SentinelOne

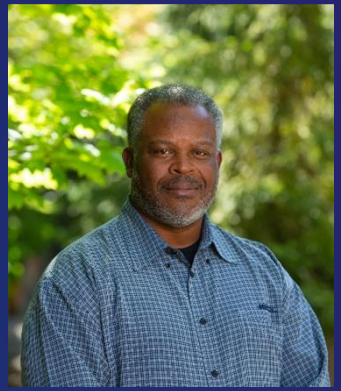
MICROSERVE

Empowering People through Technology

From Detection to Response: Winning the Cybersecurity Battle in Public Sector

Victoria Convention Centre
March 11, 2025

PRESENTERS



Cornelius Temple

Regional Sales Manager – BC Sales
Microserve

Elie Nasrallah

Solution Engineer
SentinelOne

MICROSERVE SERVICE PORTFOLIO

End-User Computing

Managed Print Services

Managed Services

Data Center & Network

Audio Visual

IT Staffing Services

Cybersecurity

Backup & Disaster Recovery

Modern Workplace

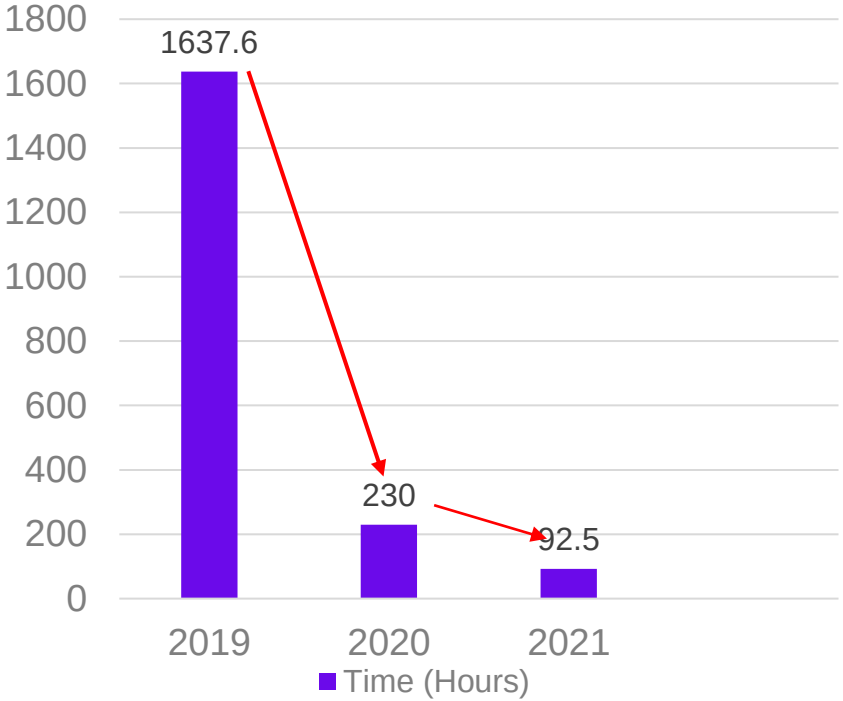
Training & Adoption

Cloud Solutions

IT Procurement

MICROSERVE

Attackers are Continuously Evolving



Initial Network Access to Payload Deployment*

- Attackers are becoming faster and more sophisticated
- Average Ransomware Duration going down from 68 days (in 2019) to less than 4 days (2022)
- Research** suggests average encryption times across Ransomware strains is 24.52 minutes
- LockBit being the fastest encrypting ransomware 5:50 minutes.

*Countdown to Ransomware: Analysis of Ransomware Attack Timelines by IBM

**Ransomware Encrypts Nearly 100,000 Files in Under 45 Minutes by Splunk

All SecOps Teams Have Similar Top Level Goals

Build Resilience Against Cyber Attacks

Minimize Business Impact & Loss Due to Cyberattacks

Meet Compliance Objectives

Save Company's Mission

Your SecOps Team Wants...

Reduce Mean Time to
Detect. Investigate. Respond.

Reduce Total Cost of Ownership (TCO)

Improve SecOps
Efficiency, Skillset & ROI

Improve
Performance & **Scale**

Evolution of Security

AV/ Old Legacy Protection

Signatures (Anti Virus)

- People powered
- Lacks scale and coverage
- Rarely finds advanced attacks

Legacy EDR:
People Driving Tech

Cloud Based Monitoring

- People/expert powered; technology assisted
- Data intensive “haystack” telemetry
- Reactive responses. Complex recovery.

