Moving Towards an Advanced Fusion Center

Lesly White

Sr. Director, Cyber Operations, SIEM and Sensor| Optiv

OPTIV

splunk> .conf19

Topics

- Current State of Security Operations
- What is an Advanced Fusion Center?
- The Growing Scope of Security Operations
- The Journey Forward

Current State of Security Operations

.conf19

splunk>

OPTIV

Current State

Over the past few years companies have made significant investments in technology and people to defend against cyber threats.

Operating management, senior leaders, and boards are frustrated their security posture is still challenged, a financial “black hole”, and they continue to face a risk of a successful attack.

Executive leadership would like to mature and optimize their cyber operations, have assurance the investments are beneficial, and have confidence the business is protected.

Skills required to build an internal team are scarce

Many companies have a hard time staffing a SOC for 8x5 operation, much less 24x7 operations with the appropriate skills.

Poor integration of controls

Companies have made significant investment in control infrastructure; yet little of the value has been sufficiently leveraged (limited implementation, poor data integration, operational challenges with new toolsets).

Corporate alignment

Lack of feedback, metrics reporting, and cybersecurity program understanding results in less buy-in from leadership.

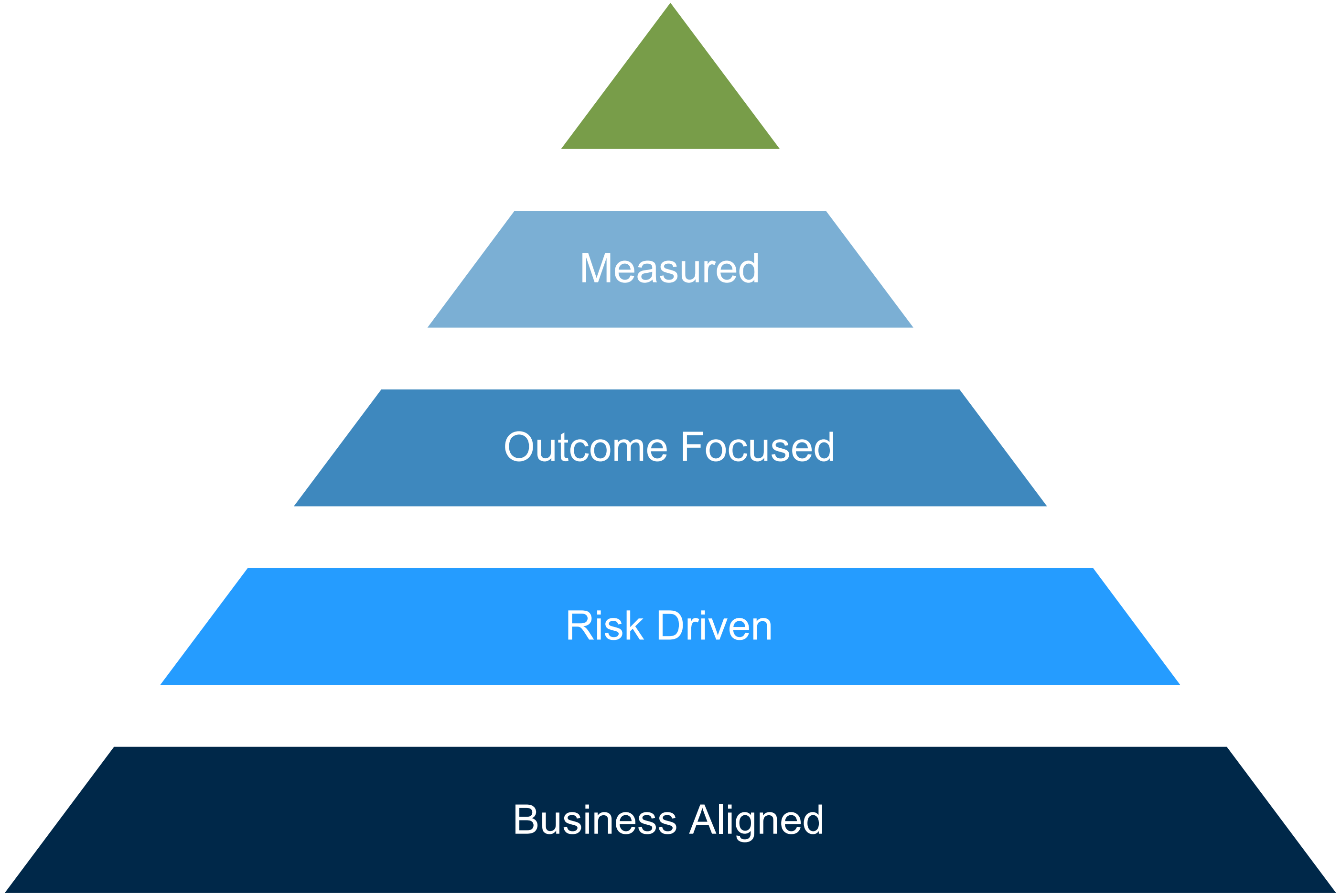
OPTIV

splunk> .conf19

Advanced Fusion Center

Combined
Supportive
Collaborate
Synergistic
Aligned
Helpful
Joint
Reliable
Interaction
Merge
Synchronization
United
Mutual
Corps
Synergy
Center
Collaborative
Cooperative
Consistent
Team
Pooled
Union
Concerted
Meld
Esprit
Shared
De
Allied
Fusion
Synthesis
Collaboration
Combination
Cooperation
Willing
Collective
Common
Blend
Partnership
Community
Dependable
Quality
Informative
Harmonized
Coordinated

