DIGISERVE
by Telkom Indonesia

SOC as The Foundation of Secure Digital Transformation

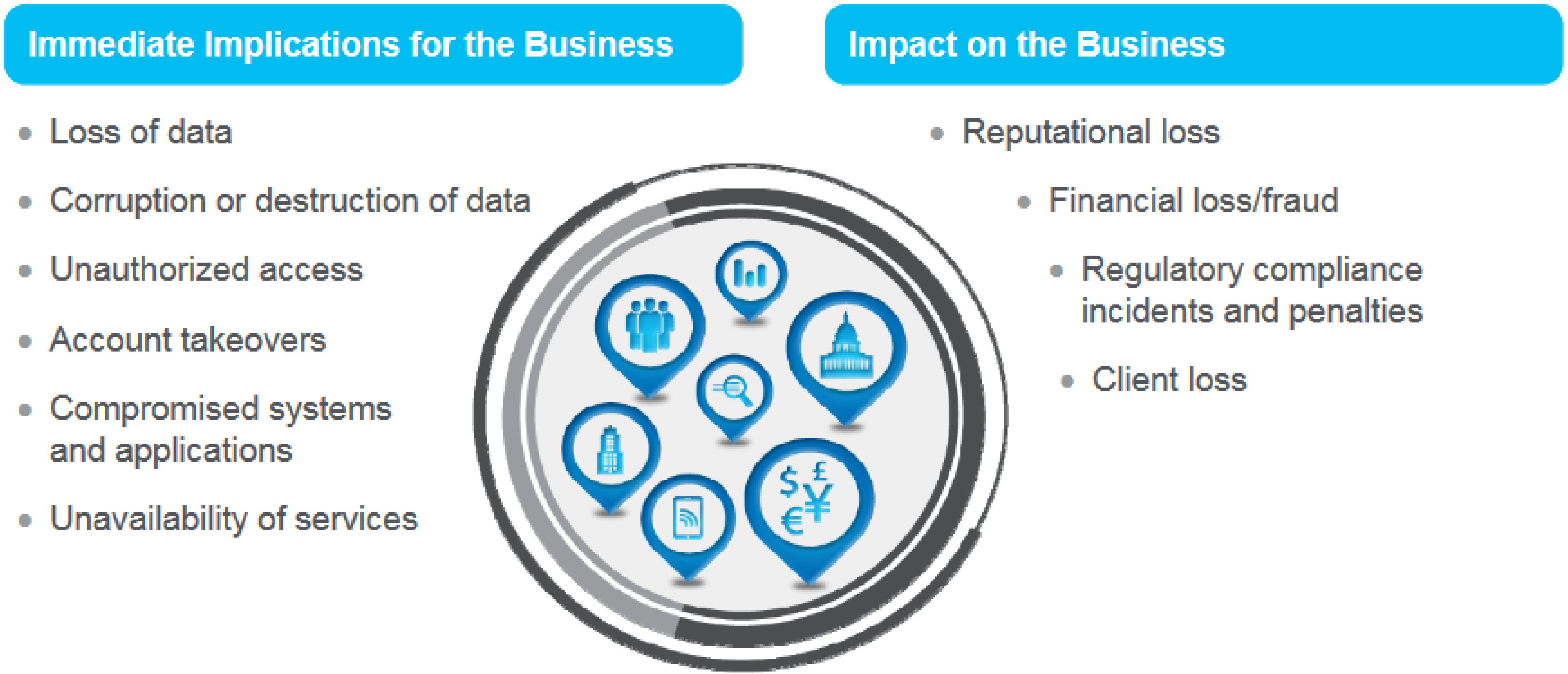
Sharing Session
24 September 2025

Digit Oktavianto
@digitoktav
https://threathunting.id

Who Am I

- **Cyber Security Researcher**
- **Co-Founder BlueTeam.ID (https://blueteam.id)**
- **Community Lead @ Cyber Defense Community Indonesia**
- **Member of Indonesia Honeynet Project**
- **Member of High Tech Crime Investigation Association (HTCIA)**
- **{GCIH | GMON | GCFE | GICSP | | GCTI | GEIR | CEH | CSA | CND | ECSA | ECIH | CHFI | CTIA | ECSS | eCIR | eCTHP | eCMAP} Certifications Holder**

Cyber Security Incident and Its Impact to Business



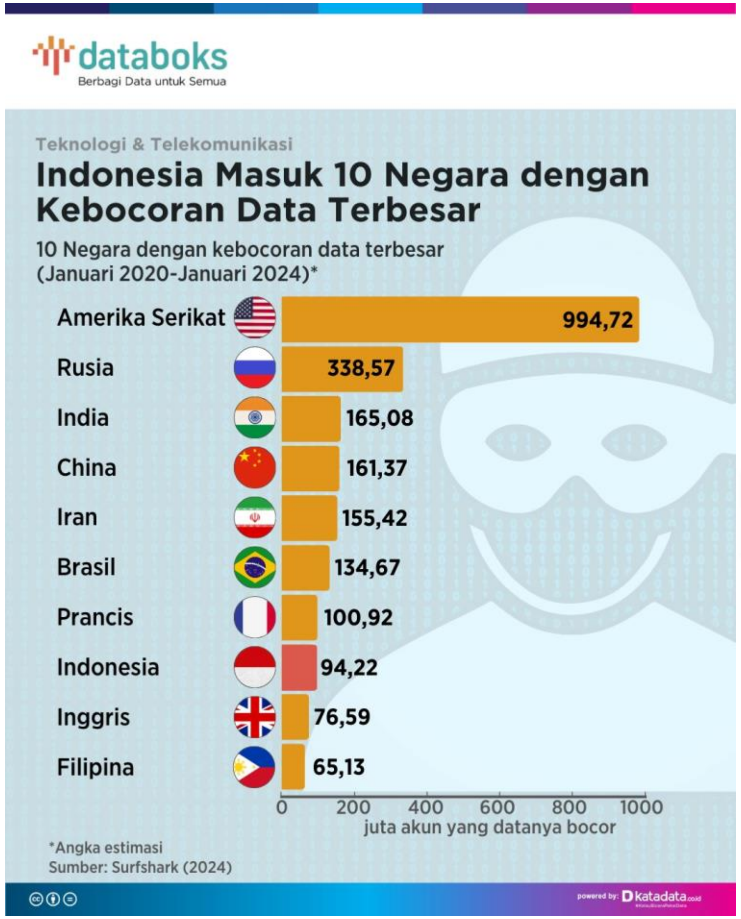
Immediate Implications for the Business

- Loss of data
- Corruption or destruction of data
- Unauthorized access
- Account takeovers
- Compromised systems and applications
- Unavailability of services

Impact on the Business

- Reputational loss
- Financial loss/fraud
- Regulatory compliance incidents and penalties
- Client loss

http://pubdocs.worldbank.org/en/513651432913969312/Ruth-Wandhoefer-Citi-FinSAC-Cyber-Seminar-18-19-May.pdf



databoks
Berbagi Data untuk Semua

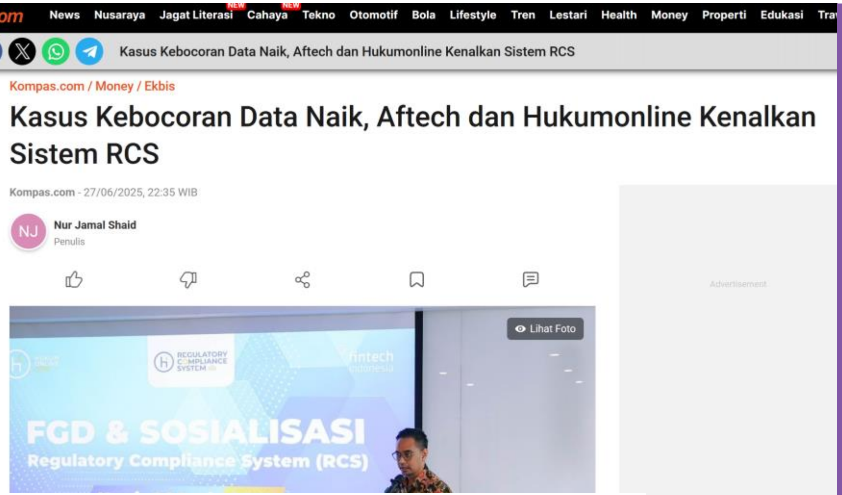
Teknologi & Telekomunikasi

Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar

10 Negara dengan kebocoran data terbesar (Januari 2020-Januari 2024)*

*Angka estimasi
Sumber: Surfshark (2024)