Tech Assisting People

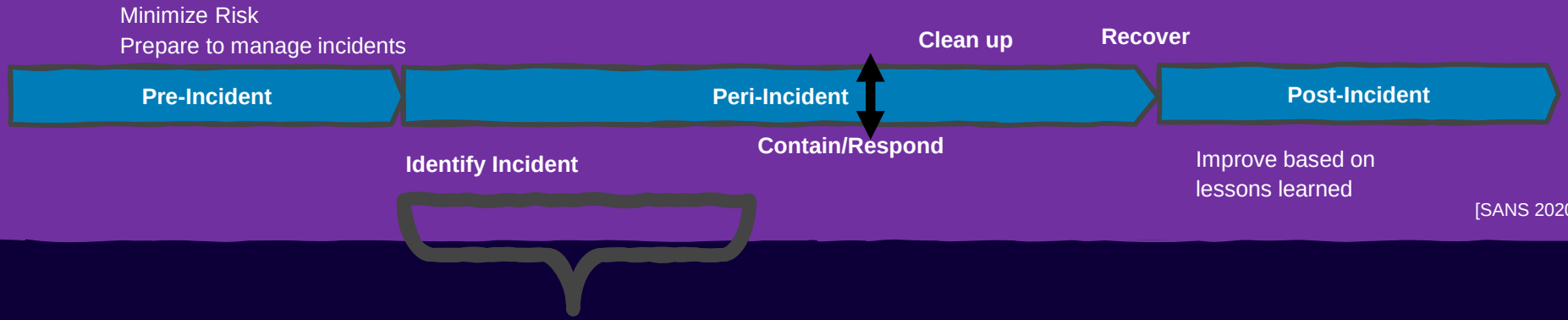
SentinelOne
Secure Tomorrow

Purple AI

AI on Device + Cloud

- Data platform to assist people
- Machine-built context + response
- Automations shrink mean time to respond & recovery.