Setting the Foundation



Measured

Outcome Focused

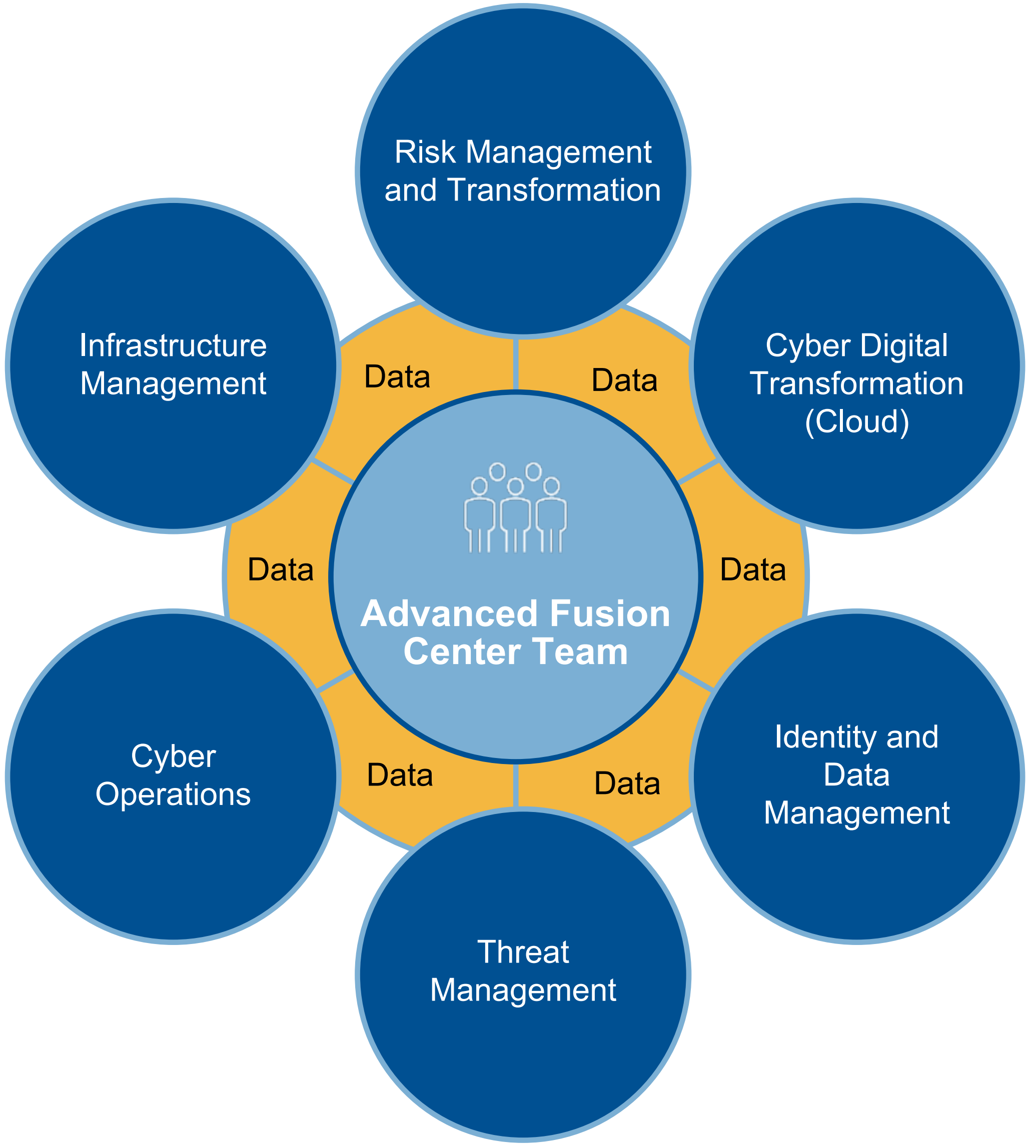
Risk Driven

Business Aligned

OPTIV

splunk> .conf19

Fusion Center is the Hub of Security Function and Data Integration


Risk Management and Transformation
Infrastructure Management
Cyber Digital Transformation (Cloud)
Data
Data
Data
Data
Advanced Fusion Center Team
Cyber Operations
Identity and Data Management
Data
Data
Threat Management

