



IMPROVING AND MATURING YOUR SECURITY OPERATION CENTER (SOC)

Nipon Komomsuwan

NetWitness Product Director, SEA , Sri Lanka & Mongolia

SECURITY CHALLENGES:

INCOMPLETE VISIBILITY



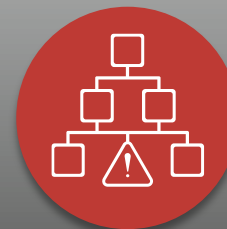
Difficult to see any and all threats – wherever they reside in a modern IT infrastructure

RESOURCE SHORTAGES



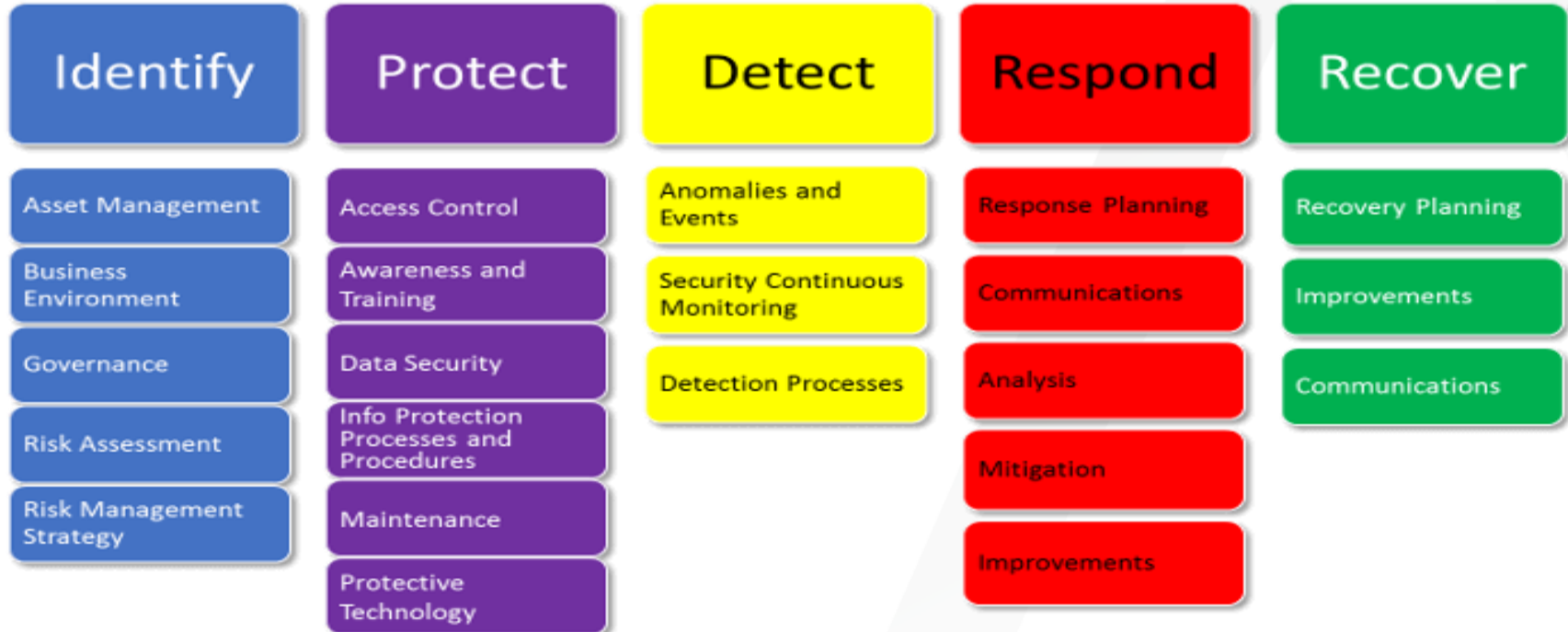
Skilled analysts are in short supply, and teams struggle to effectively combat threats