powered by: katadata



Kasus Kebocoran Data Naik, Aftech dan Hukumonline Kenalkan Sistem RCS

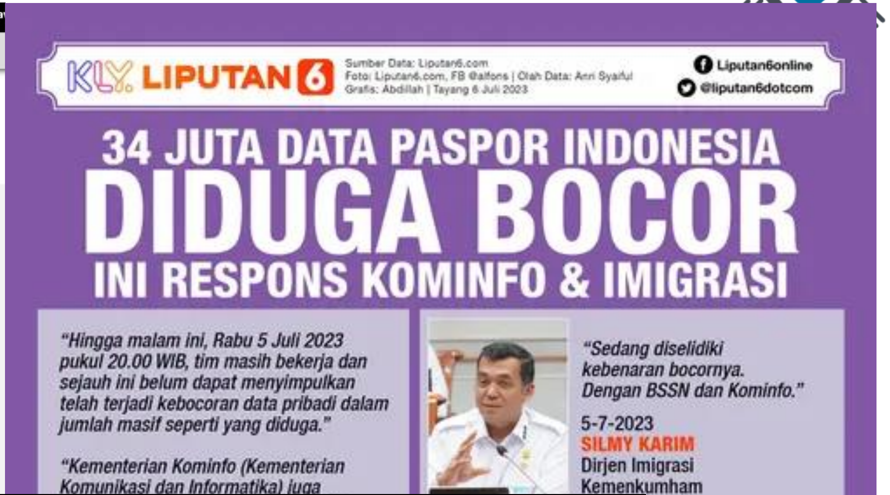
Kompas.com / Money / Ekbis

Kasus Kebocoran Data Naik, Aftech dan Hukumonline Kenalkan Sistem RCS

Kompas.com - 27/06/2025, 22:35 WIB

Nur Jamal Shaid
Penulis

Lihat Foto
REGULATORY COMPLIANCE SYSTEM
fintech indonesia
FGD & SOSIALISASI
Regulatory Compliance System (RCS)
Advertisement



KLY. LIPUTAN 6
Sumber Data: Liputan6.com
Foto: Liputan6.com, FB @alfons | Olah Data: Anri Syaiful
Grafis: Abdillah | Tayang 6 Juli 2023
Liputan6online
@liputan6dotcom

34 JUTA DATA PASPOR INDONESIA DIDUGA BOCOR INI RESPONS KOMINFO & IMIGRASI

"Hingga malam ini, Rabu 5 Juli 2023 pukul 20.00 WIB, tim masih bekerja dan sejauh ini belum dapat menyimpulkan telah terjadi kebocoran data pribadi dalam jumlah masif seperti yang diduga."

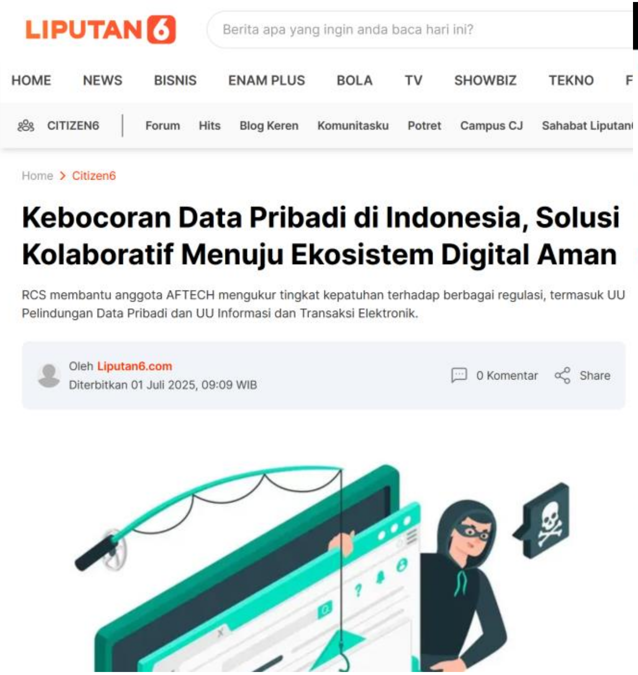
"Kementerian Kominfo (Kementerian Komunikasi dan Informatika) juga

"Sedang diselidiki kebenaran bocornya. Dengan BSSN dan Kominfo."

5-7-2023
SILMY KARIM
Dirjen Imigrasi
Kemenkumham

gkinan valid, karena
M (Nomor Induk
asian) yang hanya
(Direktorat Jenderal)
. Masih agak terbatas
a dan kualitas datanya
menarik bagi kriminal,
gkan data-data yang
ebelumnya."

3
TANUJAYA
eamanan Siber

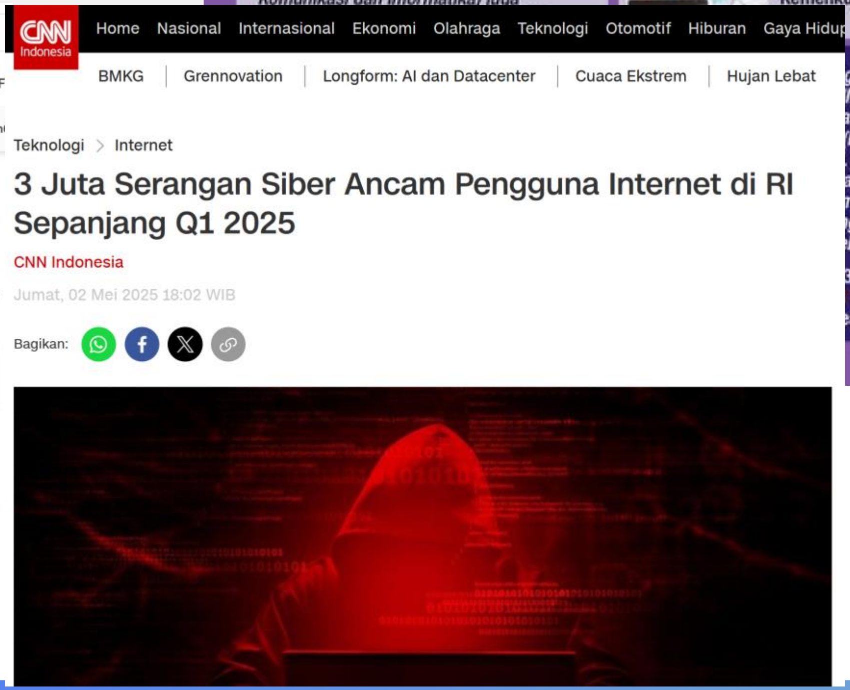


Home > Citizen6

Kebocoran Data Pribadi di Indonesia, Solusi Kolaboratif Menuju Ekosistem Digital Aman

RCS membantu anggota AFTECH mengukur tingkat kepatuhan terhadap berbagai regulasi, termasuk UU Pelindungan Data Pribadi dan UU Informasi dan Transaksi Elektronik.