OPTIV

End State Goal

World Class Cyber Operations Center

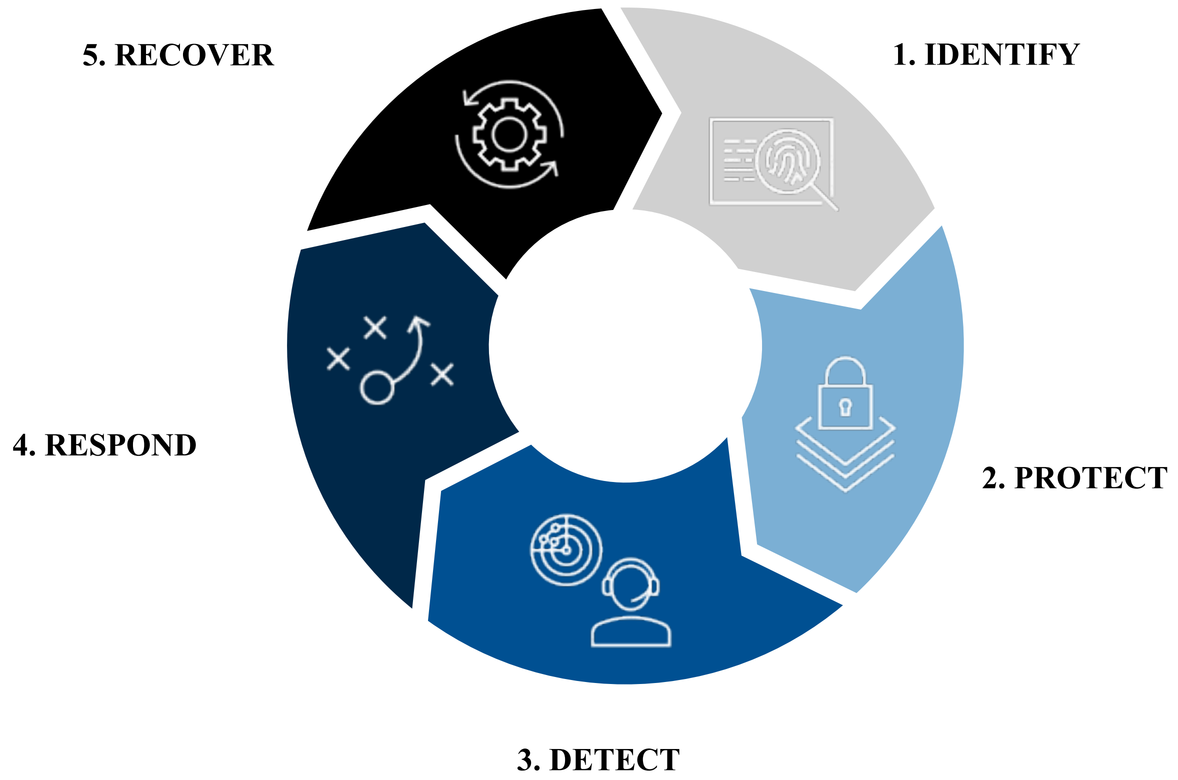
Right Capabilities

Right Focus

Right Organization

Right Governance

Framework Lifecycle



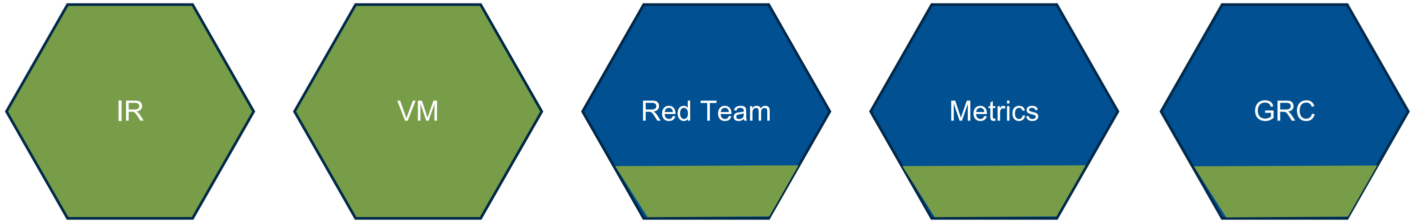
- Assurance that the activities support the business objectives and are aligned with the greater IT and security organization
- SOC has the authority to act on its given responsibilities
- Performance is measured and measurable (i.e. metrics and reporting)
- Activities are consistent with applicable laws and regulations through adherence to policies and internal controls

