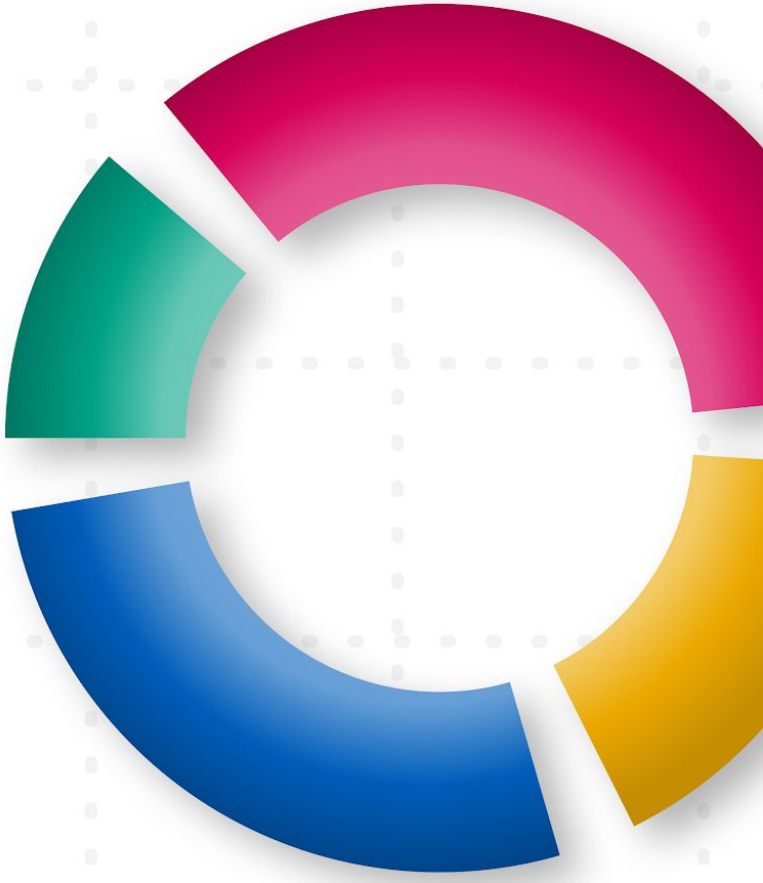
PICUS

VIRTUAL EVENT

SOC ReLoad 2021

Achieve a Modern SOC Through a Threat-Centric Approach



SOC ReLoad
#SOCReLoad21

KEYNOTE

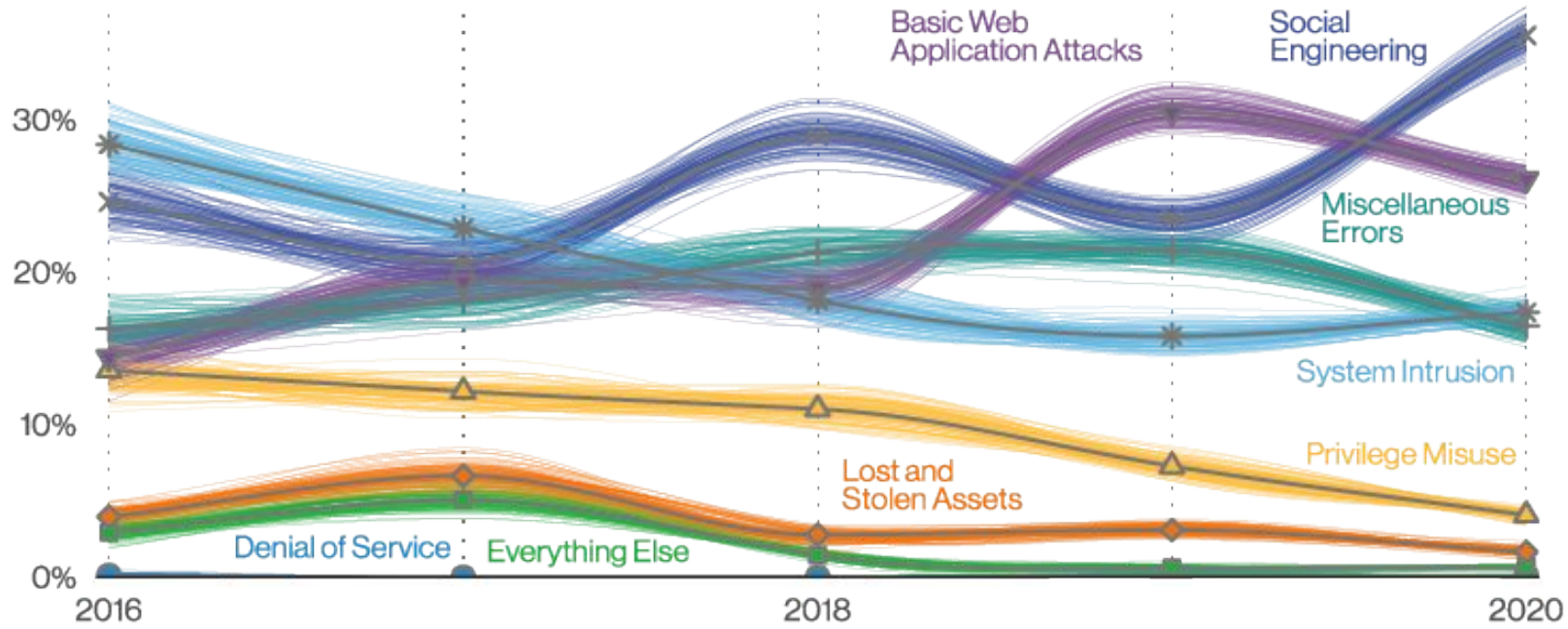
Key Strategies to Building a Modern SOC: How to Supercharge Your Security Operations Center to Keep Pace with Emerging Threats

Chris Crowley
SOC Class-Course Author

SANS

Do you Prefer the Status Quo?

- We see minor variations in what attackers are doing
- Yet we continue to be reactive instead of proactive



Patterns over time in breaches

Security Stagnation

- **Business impact and costs are increasing**
- **Cyber spending is booming**
  Cyber investment $12B in 2021 so far, up to 20% from 2020 *(NYT)*
- **Cyber is supposed to provide loss prevention**
- **Does your SOC deliver?**

Are you wasting your security spend?

Supercharging the Modern SOC

- **Supercharge**: (*verb*) Make faster or more powerful

- **Cyber Supercharge**:
  - Staff
  - Capability
  - Technology

- Purge complaisance, embrace bold action

- Let's look at components to supercharge your SOC…

Supercharging is Required

Develop IT Operational Excellence

Component 1

- **Effectively deploy all of the following:**
  - Operating system and application controls and patching
  - System architecture
  - Signing & encryption for communication
  - Multi-factor authentication
  - Application restriction (whitelisting)
  - Detection and response technology

Operational Excellence Aids Security

Match IT's Pace

- **The lifespan of information systems is about 5 years**
  - IT systems are the brains of other business systems
  - Durable and adaptive IT systems is the objective
- **Patch deployment and system replacement**
  - Known part of the IT investment
- **Keep up with the pace of IT development and deployment**
  - Prepare for the next generation now

Align Cyber Operations to Your Business

Component 2

- **Validation provides confidence to focus on the right systems and detections**
  - MITRE ATT&CK defensive coverage
  - Track what you've encountered
  - Use cases focused on business risk