Oleh Liputan6.com
Diterbitkan 01 Juli 2025, 09:09 WIB



Teknologi > Internet

3 Juta Serangan Siber Ancam Pengguna Internet di RI Sepanjang Q1 2025

CNN Indonesia

Jumat, 02 Mei 2025 18:02 WIB

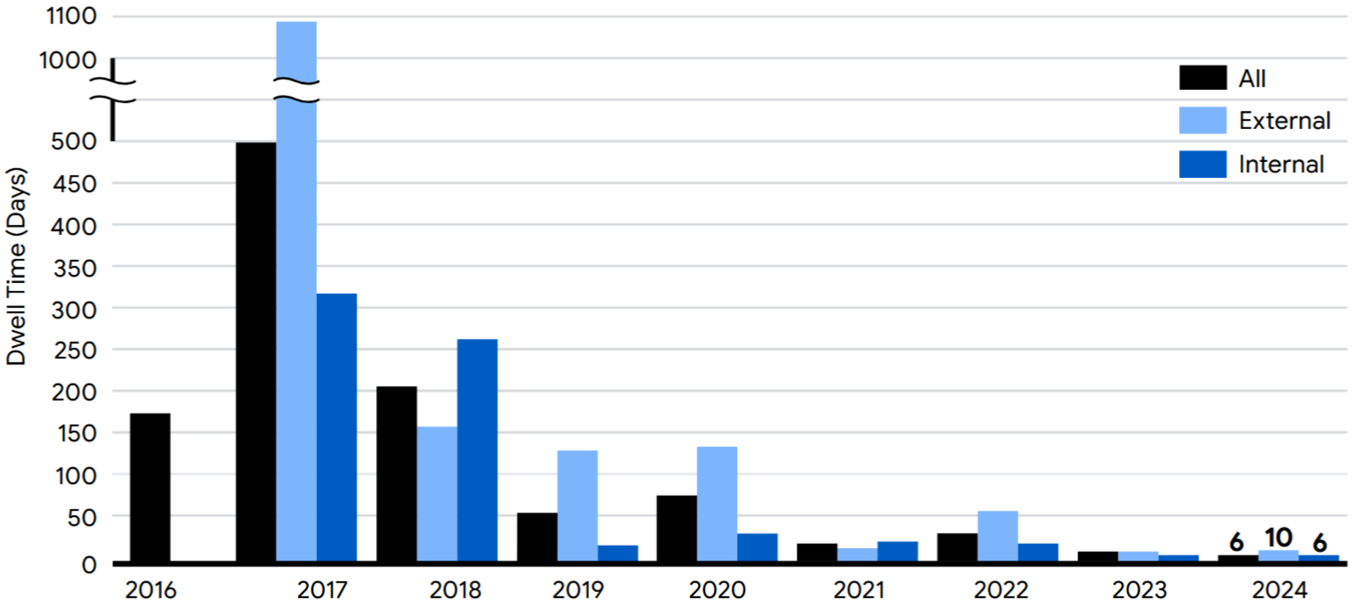
Dwell Time In Cyber Security

Median Dwell Time

The median dwell time for all intrusions in JAPAC in 2024 was six days overall, 10 days for externally notified events, and six days for internally discovered intrusions. For ransomware-related intrusions in JAPAC in 2024, the median dwell time was just four days. For non-ransomware-related compromises, the median dwell time increased to 12 days.

Dwell time is calculated as the number of days an attacker is present in a victim network before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude.

JAPAC Median Dwell Time, 2016-2024



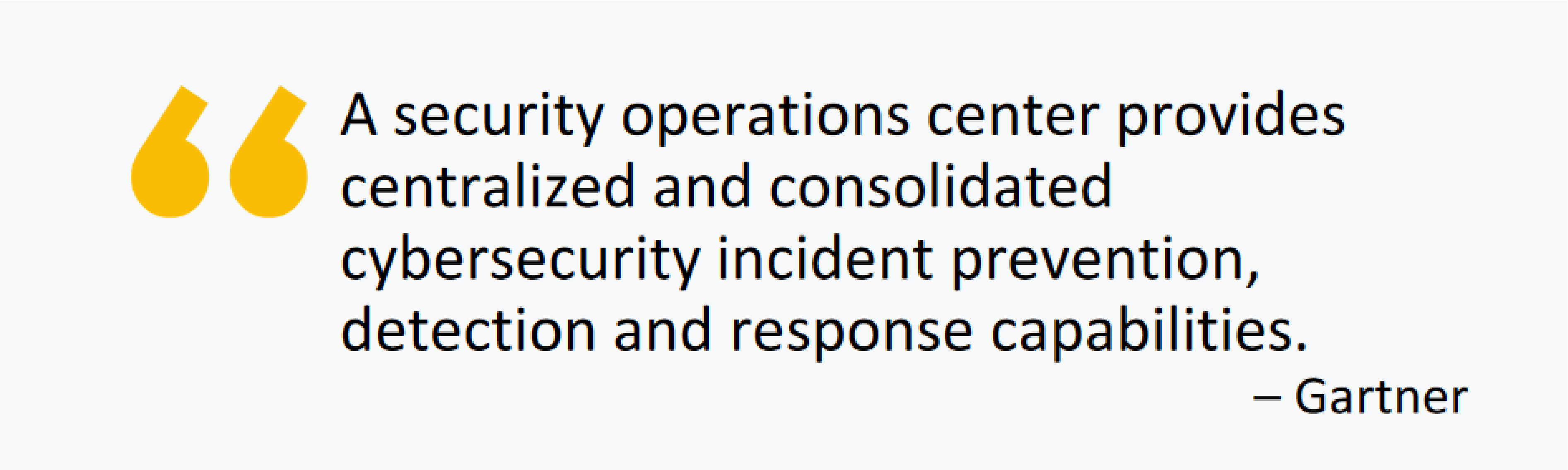
Mandiant M-Trend Report 2025

There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco

Businesses whose cyber security is 'all sorted'
misconfigured firewalls
out of date software
using the same password for everything
no access controls

What is a SOC?