The Growing Scope of Security Operations Center

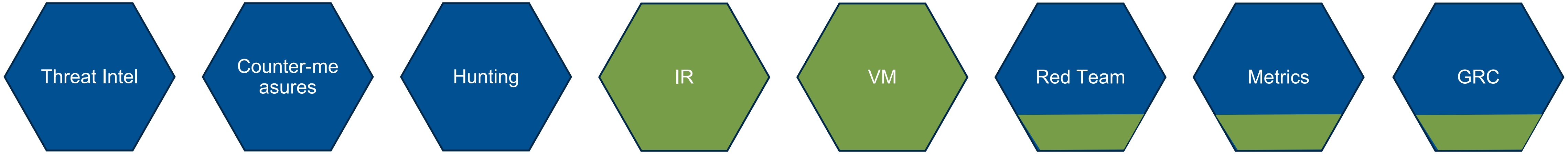
.conf19
splunk>

OPTIV

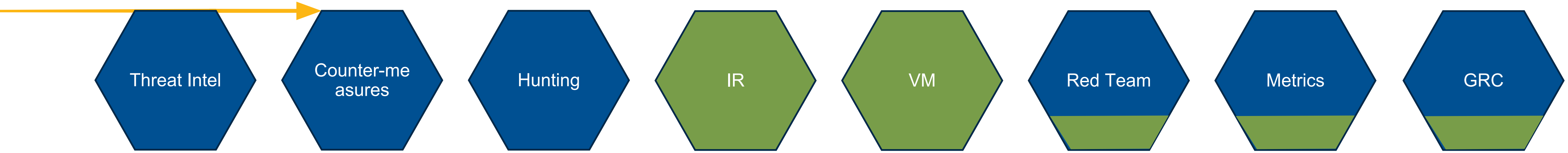
Traditional SOC Functions



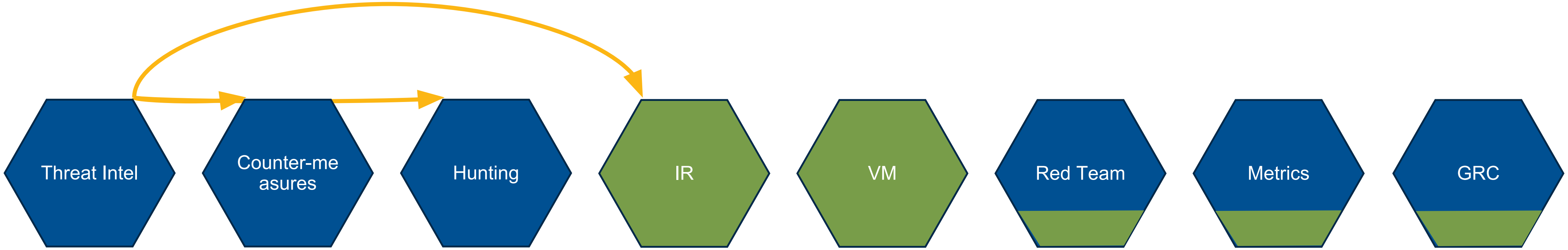
Expanding SOC Functions



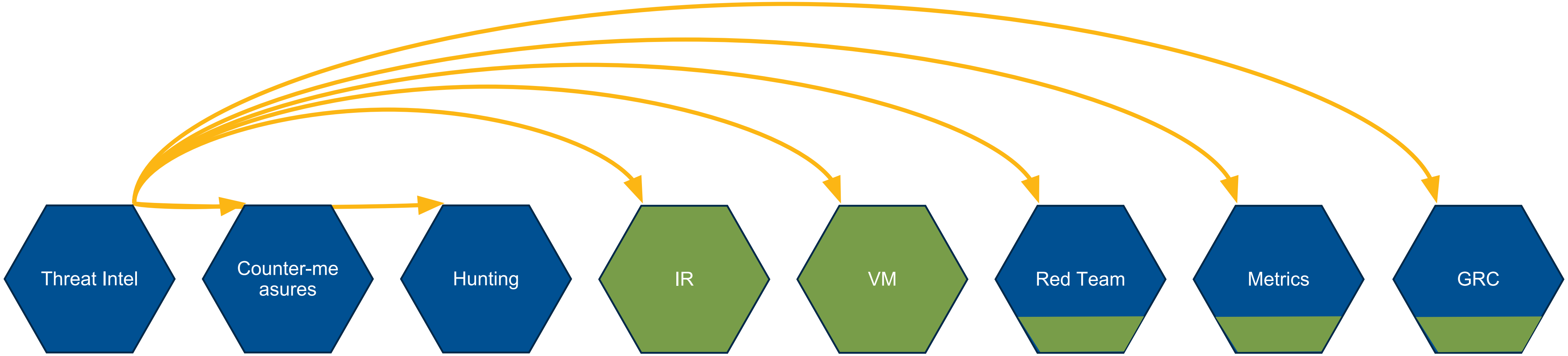
Integrating SOC Functions