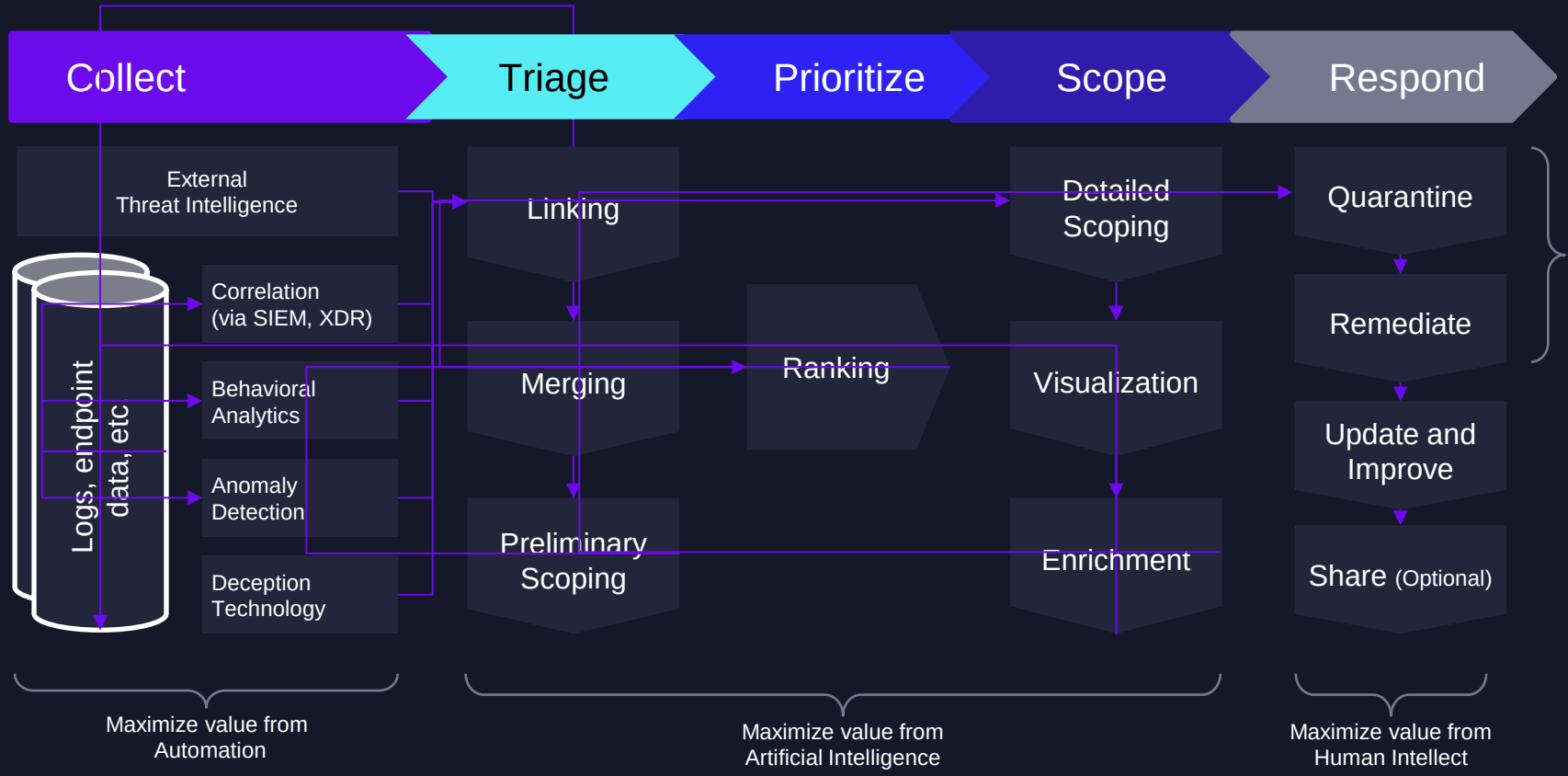
Incident Response



End-to-end “time to containment”

1. MTTD – Mean Time To Detect
2. MTTI- Mean Time to Investigate
3. MTTR – Mean Time To Respond

Workflow of an Attack Investigation



Benefits of Human-Machine Teaming

Simplified Triage

- Improve Artifact Extraction
- Automate Data Gathering
- False-Positive Reduction
- Signal from Noise
- Reduced Complexity

Integrated Response

- Conformity and Visibility of Actions
- Designed for Repeatability
- Improve Confidence
- Reduce MTTD & MTTR

Staff Efficiencies

- Optimize FTE Requirements
- Automate Tier 1 tasks
- Analyst Coaching
- Reduce Alert Fatigue
- Actually Have Time for Team Training