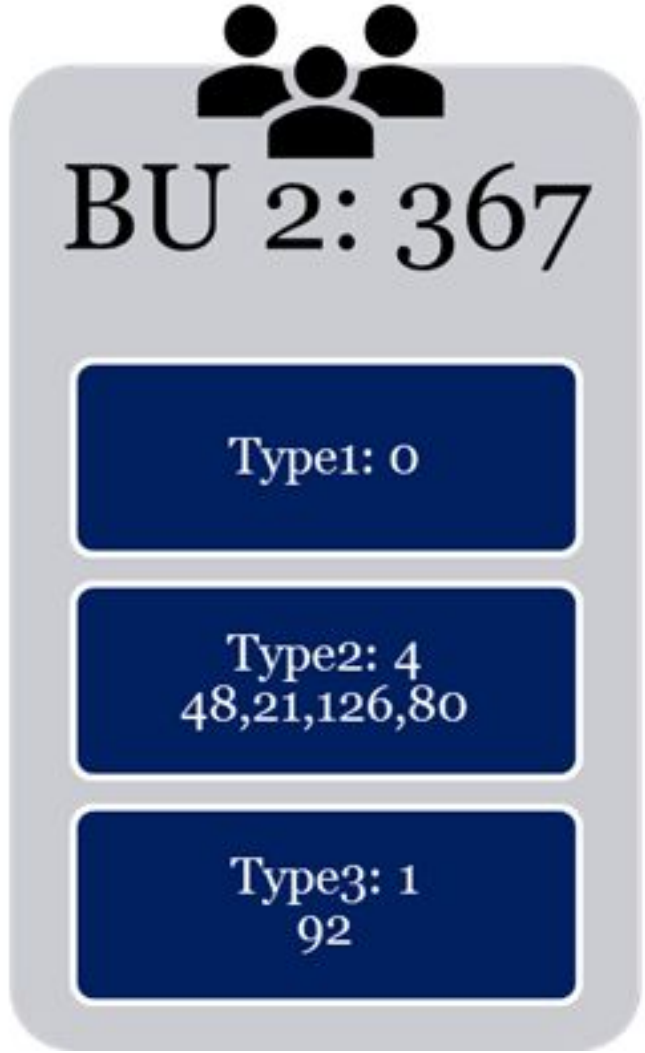
Optimize What is Ignored

Report Useful Metrics

Component 3

Quantify:

- **Loss prevention to show SOC's value**
- **Impact based on affected system value**
  - Prerequisite: system inventory and valuation
  - Organizational risk evaluation



Optimize Collected Data and Analysis

Engineer Relevant Detections

Component 4

- **Gain visibility where needed**
- **Build environmentally cued detection opportunities**
  - Behavioral differentiations trained through tracking, machine learning, or speculated
- **Utilize threat Intelligence**
  - Historically applied once ingested
  - Predictive based on knowledge of attack surface
  - Developed internally, then strategically shared to ruin adversary capability

Engineer Relevant Detections

Embrace Hunting as a Paradigm

Component 5

- **Build a team hunting framework**
- **Reward hunting mindset**
  - *We're compromised, but we can't yet see it*
- **Cultivate staff creativity and relentless pursuit of adversaries**

Hunting as a Paradigm

- **Hunting is "clumsy but swift"**
  - Use case ideas on where engineering is worth it
  - Fills gaps: rapid, responsive, and ad hoc
- **It exposes gaps too**
  - Posture improvements are outcome of hunts

