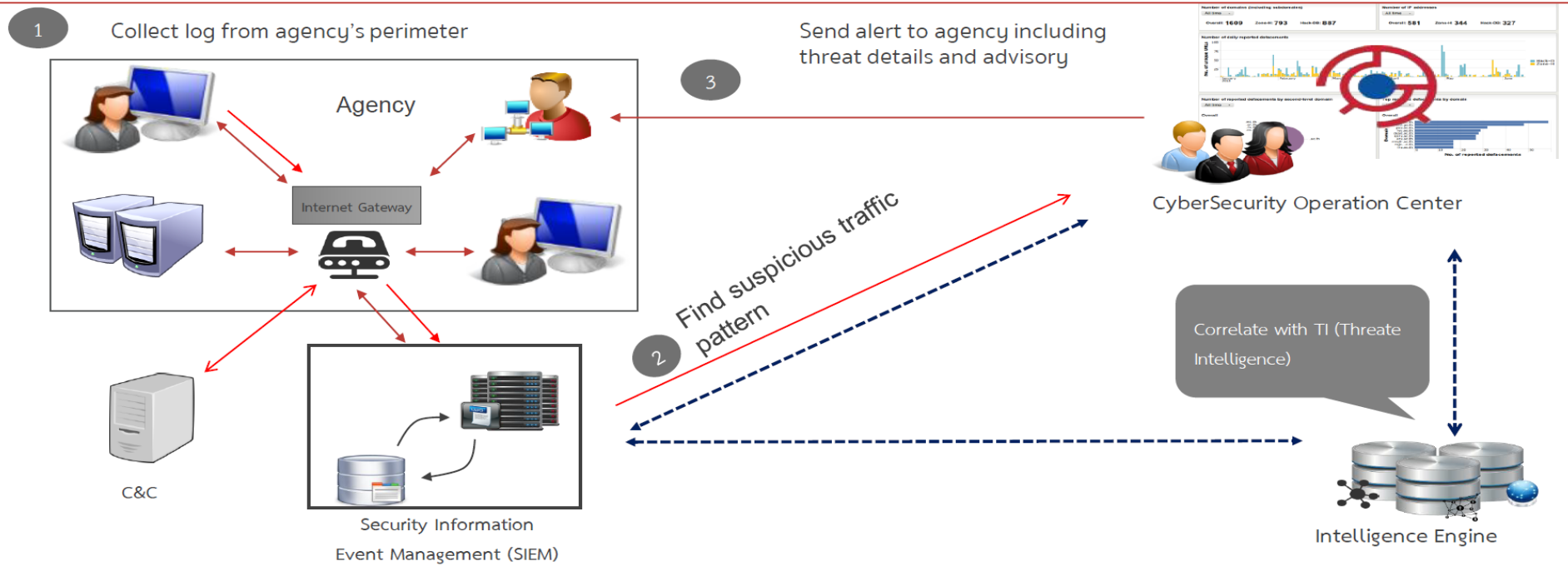


RESPOND – INCIDENT PRIORITIZATION



LEVERAGING NATIONAL SOC

Government Threat Monitoring (GTM)



**Source: ThaiCert - Presented at RSA Charge 2017

RSA

QUESTIONS & THANK YOU