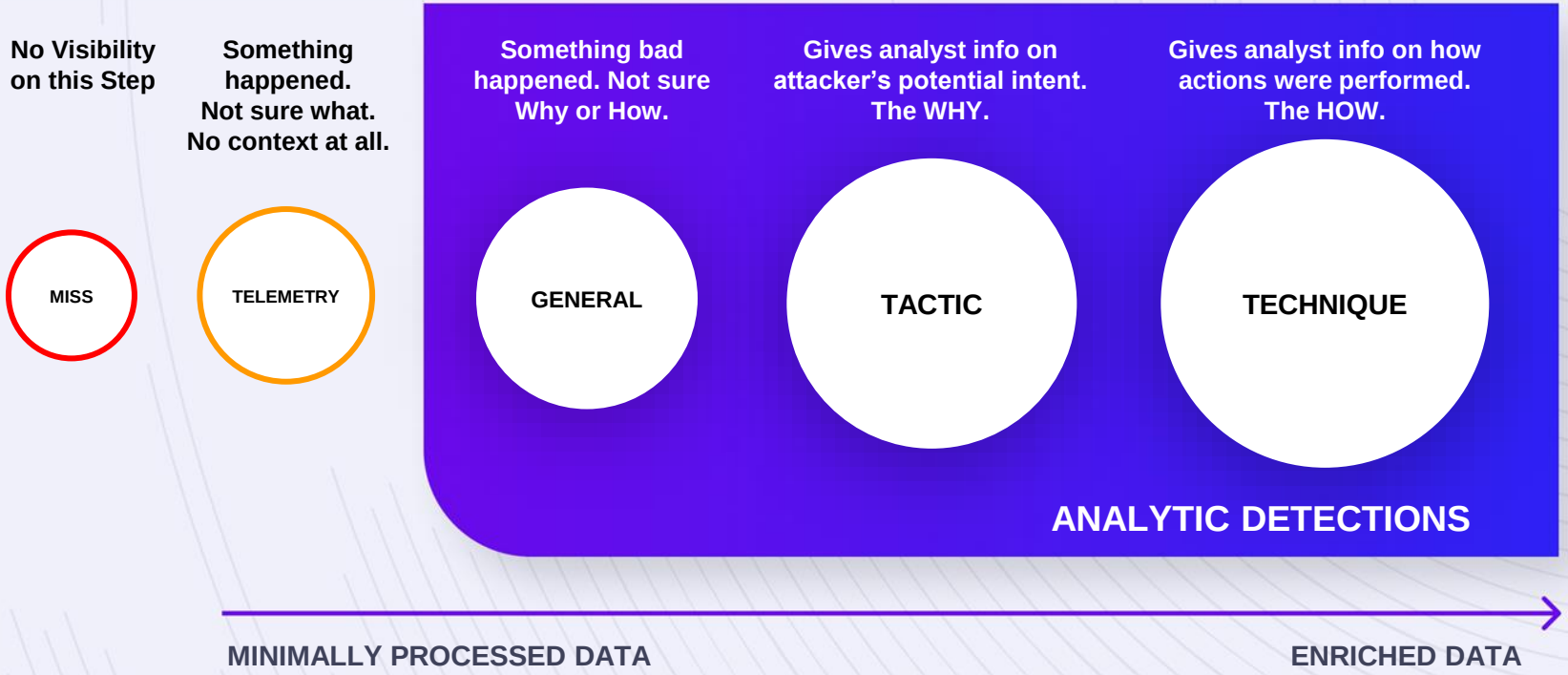
The Critical Role of Digital Forensics in IR

1. **Preserving Evidence**
2. **Identifying the Source of the Attack**
3. **Understanding the Scope of the Incident**
4. **Supporting Incident Response Activities**
5. **Legal and Regulatory Compliance**
6. **Post-Incident Analysis**
7. **Mitigating Reputation Damage**

Cybersecurity Metrics for the Board Level

- **Mean Time to Detect (MTTD)**
  - Importance: Shows the efficiency of the detection capabilities.
  - How quick can the security team can identify potential threats.
- **Mean Time to Respond (MTTR)**
  - Importance: Demonstrates how efficiently the security team can respond to detected threats.
  - Reflects the ability to contain and remediate incidents following detection.
- **Mean Time to Contain (MTTC)**
  - Importance: Measures the speed at which threats are stopped from spreading within the network.
  - Indicates good lateral movement controls and fast quarantine effectiveness

Detection Categories



MODIFIER DETECTION TYPES →

Config Change

Delayed

AI Endpoint Detection and Response (EDR)

- Protect against malware with autonomous, machine-speed prevention powered by on-device AI.
- Detect ransomware with behavioral and static AI models that analyze anomalous behavior and identify malicious patterns in real-time
- Detect, Hunt and Investigate with AI for Rapid MTTD & MTTR

Key Takeaways

01

Assume ‘Attacker mindset’, then SecOps mindset, and focus on incidents more than just closing alerts

02

Maximize efficiency utilizing available Automation, and effectiveness using a Data Driven Approach

03

Increase Incident Preparedness by having defined, tested, and team trained SOPs and Playbooks

04

Use Tech Assisting Human approach vs Human Assisting Tech

Q&A

Ask us directly or Contact your Microserve Account Manager.

FOR INQUIRIES EMAIL:
INFO@MICROSERVE.CA

VISIT: MICROSERVE.CA

MICROSERVE

MICROSERVE
Celebrating 35 Years in Business

Special Thanks To Our Partners

VANCOUVER
280 - 4400 Dominion Street
Burnaby, BC V5G 4G3
Tel: 604-473-9883

VICTORIA
1969 Keating X Rd
Saanichton, BC V8M 2A4
Tel: 250-652-3737

EDMONTON
5607 67 Ave NW,
Edmonton, AB T6B 2R8
Tel: 780-496-9585

CALGARY
2611 Hopewell Pl NE #117,
Calgary, AB T1Y 7J7
Tel: 403-250-5888

www.microserve.ca