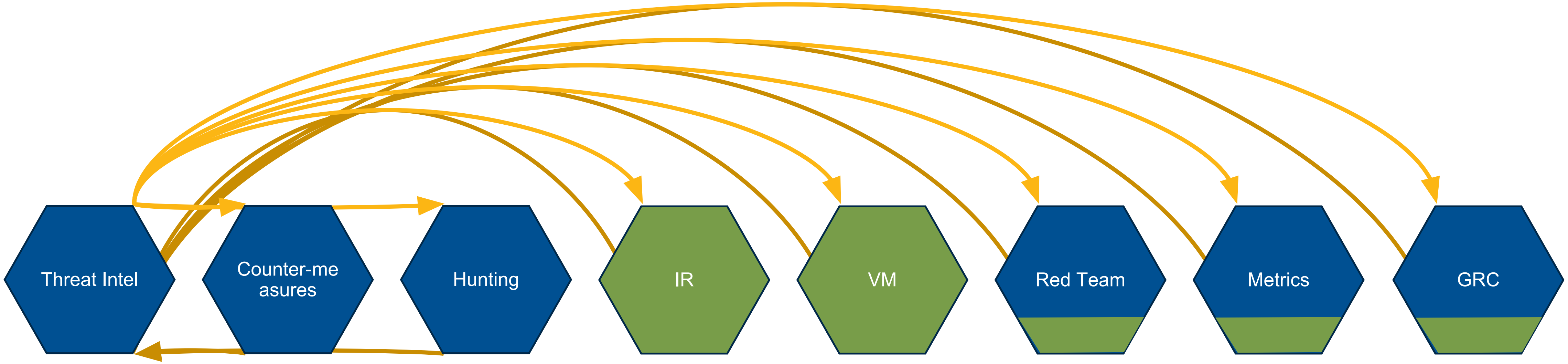
Integrating SOC Functions



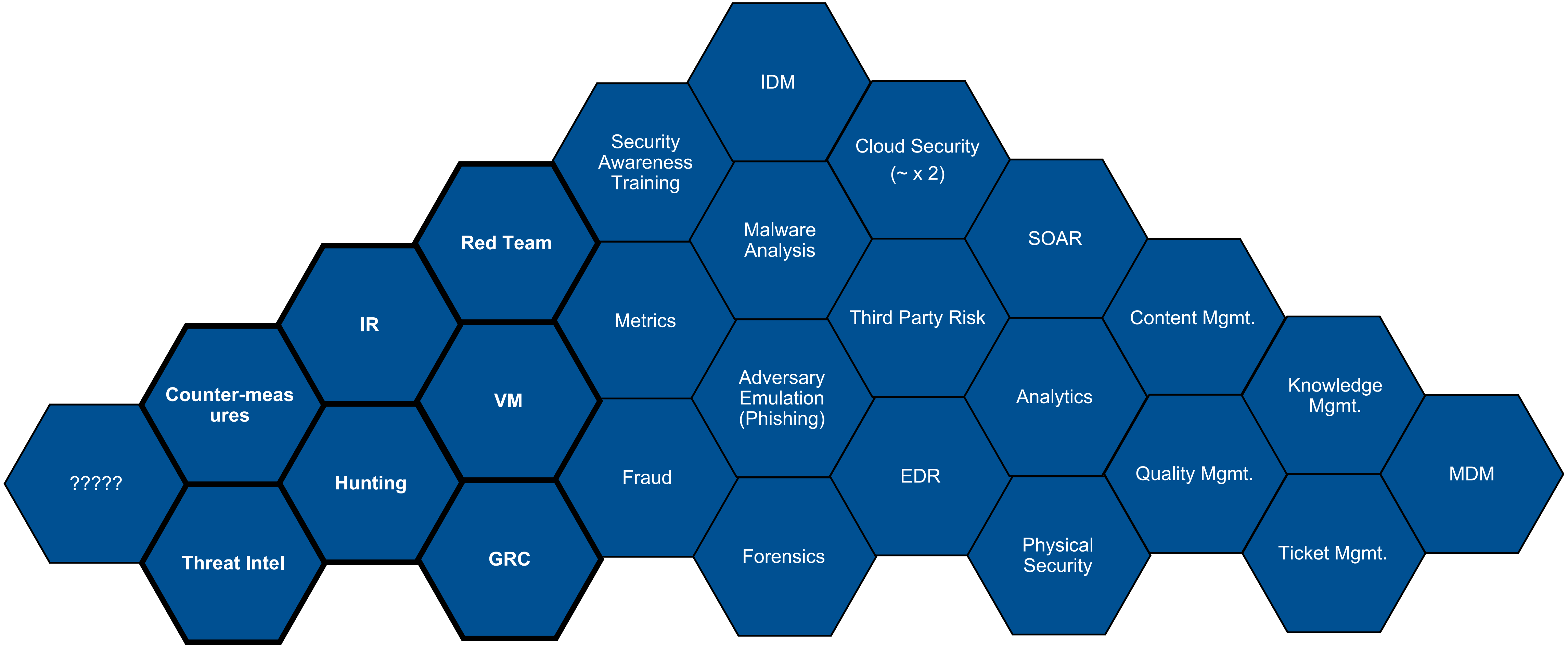
Integrating SOC Functions



Feedback Loop For Continuous Improvement



Another Way To Look At An Integrated Advanced Fusion Center



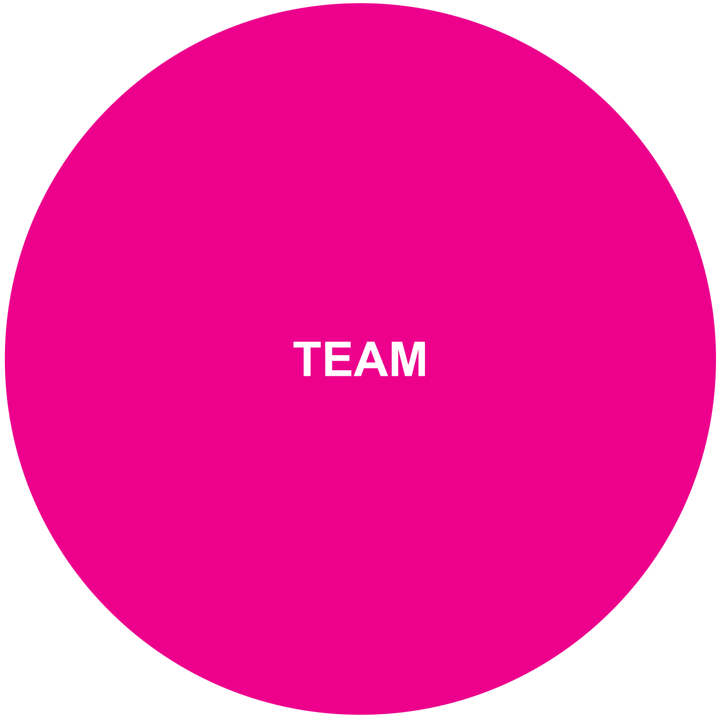
OPTIV

splunk> .conf19

Making the Journey

If You Are Investing In a SOC Team, Do It Differently!

- Integrate Analysts and Engineers as one team
- The flexible SOC
- Use efficiencies to shift workload to proactive tasks
- Richer job roles lead to lower attrition
- Reduce the menial tasks, focus on higher value