Hunting to Supercharge Engineering

Deceive the Adversary

Component 6

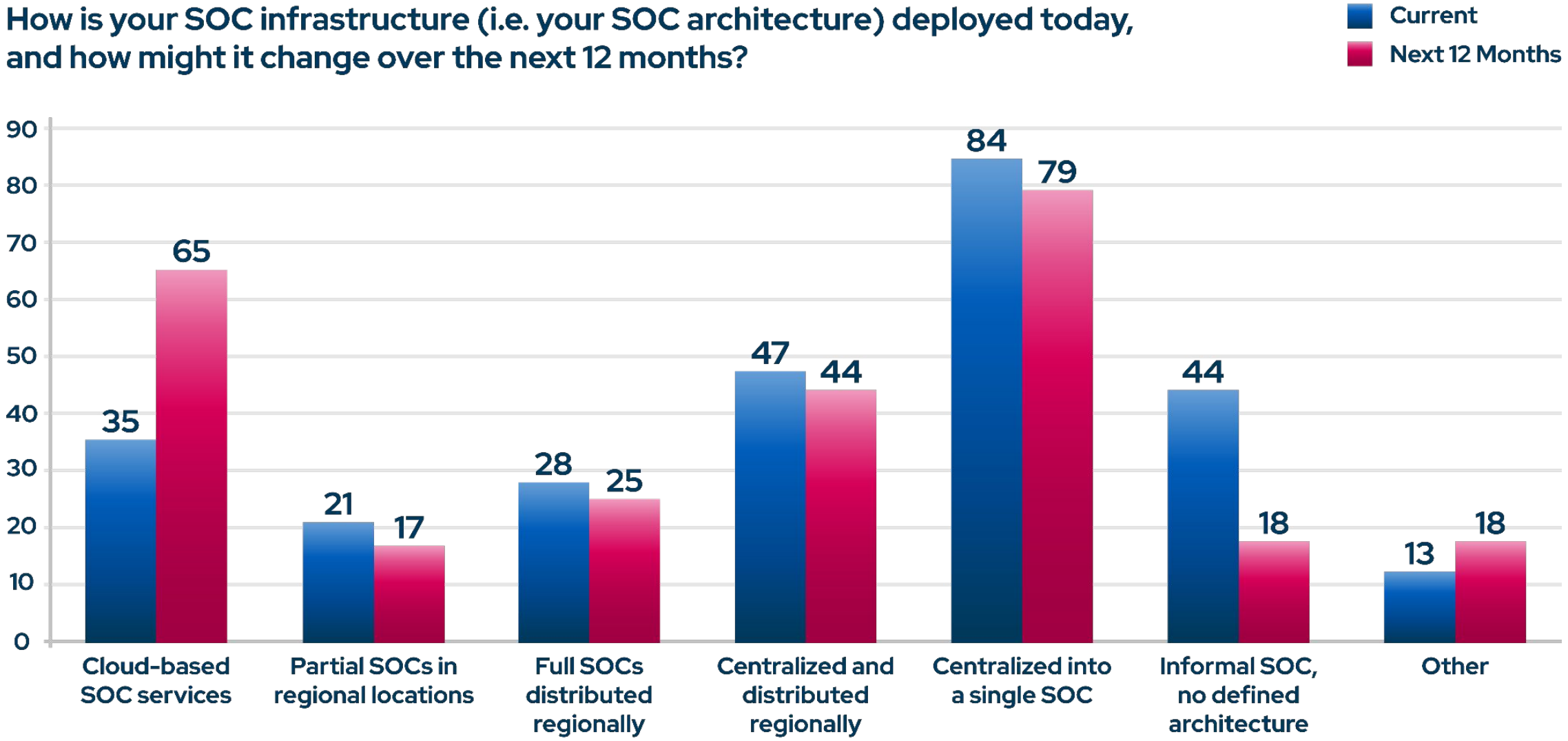
- Switch suspect systems into observation networks for containment to aid verification
- Post email addresses to lure spam for easier identification
- **Hint**: “Live off the land” traps listed at LOLBALS-Project