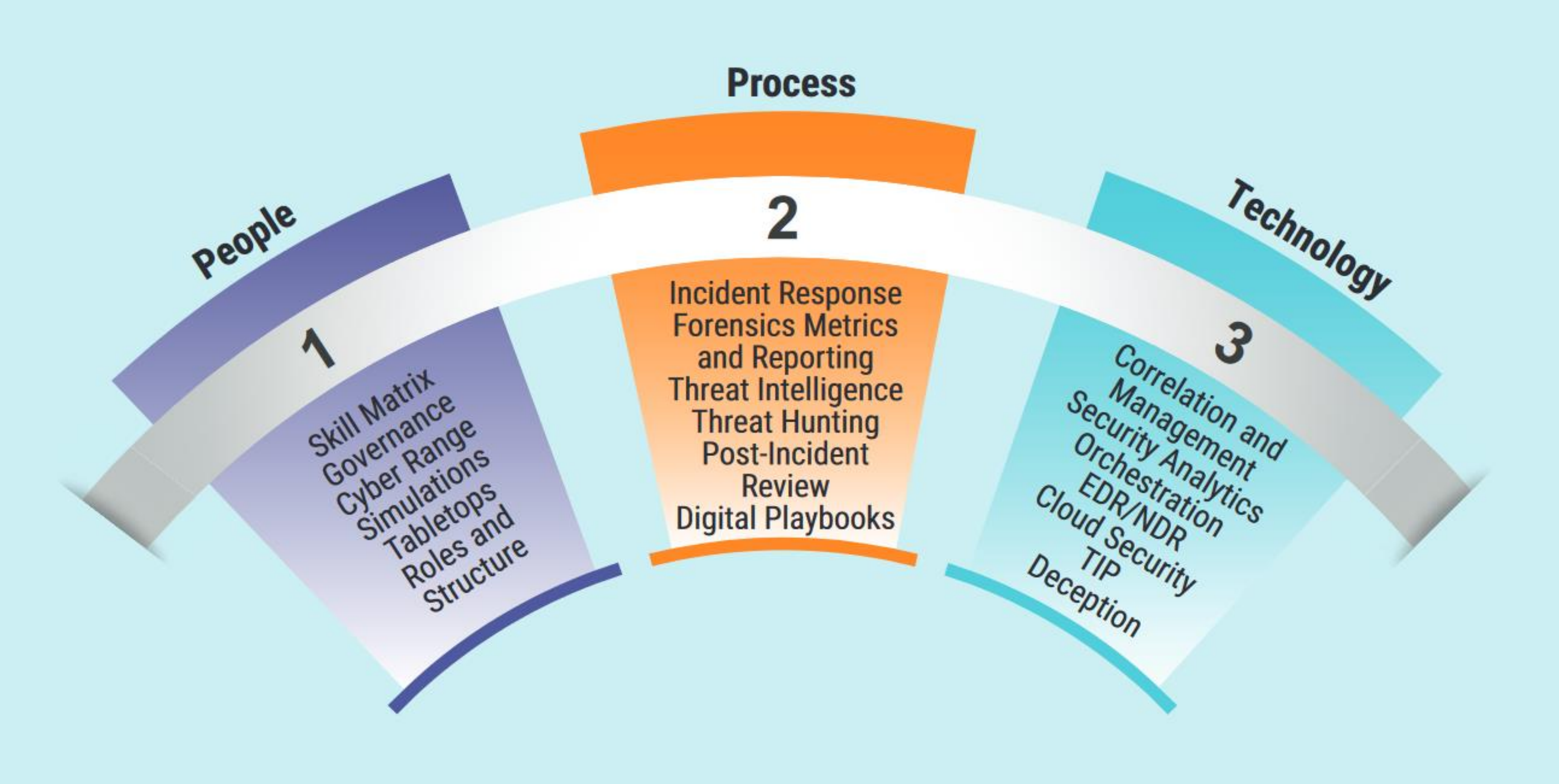


> A security operations center provides centralized and consolidated cybersecurity incident prevention, detection and response capabilities.
>
> – Gartner

SOC Benefits

- Detect and analyze before attacks impact the business
- Investigate, prioritize, and remediate incidents
- Unleash the potential of your existing security team
- Evolve existing tools with better visibility & workflow

Critical Components of SOC



People

1

Skill Matrix
Governance
Cyber Range
Simulations
Tabletops
Roles and
Structure

Process

2

Incident Response
Forensics Metrics
and Reporting
Threat Intelligence
Threat Hunting
Post-Incident
Review
Digital Playbooks

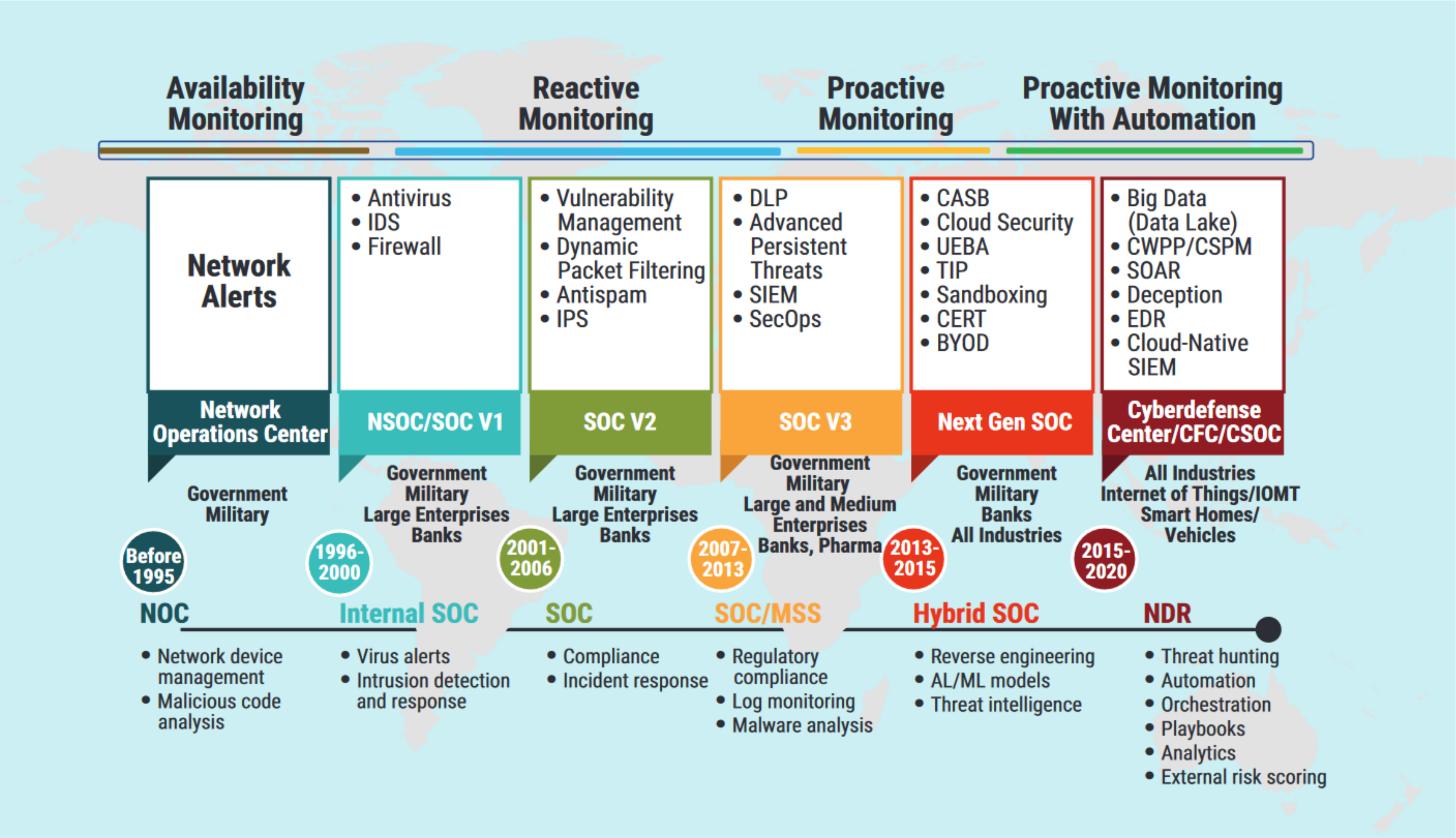
Technology

3

Correlation and
Management
Security Analytics
Orchestration
EDR/NDR
Cloud Security
TIP
Deception

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

Evolutions of SOC



Availability Monitoring

Reactive Monitoring

Proactive Monitoring

Proactive Monitoring With Automation

Network Operations Center (Before 1995)

Network Alerts

Government
Military

NOC

- Network device management
- Malicious code analysis

NSOC/SOC V1 (1996-2000)

- Antivirus
- IDS
- Firewall

Government
Military
Large Enterprises
Banks

Internal SOC

- Virus alerts
- Intrusion detection and response

SOC V2 (2001-2006)

- Vulnerability Management
- Dynamic Packet Filtering
- Antispam
- IPS

Government
Military
Large Enterprises
Banks

SOC

- Compliance
- Incident response

SOC V3 (2007-2013)

- DLP
- Advanced Persistent Threats
- SIEM
- SecOps

Government
Military
Large and Medium Enterprises
Banks, Pharma

SOC/MSS

- Regulatory compliance
- Log monitoring
- Malware analysis

Next Gen SOC (2013-2015)

- CASB
- Cloud Security
- UEBA
- TIP
- Sandboxing
- CERT
- BYOD

Government
Military
Banks
All Industries

Hybrid SOC

- Reverse engineering
- AL/ML models
- Threat intelligence

Cyberdefense Center/CFC/CSOC (2015-2020)