TEAM

ELEVATING YOUR LEVEL OF MATURITY

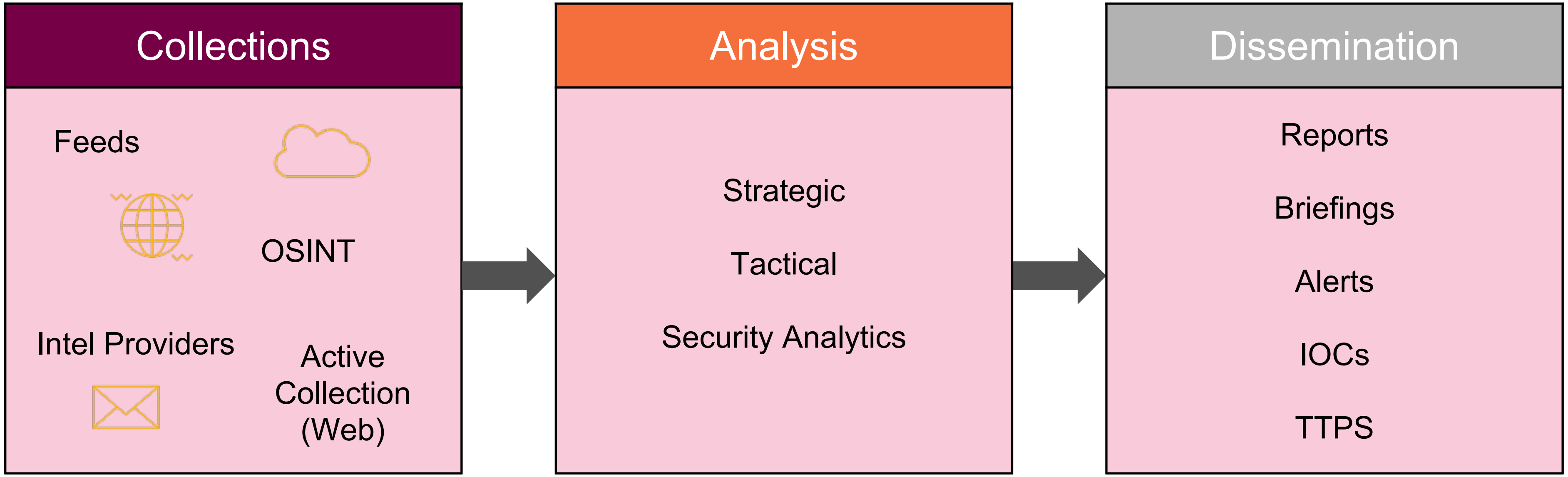
External Threat Intelligence

- Make security news collection part of the SOC.
- Publish advisories internally.
- Change the work routine of the Analyst.
- Use feeds in detect mode and potentially block mode.
- Manage intelligence using a Threat Intelligence Platform (TIP).
- At a minimum, use intelligence to protect your brand.

FUEL PROACTIVE THREAT HUNTING

ELEVATING YOUR LEVEL OF MATURITY

Threat Intelligence



Collections

Feeds

OSINT

Intel Providers

Active Collection (Web)

Analysis

Strategic

Tactical

Security Analytics

Dissemination

Reports

Briefings

Alerts

IOCs

TTPS

Security Orchestration and Automation

- Enrichment – Add detailed context to alerts for enhanced decision making.
  - Threat Intelligence – Utilize intel data to inform and add context to security alerts.
  - Security Stack Integration – Leverage capabilities from available platforms.
- Single Pane of Glass – Unified console to perform complete alert triage and analysis processes, knowledge and case management.
- Efficiency and Consistency – Automate manual processes and workflows to save time and labor and provide a consistent result.
- End to End Automation – Fully automate complex processes to allow analysts more time to analyze, hunt, and work towards resolution.

More Offensive Security – Red Teaming or Adversary Emulation

- Digital transformation is expanding the attack surface.
- Probe your defenses using the perspective of the enemy.
  - 75% of the vulnerabilities Optiv offensive cyber teams exploited in 2018 were not identified by a vulnerability scanning platform.
  - Focus on expected threat vectors that the cyber attacker will use.
- Do this as frequently as you can. Such as an always on activity.

KPI’s and Reporting

Business KPIs = Measuring Effectiveness. SLA’s = Accountability

- **Likelihood of a successful attack**
  Likelihood will be assessed based on the security profile of each business unit determined by the coverage and settings of security controls. Other components may be added by the client.
- **Impact**
  Impact of events during the period measured by impact to Confidentiality / Integrity / Availability for a defined asset that the security stack can protect.
- **Time to detect**
  Measures the delta between the event being logged and an incident case being created.
- **Time to respond**
  Measures the delta between the case creation and email to the customer with remediation recommendation and the beginning of containment efforts.
- **Maturity**
  Quarterly ranking maturity of SOC elements such as cyber threat intelligence, red team testing, logging level and accuracy.

THREAT ANALYSIS CASE TYPE	INITIAL ACKNOWLEDGEMENT (PROVIDED IN RFP RESPONSE)	TIME TO RESPOND
Sev1/Critical	30 Minutes	4 Hours
Sev2/High	90 min	24 Hours (1 Calendar Day)
Sev3/Medium	4 Hours	2 Calendar Days
Sev4/Low	16 Hours	7 Calendar Days

OPTIV

.conf19®

splunk>®

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION