SANS

BLUE TEAM

SUMMIT & TRAINING

Live Online

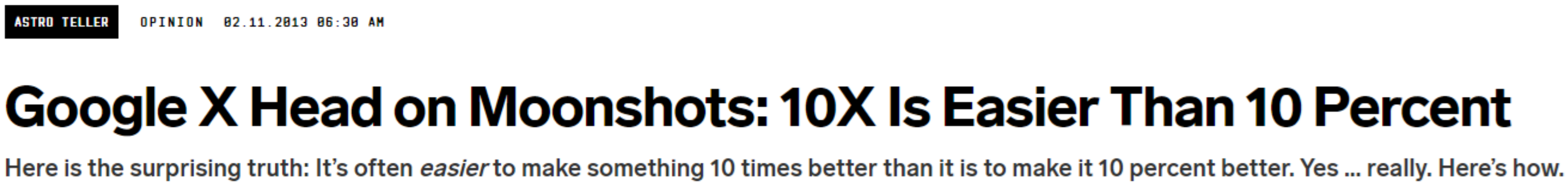
Summit: September 9–10, 2021

Can We REALLY 10X the SOC?

Dr Anton Chuvakin

Outline

- Reminder: SOC today
- Why change the SOC?
- Improve SOC 10% or 10X?
- Possible routes to 10X SOC



ASTRO TELLER OPINION 02.11.2013 06:30 AM

Google X Head on Moonshots: 10X Is Easier Than 10 Percent

Here is the surprising truth: It's often *easier* to make something 10 times better than it is to make it 10 percent better. Yes ... really. Here's how.

Reminder: SOC today

What is a SOC?

> A security operations center provides centralized and consolidated cybersecurity incident prevention, detection and response capabilities.
>
> – Gartner

TEAM

PROCESSES

TECHNOLOGY

Why change the SOC?

Forces that Push SOC

Force 1: Expanding attack surface
More things to secure...

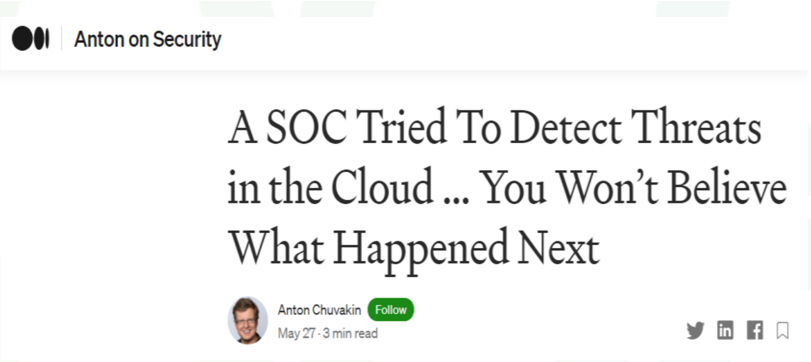
Force 2: Security talent shortage
More things to secure than people...

Force 3: Too many alerts from too many tools
More things to secure that all scream for attention...

(source)

Also, Here is Cloud!

- Uncommon log collection methods
- Telemetry data volumes may be high
- Alien licensing models for security tools
- Alien detection context (!)
- Lack of clarity on cloud detection use cases
- Governance sprawl
- SOC teams lacking cloud skills
- Ill-fitting tools
- Lack of input from SOCs into cloud decisions