- Big Data (Data Lake)
- CWPP/CSPM
- SOAR
- Deception
- EDR
- Cloud-Native SIEM

All Industries
Internet of Things/IOMT
Smart Homes/
Vehicles

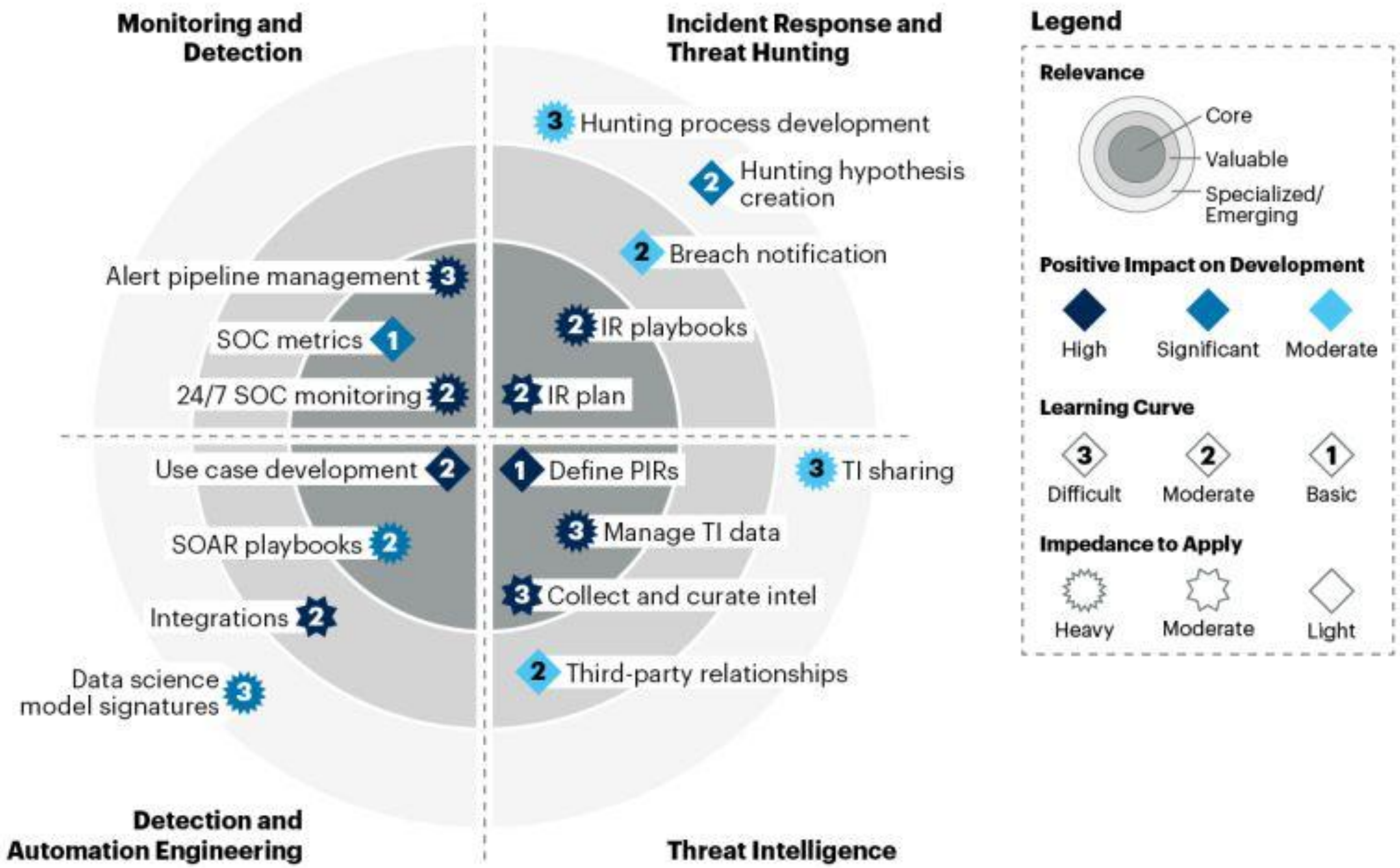
NDR

- Threat hunting
- Automation
- Orchestration
- Playbooks
- Analytics
- External risk scoring