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



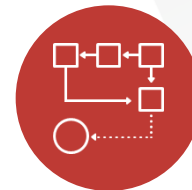
Detection of Advanced Attacks

- ▶ 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

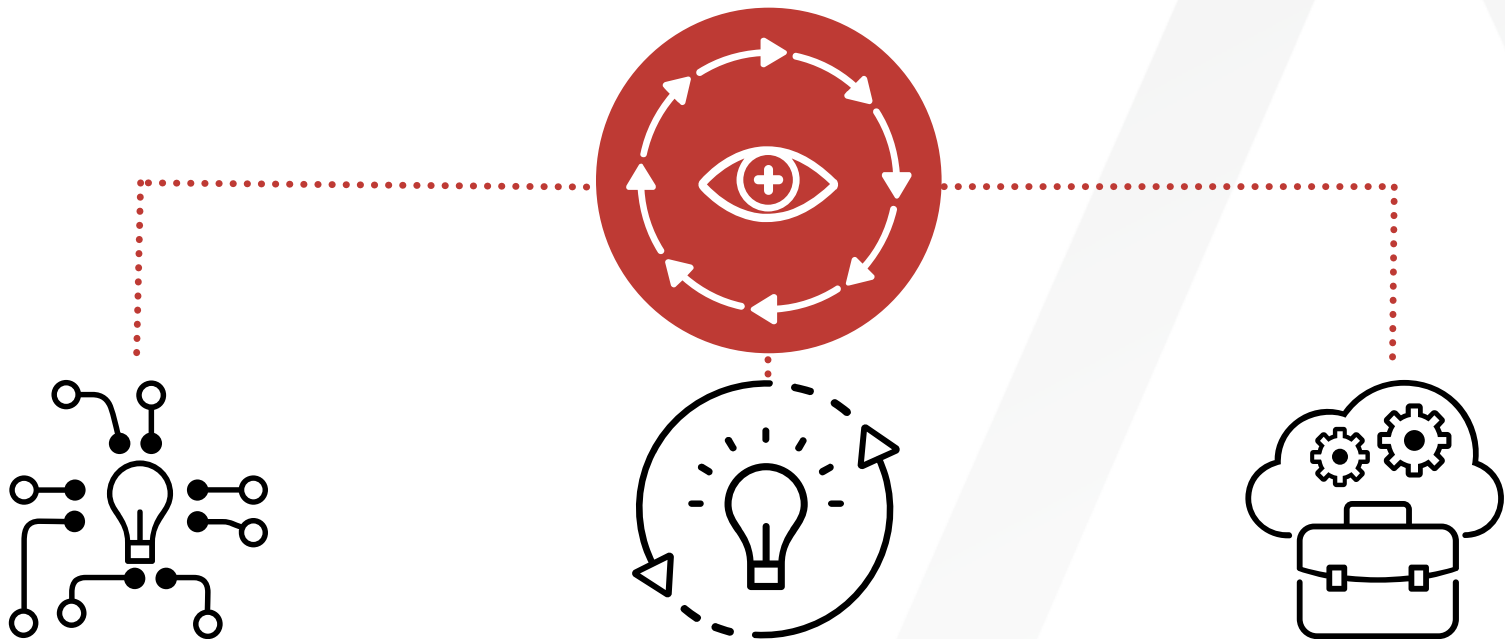
- ▶ Validation of incidents with Endpoint and Cloud visibility and analysis
- ▶ Orchestration across your entire security arsenal to accelerate incident response and automation