Anton on Security

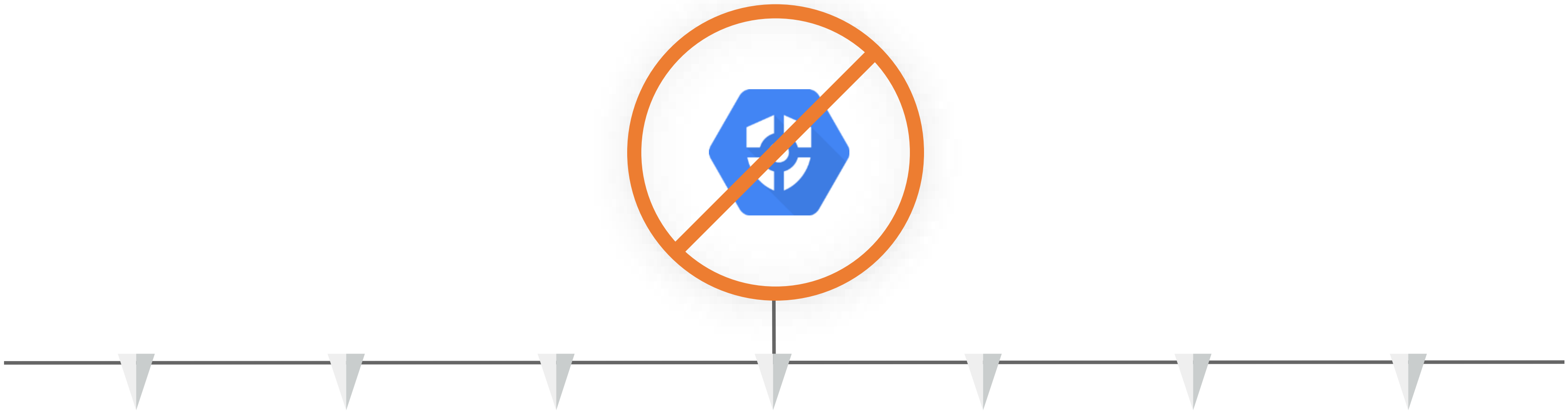
A SOC Tried To Detect Threats in the Cloud … You Won’t Believe What Happened Next

Anton Chuvakin

May 27 · 3 min read

Improve SOC 10% or 10X?

“Classic” SOC … Let’s Make It 10% Better …



Inspired by IT helpdesk philosophy

Treats incidents as rare and abnormal

+10%

Focuses on alert pipeline, and pairs alerts to analysts

+10%

Centered on a SIEM (SOC = SIEM analyst team)

Has walls between alert handlers and alert tuners

+10%

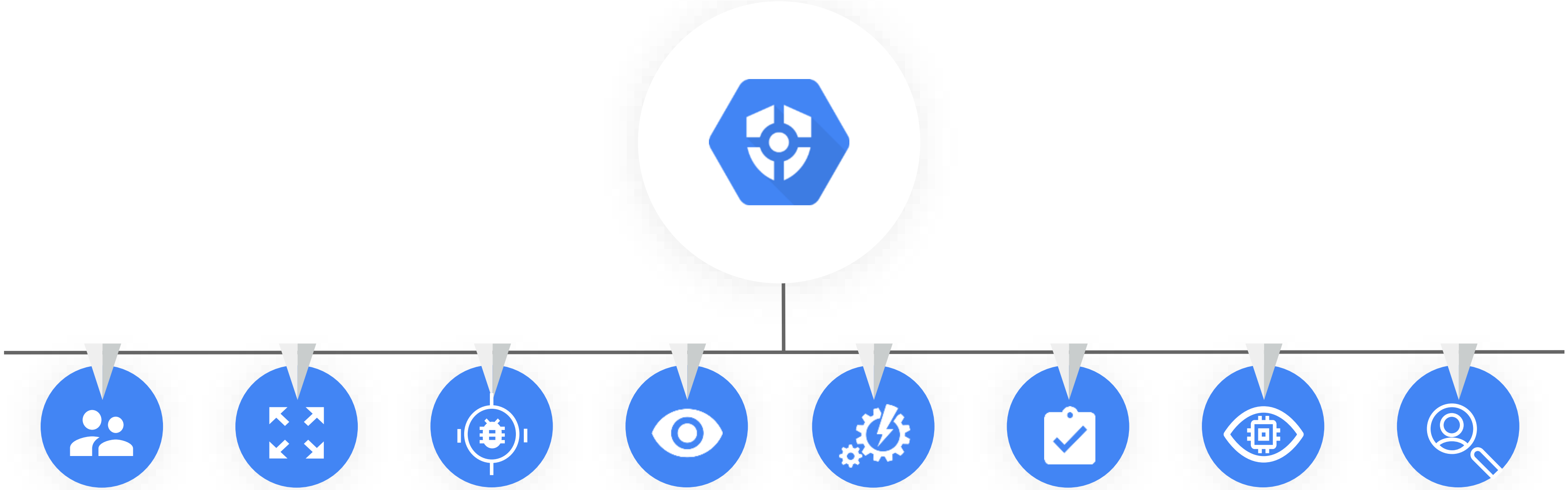
Threat intelligence is sometimes consumed

+10%

Shallow metrics on handling time

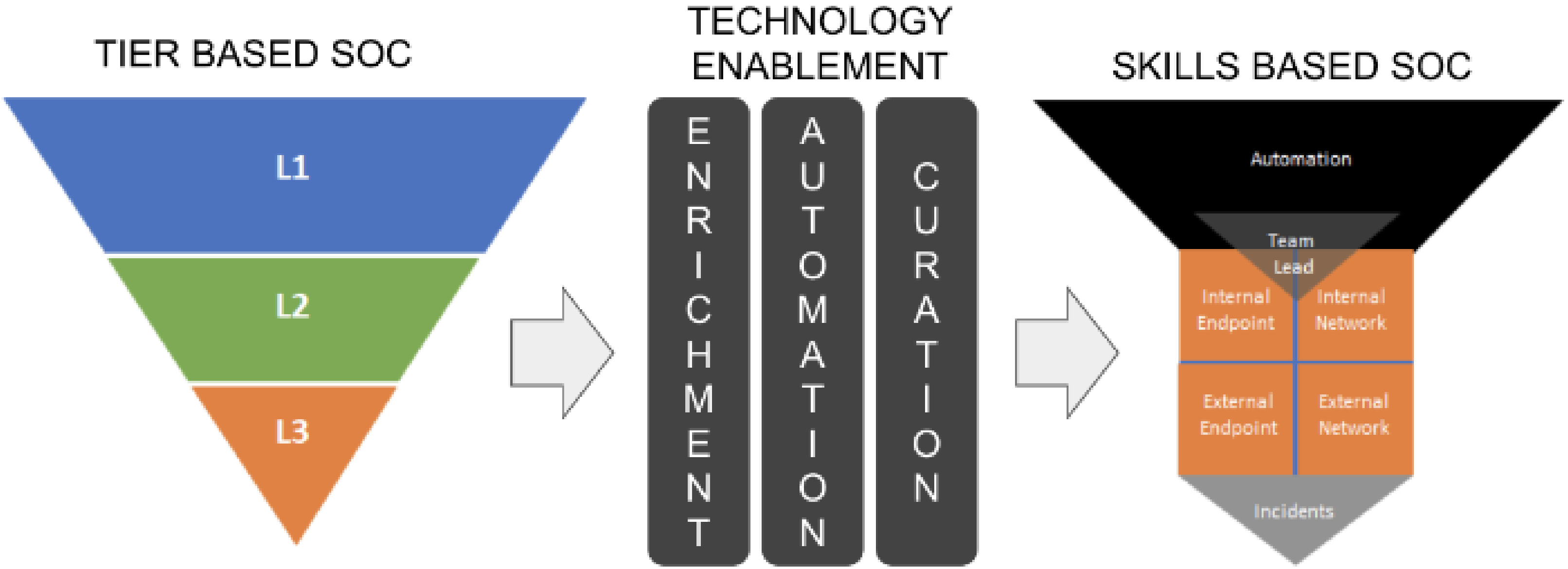
OLD SOC! **NOW** WITH +10% FASTER ALERT TRIAGE AND 10% LOWER FALSE POSITIVES! :-)

Modern SOC



- Teams are organized **by skill, not rigid level**
- Process **structures around threats,** not alerts
- **Threat hunting** covers cases where alerts never appear
- **Multiple visibility approaches,** not just logs
- **Automation** via SOAR works as a force multiplier
- Deeper **testing and coverage analysis**
- **Threat intelligence** is consumed and created
- **Detection engineering** (analysts are engineers)

Highlights of Modern SOC: People



Highlights of Modern SOC: Process

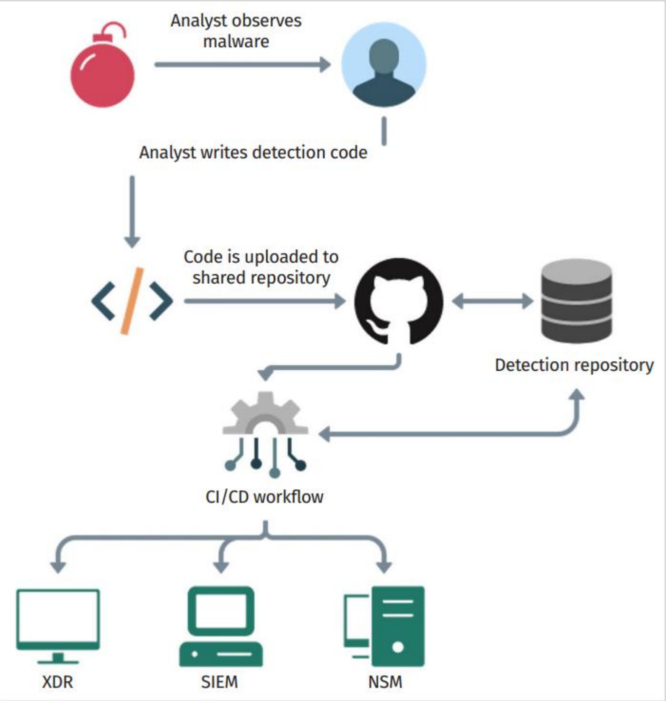


Figure 5. Flow of Detections as Code

1 Detection content versioning

2 Proper “QA” for detection content”

3 Content (code) reuse and modularity

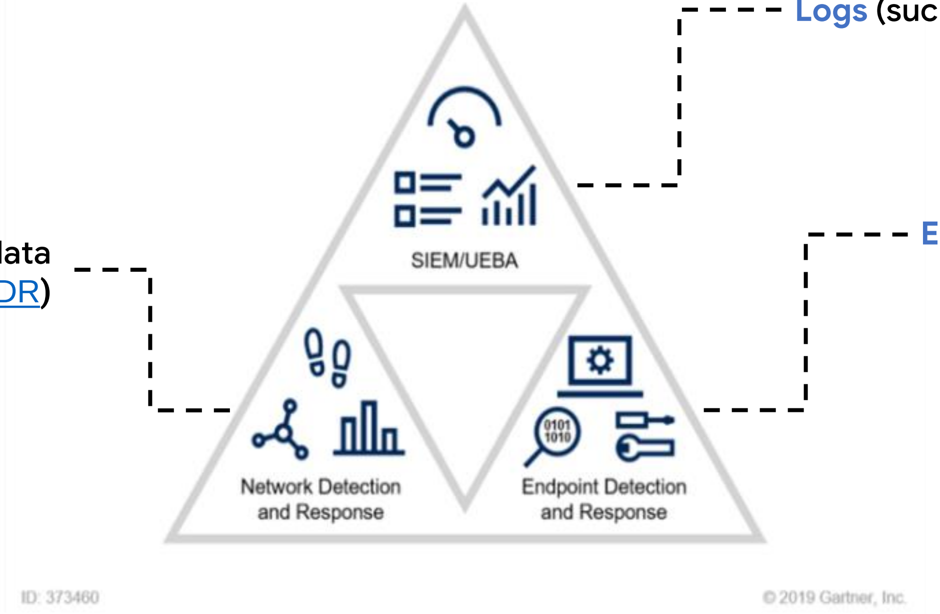
4 Cross-vendor and cross-tool content

5 Metrics, coverage and improvement

P.S. This is not about programming as such

Highlights of Modern SOC: Technology

Security Operations Visibility Triad


SIEM/UEBA
Network Detection and Response
Endpoint Detection and Response

ID: 373460

© 2019 Gartner, Inc.

Logs (such as via SIEM)

Network data (such as via NDR)

Endpoint data (such as via EDR)

Usually unified by **SOAR**

P.S. Logs aren't always #1 on the list

Possible routes to 10X SOC

SOC Transformation Framework

	Tactical	Strategic	Transformational
People	Grow the analysts to develop detections Hire partners to augment your team	Rotate analysts and engineers	Federated workforce that operates synergistically across org-wide risks Analysts are engineers and develop scalable solutions to security issues
Process	Optimize the alert triage process Expand the use of threat intelligence	Start threat hunting Refine threat intelligence	Threat hunters and blue team drive collaborative missions & objectives Create threat intelligence
Technology	Evolve SIEM, expand to other visibility approaches Experiment with SOAR & automation	Adopt SaaS tools for SIEM, EDR, etc Deploy automation use cases	Leverage a cloud-native tech stack Develop AI/ML use case engineering

Plan, advocate, evangelize, and drive a transformation of your SOC to a Security Operations Center of Excellence.

People Transformation

TACTICAL

Grow the analysts to develop detections

Hire partners to augment your team

Offer learning paths and certification opportunities to your workforce

Define a clear boundary to manage a healthy work-life balance for your team

STRATEGIC

Rotate analysts and engineers

Provide comprehensive onboarding and skills development programs

Offer stretch opportunities, career alignment, and leadership training

Revamp your hiring program to seed talent potential and skills-based personnel

TRANSFORMATIONAL

Federated workforce that operates synergistically across org-wide risks

Analysts are engineers and develop scalable solutions to security issues

Continual growth & development of talent and a consistent promotion pipeline

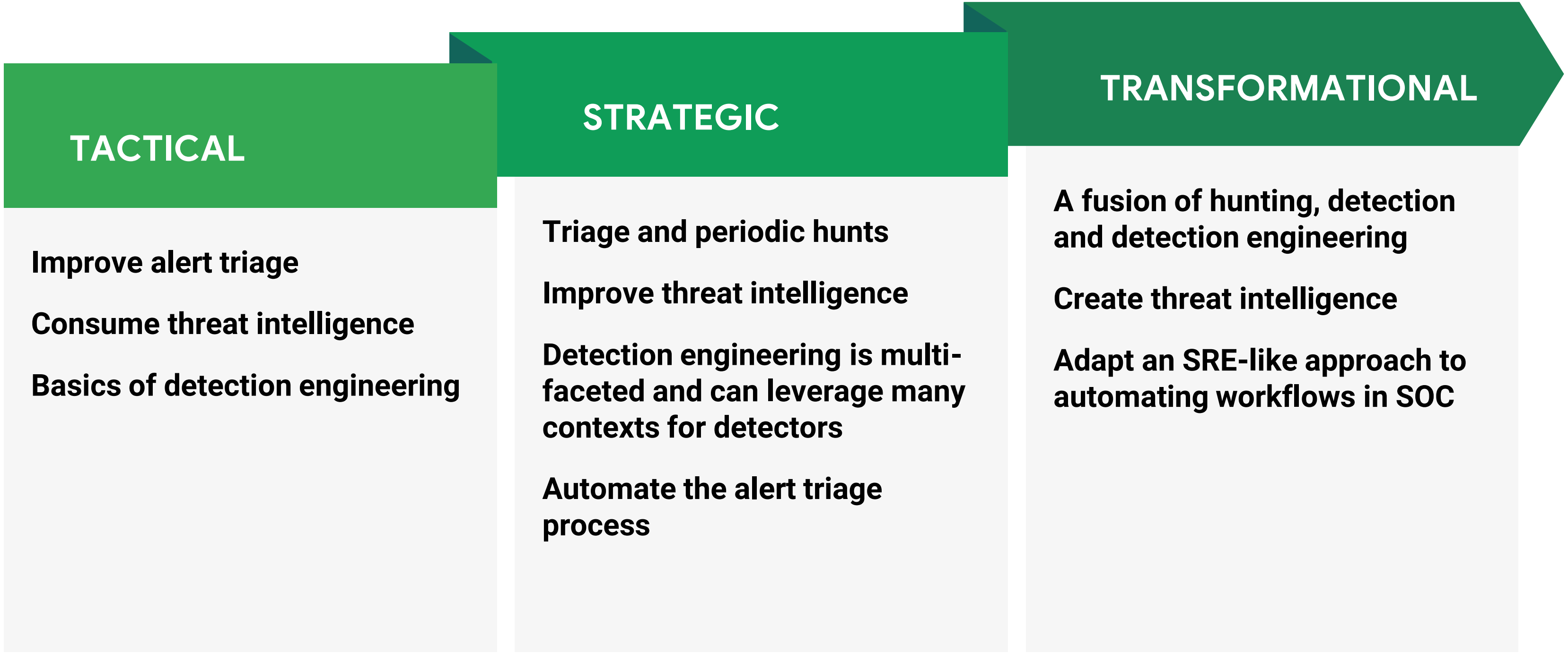
Engage your personnel to represent your team in the industry - talks, speaking opps, conferences, etc

5 Key Steps To Take

People

1. Remove walls in a SOC that separates analysts and engineers
2. Identify skills needed in your SOC, start to hire skills, not levels
3. Boost productivity with automating routine tasks (via SOAR)
4. Take advantage of partners & 3rd parties
5. Create a culture of empowerment and innovation

Process Transformation



TACTICAL

Improve alert triage

Consume threat intelligence

Basics of detection engineering

STRATEGIC

Triage and periodic hunts

Improve threat intelligence

Detection engineering is multi-faceted and can leverage many contexts for detectors

Automate the alert triage process

TRANSFORMATIONAL

A fusion of hunting, detection and detection engineering

Create threat intelligence

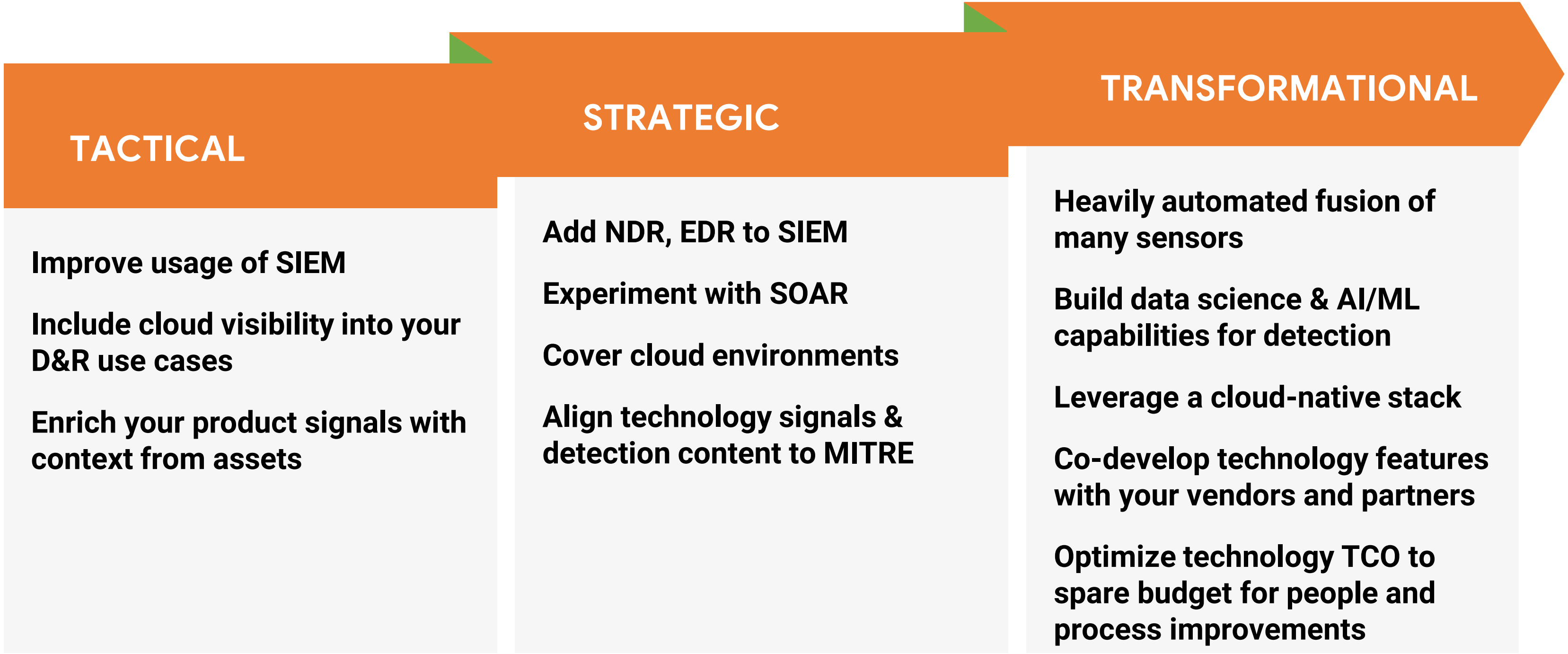
Adapt an SRE-like approach to automating workflows in SOC

5 Key Steps To Take

Process

1. Solidify the basics; don’t hunt before you can detect well
2. Focus on threat intelligence to boost other SOC work
3. Drive an “SRE” approach - 50% time towards automation
4. Add hunting, testing and analytics afterwards
5. More transparency will allow more creative problem solving

Technology Transformation



TACTICAL

Improve usage of SIEM

Include cloud visibility into your D&R use cases

Enrich your product signals with context from assets

STRATEGIC

Add NDR, EDR to SIEM

Experiment with SOAR

Cover cloud environments

Align technology signals & detection content to MITRE

TRANSFORMATIONAL

Heavily automated fusion of many sensors

Build data science & AI/ML capabilities for detection

Leverage a cloud-native stack

Co-develop technology features with your vendors and partners

Optimize technology TCO to spare budget for people and process improvements

5 Key Steps To Take

Tech

1. Don’t discard a SIEM / UEBA
2. Expand visibility: NDR, EDR (XDR?), cloud, etc
3. Be aware that SaaS tools will win in the end
4. Use SOAR to automate
5. Use ML, but don’t assume magic...

Without THIS you won’t be SECURE. So INFLUENCE!

	Prevent	Detect	Respond	Secure
Tactical	Migration to the cloud w/ best practices on security architecture & patterns	Ingestion & centralization of all critical data sources, likely outsourcing key SOC roles	Ad-hoc investigative capabilities, outsourcing all response activities	Struggle to react to evolving threats
Strategic	DevOps / Automated Deployment / Config-as-Code. Effective vuln management.	Integrated tooling, SOAR implementation, IOC-matching & strong TI	Dedicated IR team & clearly defined roles, playbooks, and use case coverage	Ability to react to new and existing threats + hunt, but still resource constrained
Transformational	All changes fully controlled, reviewed, and implemented. Highly effective vuln management.	Predictive analytics, detection engineering & automation, threat hunting, behavioral analytics	Adversarial deception, response automation, chaos engineering, full use case coverage	Fully proactive. Minimal MTTD, MTTR, and RTO.

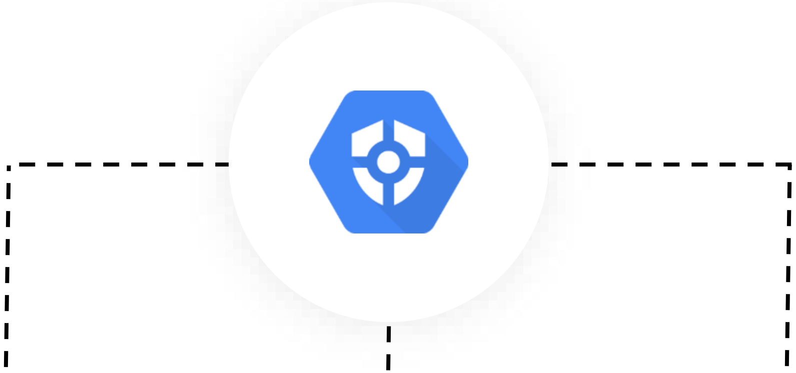
Recommendations

- If SOC = detection team, than **SOC lives on in the modern world**
- Modernize your SOC but **preserve the mission: detection and response**
- Evolve SOC to more **automation** to catch up with modern IT
- **“DevOps” or SRE your detection engineering** (Dev = content creator, Ops = analyst)
  - An idea with 10X SOC potential
- Learn **new detection context** for cloud and cloud-native tools
- **Mercilessly discard tools** that don’t fit the cloud practices or fail to support cloud technology

Resources

- “Modernizing SOC ... Introducing Autonomic Security Operations”
- “New Paper: “Autonomic Security Operations — 10X Transformation of the Security Operations Center””
- “SOC in a Large, Complex and Evolving Organization” (ep26)
- “The Mysteries of Detection Engineering: Revealed!”’ (ep27)
- “Kill SOC Toil, Do SOC Eng”
- “A SOC Tried To Detect Threats in the Cloud … You Won’t Believe What Happened Next”
- “Role of Context in Threat Detection”

Why SOC Lives On … Transformed



SOC as a **CROWDED ROOM** may be dead…

SOC as a **Detection & Response team** is NOT dead.

The future SOC exists as a distributed and autonomic **Security Operations Center of Excellence**.