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

SOC Capability Matrix

SOC Capabilities Matrix

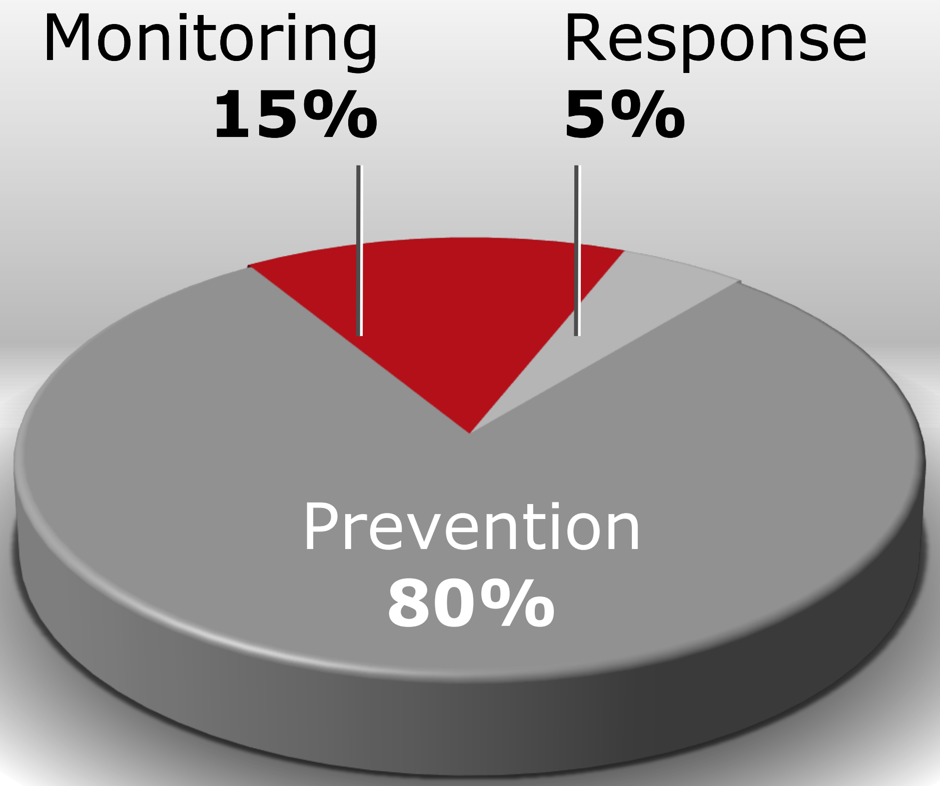


Source: Gartner

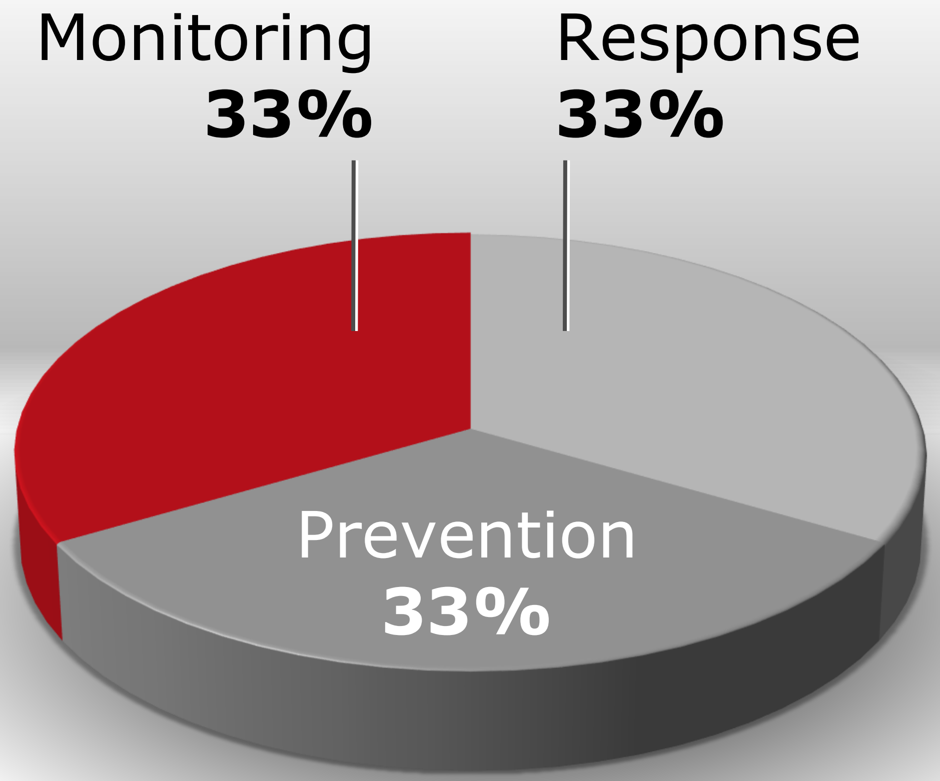
754096_C

Evolution of SOC : Traditional to Modern SOC Transformation

Shifting Priorities and Capabilities



Today’s Priorities



Intelligence-Driven Security

Battle for the Modern Security Operation Center

Today more than ever, security is not about buying the latest security novelties**; it is about building efficiencies into the processes that contribute to overall business priorities, without undermining key security prerequisites**. Currently, over half of all global businesses with 2,500 or more employees already have a security operations center (SOC) in one form or another, and 72% of those have built these capabilities within the last five years. **The most advanced organizations build their internal security operations centers so that they are integrated with overall IT governance and guided by strategic priorities on the horizon.** This change in approach is reflected in many layers:

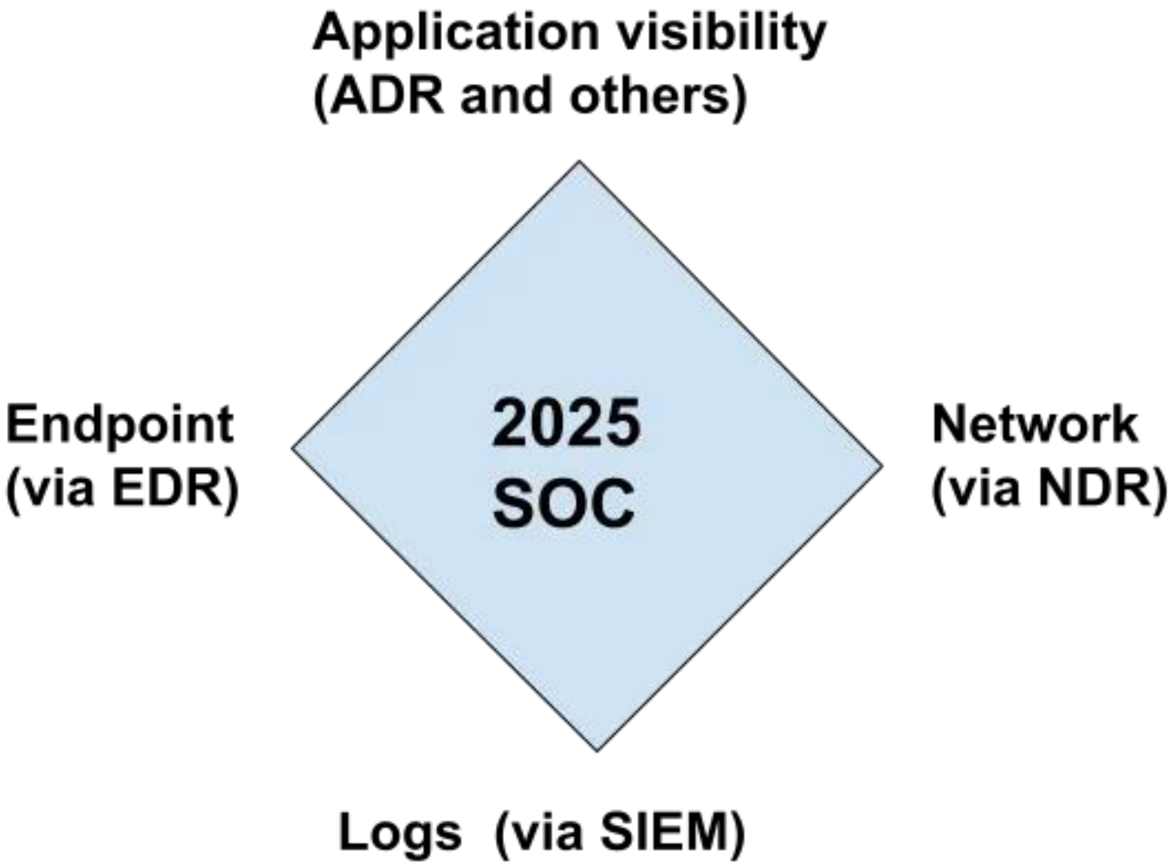
- **Cybersecurity automation intelligence response and orchestration technologies, which previously had an exclusive position at the core of the SOC**, now compete with other technologies and/or have become inclusive components of detection and response technologies and services.
- SOCs have become **collaborative projects, involving NetOps, SecOps, DevOps, and business contributors**.
- The expansion of organizational perimeters has led to floods of alerts and masses of noise, thus encouraging greater use of:
  - ➢ Functional outsourcing, whereby organizations rely on managed security services (MSS) from select service providers or security vendors (with 85% of companies currently outsourcing at least part of their SOCs to MSS providers and 32% fully outsourcing their SOCs)
  - ➢ Research and triage augmentation with threat intelligence (TI), either through paid feeds or by building a TI practice and plugging it into a specialized platform
  - ➢ Streamlining functions and SOC processes with automation and orchestration The modern SOC has evolved dramatically, as have requirements for its efficiency and effectiveness.

Source : IDC Spotlight SOC Whitepaper (https://media.kaspersky.com/en/business-security/IDC-Spotlight-SOC.pdf)

What Makes a Modern SOC

- Is it because of the Technology? **(NG-SIEM, AI/ML, SOAR, UEBA, EDR, NDR, CTI)**
- Is it because of the Service in SOC? **(Threat Intelligence Driven, Threat Hunting, Detection Engineering a.k.a Detection as a Code, Fraud Detection, Continuous Security Validation / Adversary Simulation)**
- Is it because of the Scope of Asset monitored in SOC? **(Cloud Environment, Big Data, IoT / OT)**
- Is it because of the people and roles in SOC? **(Threat Hunter, CTI Analyst, Detection / Content Engineer, Purple Team)**

SOC Quad Visibility



Application visibility
(ADR and others)

Endpoint
(via EDR)

2025
SOC

Network
(via NDR)

Logs (via SIEM)

Image Credit : https://medium.com/anton-on-security/soc-visibility-triad-is-now-a-quad-soc-visibility-quad-2025-72811401073a