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

VISIBILITY FOR ACCELERATED THREAT DETECTION

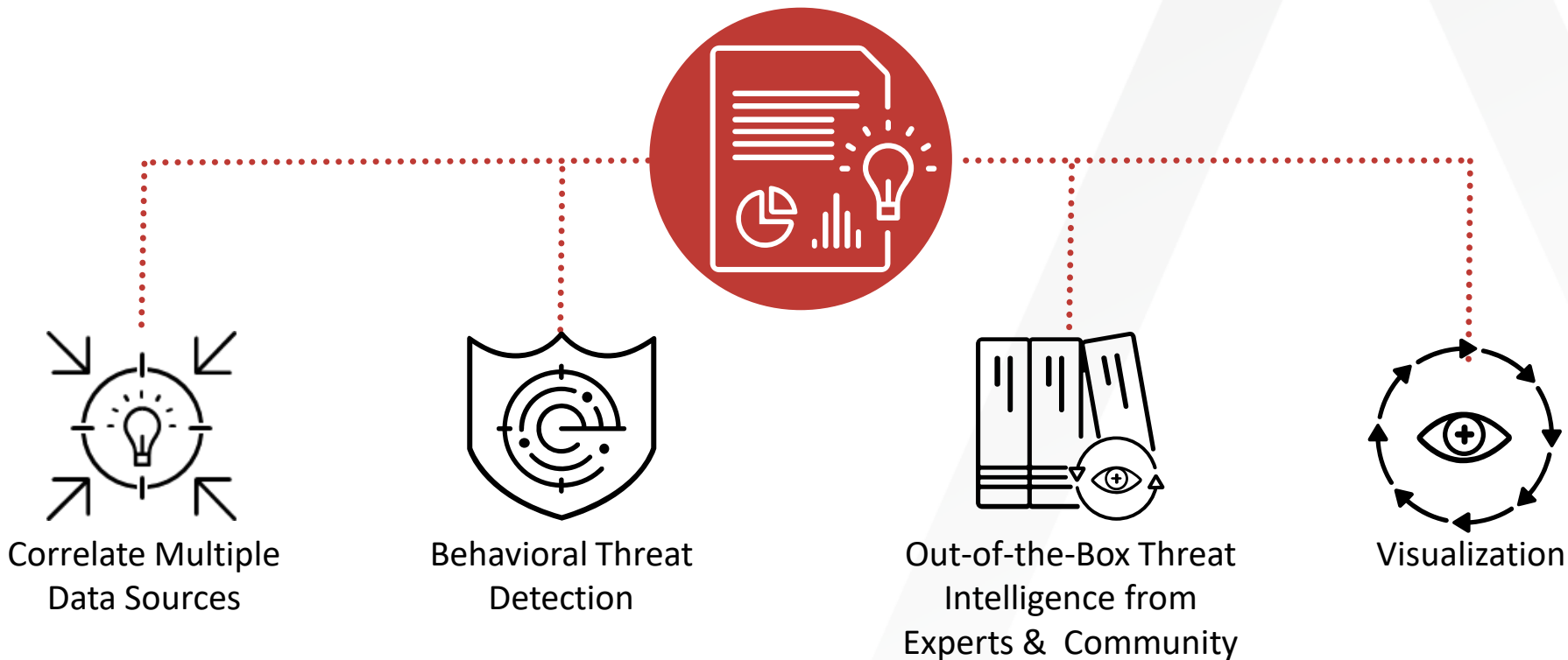


Logs, Packets, Endpoints,
NetFlow, Cloud

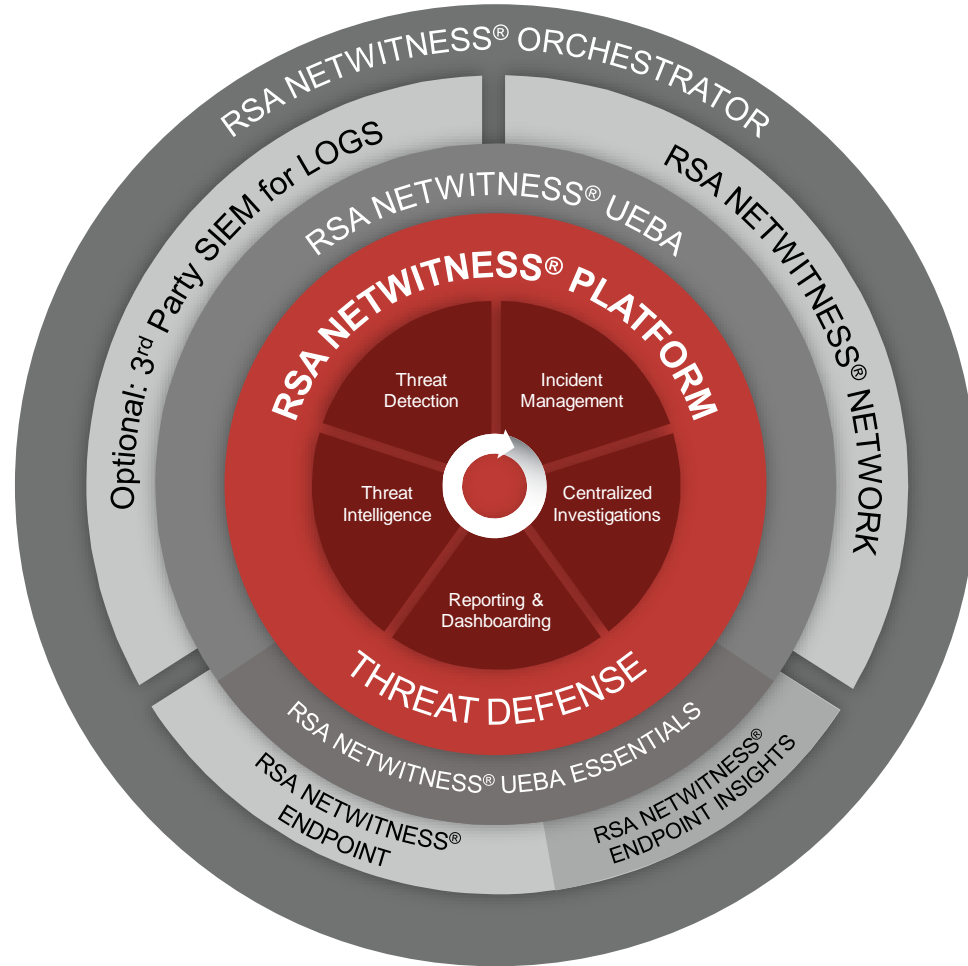
Capture-Time Data Enriched and
Transformed into Powerful Metadata

Threat Intelligence

FORCE MULTIPLIER - ANALYTICS AND ORCHESTRATION (HELPING RESOURCE SHORTAGE)



Security Platform



RESPOND – INCIDENT PRIORITIZATION

RSA **RESPOND** INVESTIGATE MONITOR CONFIGURE ADMIN admin

Incidents Alerts Tasks

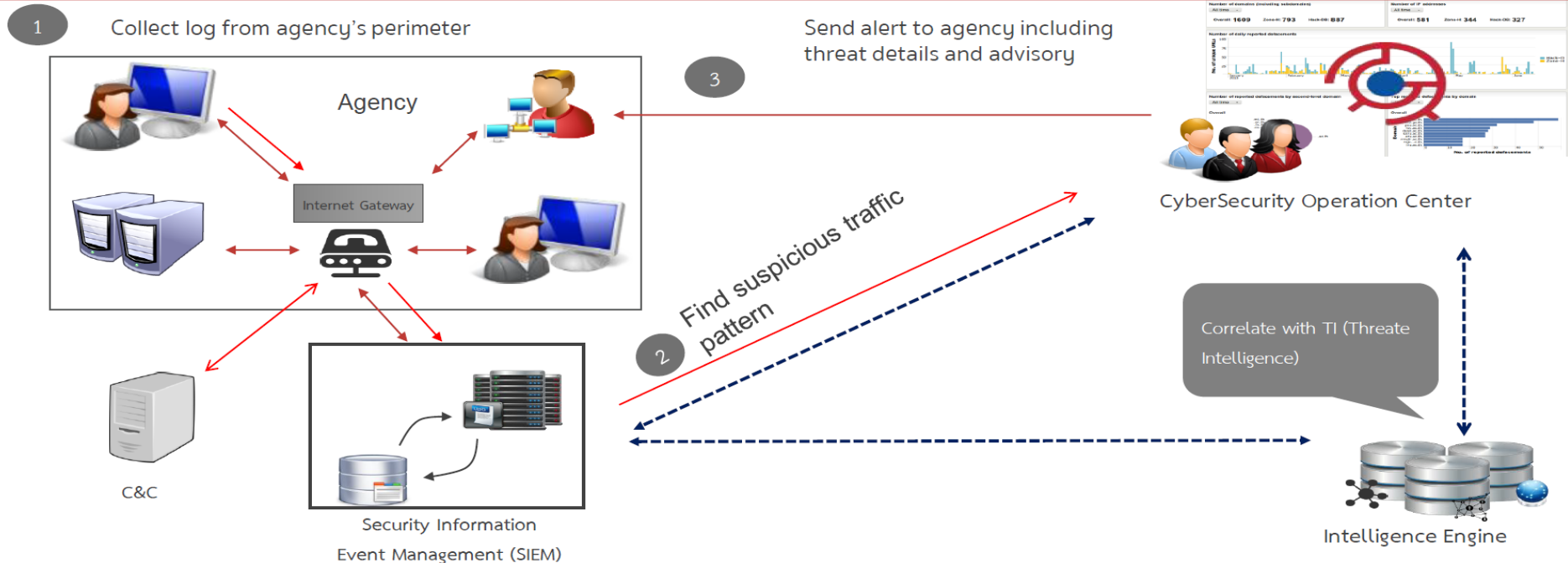
Filters

Change Priority Change Status Change Assignee Delete

TIME RANGE	CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
<input type="radio"/> All Data	10/03/2017 02:37:45 pm	CRITICAL	90	INC-17	Malware Callback Followed by Data Exfiltration	Assigned	Chris Gordon	1
<input type="radio"/> INCIDENT ID e.g., INC-123	10/03/2017 02:11:44 pm	CRITICAL	90	INC-3	Suspected Cerber Ransomware	Assigned	Chris Gordon	4
<input type="radio"/> PRIORITY <input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical	10/03/2017 02:31:21 pm	HIGH	70	INC-6	Phishing - Obfuscated Link	Assigned	Sam Polanco	1
<input type="checkbox"/> STATUS <input type="checkbox"/> New <input type="checkbox"/> Assigned <input type="checkbox"/> In Progress <input type="checkbox"/> Task Requested <input type="checkbox"/> Task Complete <input type="checkbox"/> Closed <input type="checkbox"/> Closed - False Positive	10/03/2017 02:22:01 pm	HIGH	80	INC-5	Suspected C&C with a1.c2site.kp	New		14
<input type="checkbox"/> ASSIGNEE	10/03/2017 02:14:01 pm	HIGH	69	INC-4	Multiple Suspicious Activities for IP address for 192.168.60.65	Assigned	Chris Gordon	20
<input type="checkbox"/> CATEGORIES	10/03/2017 02:11:34 pm	HIGH	75	INC-2	Suspected RIG Exploit Kit	Assigned	Chris Gordon	4