Deception Aids Detection

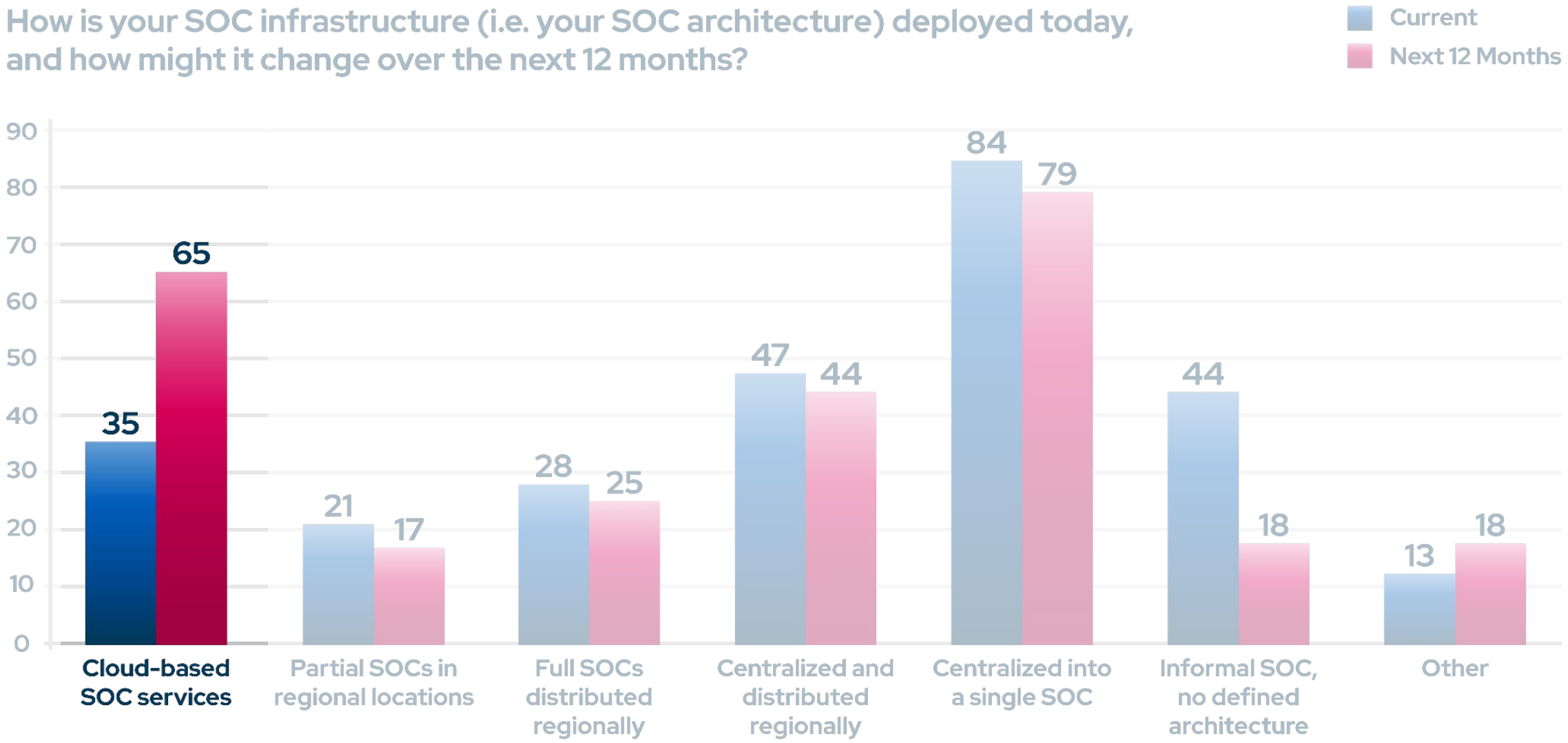
Embrace the Cloud

Component 7

How is your SOC infrastructure (i.e. your SOC architecture) deployed today, and how might it change over the next 12 months?



Cloud: 2021 SANS SOC Survey



Cloud: 2021 SANS SOC Survey

- **Embrace cloud deployments**
  - Standard, secure baseline deployments
  - Ability to quickly change
- **Utilize cloud to resolve SOC operations resource, staffing, and technology challenges**
- **Use cloud native monitoring, response, analysis**
  - Native response capabilities leveraged

Embrace the cloud

Train Superior Analysts

Component 8

- Enhance visibility through integrated tools
- Application whitelisting for execution restriction
- Automate as your standard practice
- Validate visibility and detection

Tools Supporting Analysis

- Cultivate intelligence and analysis
- Good work practices: mental health, attentiveness, awareness, skepticism, humility, communication
- Analytical methodology producing fast, effective, reproducible, and defendable assessments

Encourage Analyst Performance

Unify Your Team

Component 9

- Continuous self-training and information sharing
- Empowered, caring staff
  - Overcome technology shortcomings
  - Rise to the level of effective adversaries
- Purple teaming exposes gaps and validates analyst performance

Set Common Objectives

Supercharging Action Items

- **Key components to supercharge a Modern SOC:**
  - Develop IT Operational Excellence
  - Align Cyber Operations to Your Business
  - Report Useful Metrics
  - Engineer Relevant Detections
  - Embrace Hunting as a Paradigm
  - Deceive the Adversary
  - Embrace the Cloud
  - Train Superior Analysts
  - Unify Your Team

Action Items

THANK YOU!