What Makes a Modern SOC

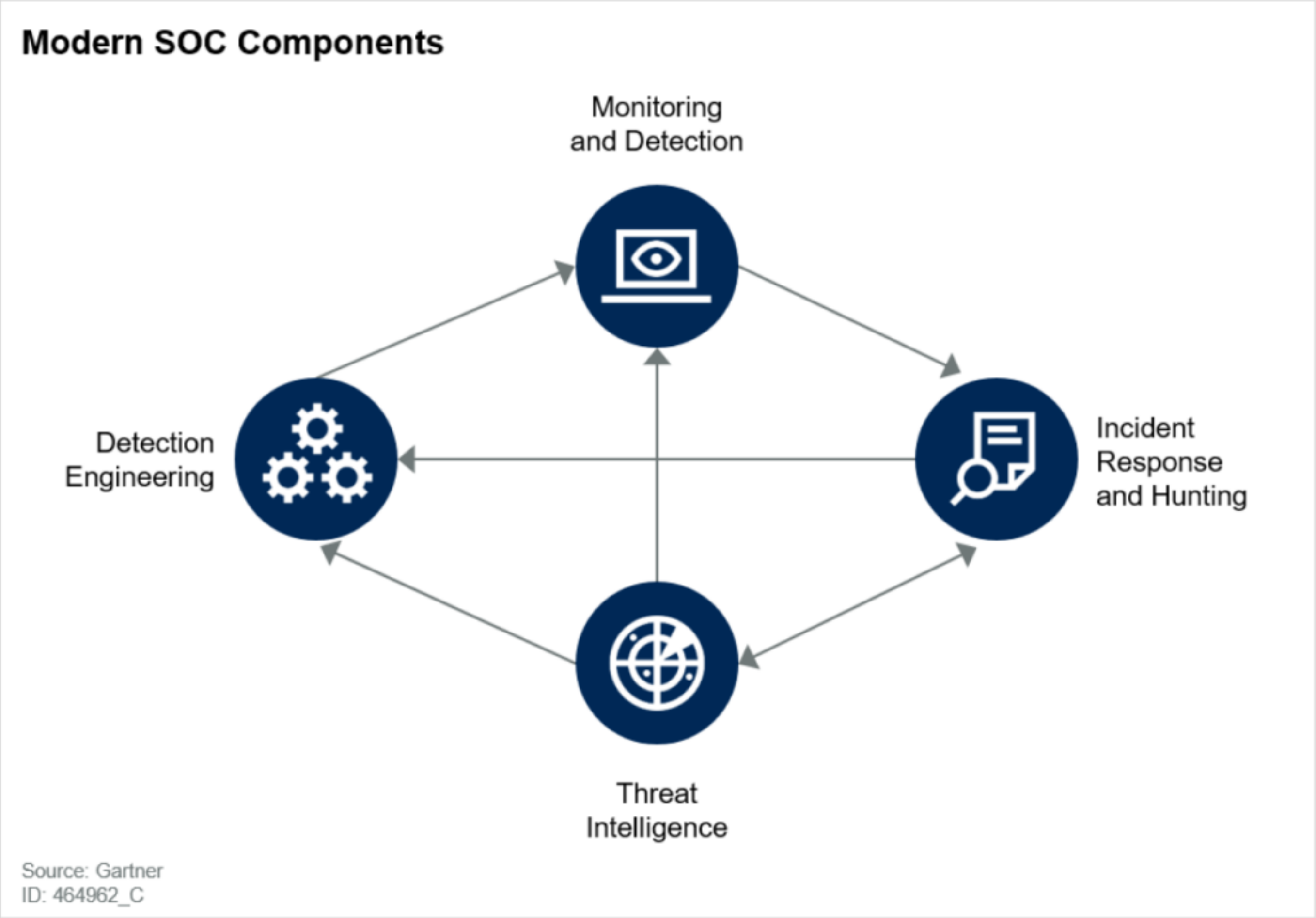
Bringing technology into the conversation, security orchestration, automation and response is a common tool used by modern SOCs, and it is key to providing mature SOC services. This is especially true for services such as incident response, which are very time dependent. Automation doesn't have to be complex. For example, simply automating how data is shared between tools so a SOC analyst doesn't have to log in to multiple tools can give valuable time back to the team.

Four areas are popular for automation:

- **Enrichment:** Improving data, eliminating manual pivots and automating workflows leading to verdicts.
- **Response:** Automating outcomes such as preventing access to a system or removing a file.
- **Threat hunting:** Taking different datapoints and using them to identify threats.
- **Threat Intelligence :** Empowers a modern SOC by providing the context and proactive insights needed to move beyond reactive incident response and anticipate, detect, and neutralize threats before they can cause harm.
- **Cyber hygiene.** Automating vulnerability management, posture and configurations

https://blogs.cisco.com/security/the-modern-security-operation-center

Modern SOC Components

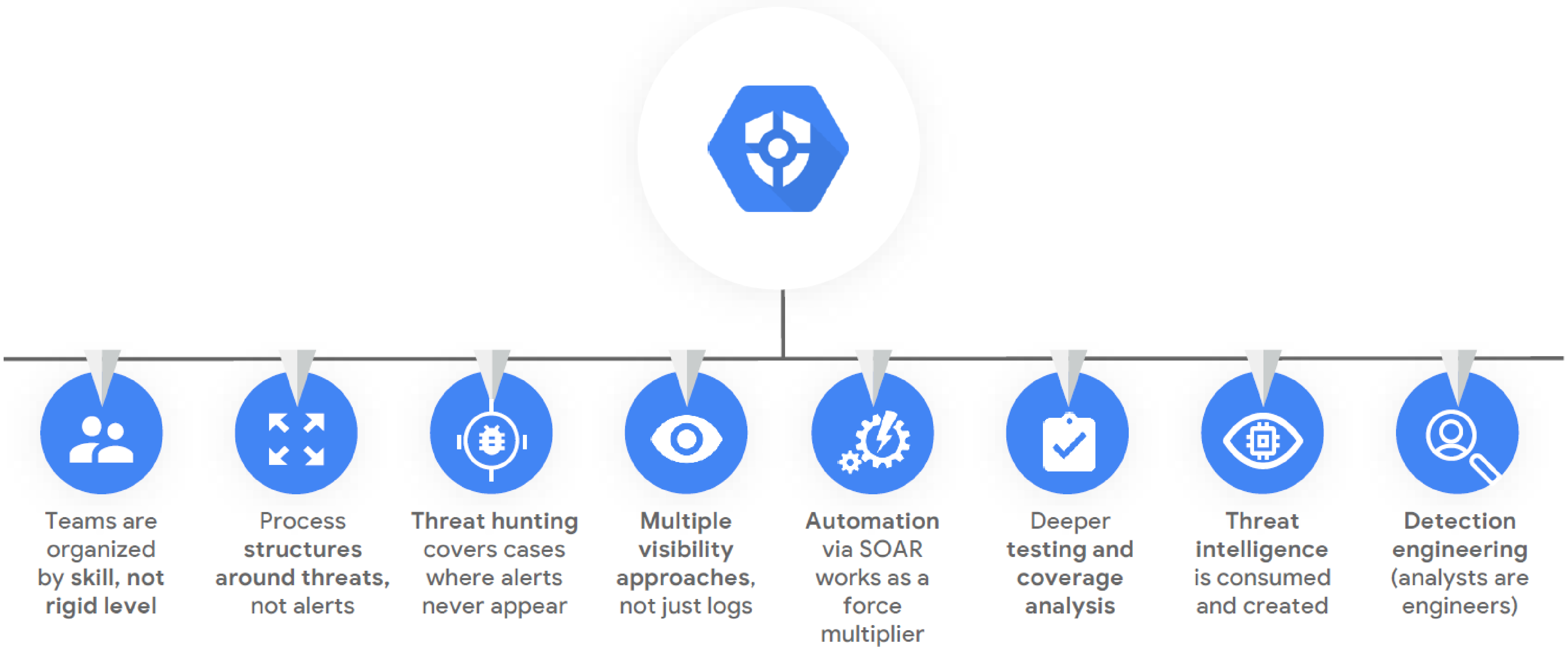


Modern SOC Components

Source: Gartner
ID: 464962_C

Source : Gartner

Highlights 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)

Anton Chuvakin : Can You Really 10x the SOC – SANS Blue Team Summit 2021
https://www.slideshare.net/anton_chuvakin/10x-soc-sans-blue-summit-keynote-2021-anton-chuvakin

Modern SOC Development Strategy

SOC Framework in a Nutshell

SOC Strategy & Governance

SOC Strategy
Program vision, objectives, approach, initiatives, roadmap

SOC Governance
SOC Organization, Reporting, Service Level Management, Policy Approvals, Recommendations, Escalation.