	10/03/2017 02:38:55 pm	MEDIUM	30	INC-19	Potential Brute Force Activity for Brute Force Login From Same...	Assigned	Sam Polanco	2
	10/03/2017 02:38:55 pm	MEDIUM	30	INC-18	Potential Brute Force Activity for Brute Force Login To Same De...	Assigned	Sam Polanco	2
	10/03/2017 02:37:19 pm	MEDIUM	50	INC-16	Suspicious Configuration Activity for System Configuration Cha...	Assigned	Sam Polanco	21
	10/03/2017 02:37:19 pm	MEDIUM	50	INC-15	Suspicious Configuration Activity for Detects Router Configurat...	Assigned	Sam Polanco	10
	10/03/2017 02:37:19 pm	MEDIUM	50	INC-14	Failed Login Activity for Multiple Failed Logins from Multiple Us...	Assigned	Alex Lane	2
	10/03/2017 02:36:58 pm	MEDIUM	50	INC-7	Failed Login Activity for Multiple Failed Logins Followed By a Su...	Assigned	Alex Lane	4
	10/03/2017 02:37:19 pm	LOW	30	INC-13	Failed Login Activity for Multiple Failed Logons from Same Sour...	Assigned	Alex Lane	2
	10/03/2017 02:37:14 pm	LOW	30	INC-12	Suspicious Privileged User Account Activity for Suspicious Privil...	Assigned	Sam Polanco	10
	10/03/2017 02:37:14 pm	LOW	30	INC-11	Suspicious User Activity for Privilege User Account Password C...	Assigned	Alex Lane	10
	10/03/2017 02:37:14 pm	LOW	30	INC-10	Failed Login Activity for Multiple Account Lockouts From Same...	Assigned	Alex Lane	6
	10/03/2017 02:36:58 pm	LOW	30	INC-9	Suspicious Privileged User Account Activity for Multiple Failed P...	Assigned	Sam Polanco	10
	10/03/2017 02:36:58 pm	LOW	30	INC-8	Suspicious User Activity for User Account Created and Deleted...	Assigned	Alex Lane	12

LEVERAGING NATIONAL SOC

Government Threat Monitoring (GTM)





QUESTIONS & THANK YOU