SOC Operations

SIEM Admin Operation
- Tool / Log Integration
- Reporting and Dashboards
- Rule & Administration
- Detection / Content Engineering

Threat Monitoring and Response
- Monitoring and Notification
- Validation and Triage
- Analysis and Escalation

Threat Hunting and Intelligence
- Internal Threat Intelligence (Assets/ Vulnerabilities/ Alerts
- External Threat Intelligence (Feeds, analysis, actionable)

SOC Technology

SIEM Technology
Log collection, processing and correlation
Data sources – structure, referential and unstructured

NBAD and Forensics
Network flow monitoring and anomaly detection
Full packet capture for forensics

Incident Management Tool
Ticketing, run book automation, incident response and collaboration and KPI monitoring

Integration
CMDB - Asset Modeling
VM – Vulnerability Mapping
Incident Mgt – Ticketing / Workflow
Threat Intelligence Feeds

Analytics
Big data – User Behavior Analytics And System Analytics
Historical log and network and application data correlation

Business Intelligence & Enrichment
Security Dashboard
Visualization – Integrated Security Posture
SIEM Tools Enrichment

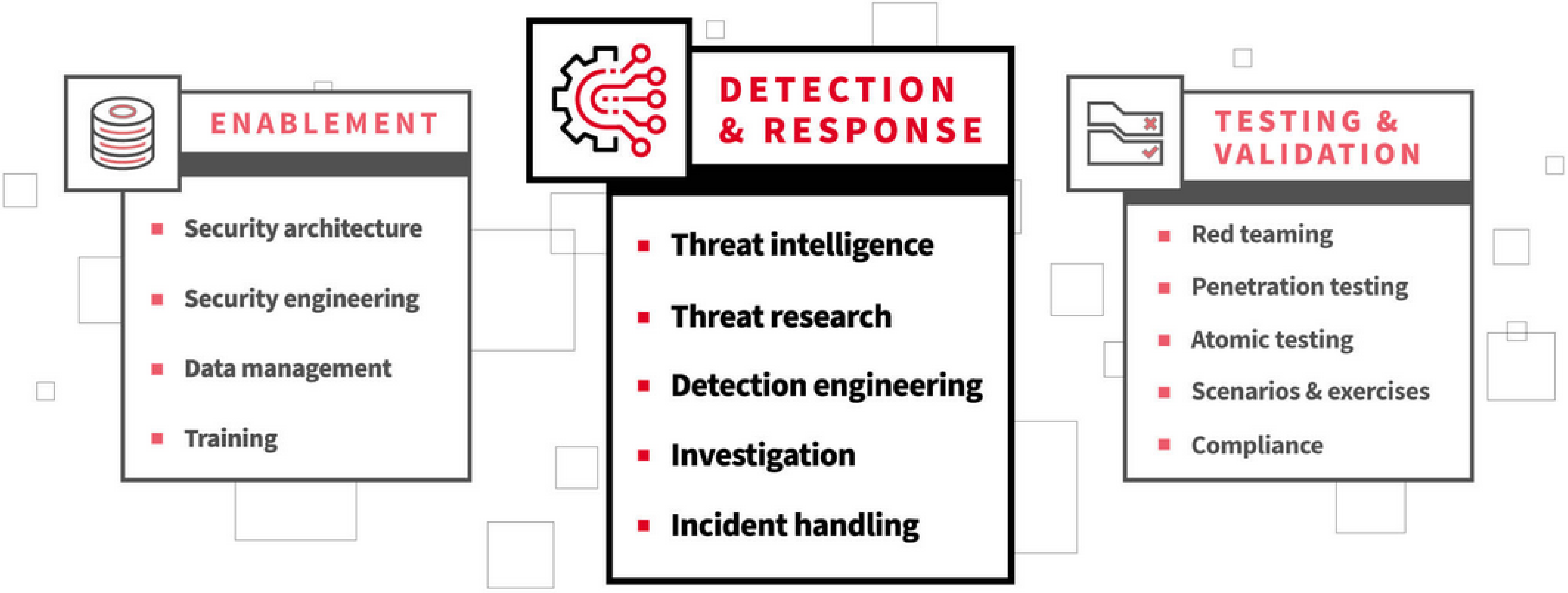
SOC Operation Function
- Active Threat Hunting
- Playbook / Run Book
- IOC Management
- Use Case Management
- Intelligence Analysis

SOC Business Function
- Requirement Analysis
- Risk Management
- Audit and Compliance Management
- Legal and Fraud Management

SOC Technology Function
- Architecture and Integration
- Development
- Server Management
- Application, User and Data monitoring

SOC - CSIRT
- Incident Response / Emergency Response
- Forensics

Development Step for Building Modern SOC



ENABLEMENT

- Security architecture
- Security engineering
- Data management
- Training

DETECTION & RESPONSE

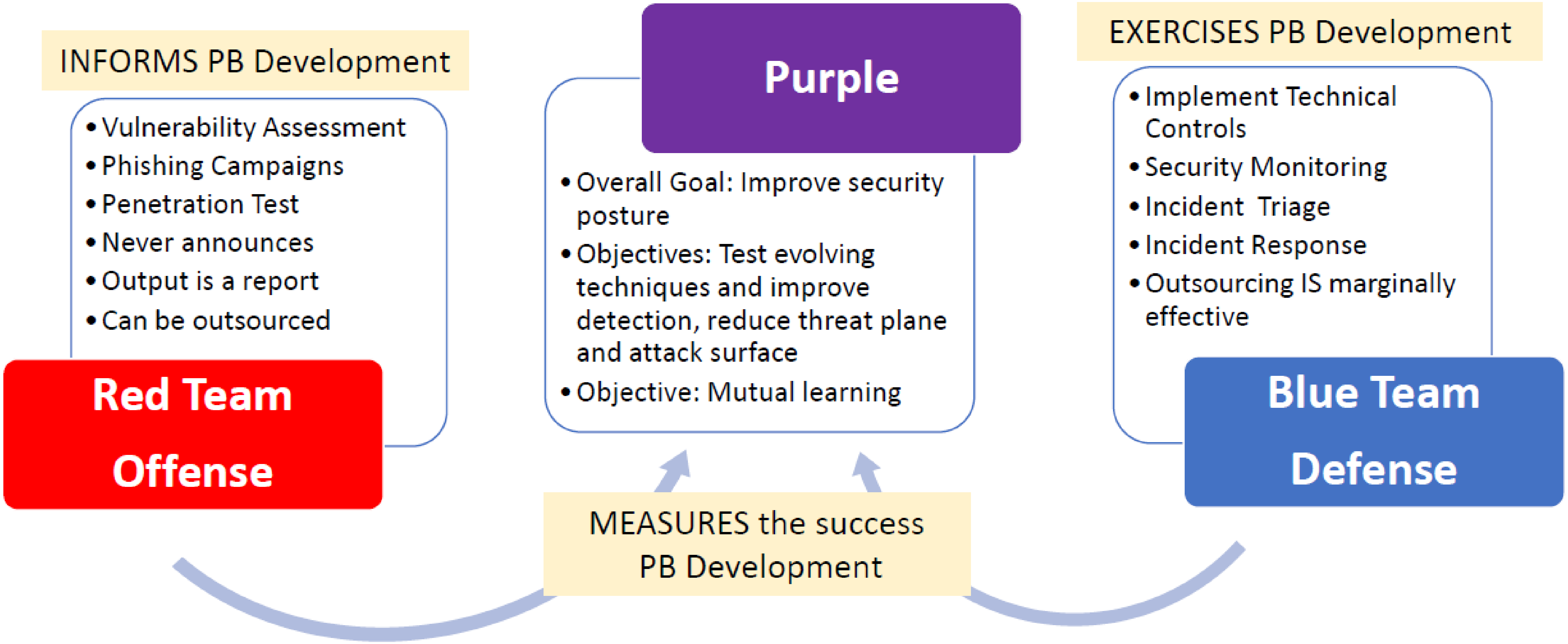
- Threat intelligence
- Threat research
- Detection engineering
- Investigation
- Incident handling

TESTING & VALIDATION

- Red teaming
- Penetration testing
- Atomic testing
- Scenarios & exercises
- Compliance

https://redcanary.com/blog/modern-security-operations-center/

Playbook Development in Modern SOC



INFORMS PB Development

- Vulnerability Assessment
- Phishing Campaigns
- Penetration Test
- Never announces
- Output is a report
- Can be outsourced

Red Team

Offense

Purple

- Overall Goal: Improve security posture
- Objectives: Test evolving techniques and improve detection, reduce threat plane and attack surface
- Objective: Mutual learning

EXERCISES PB Development

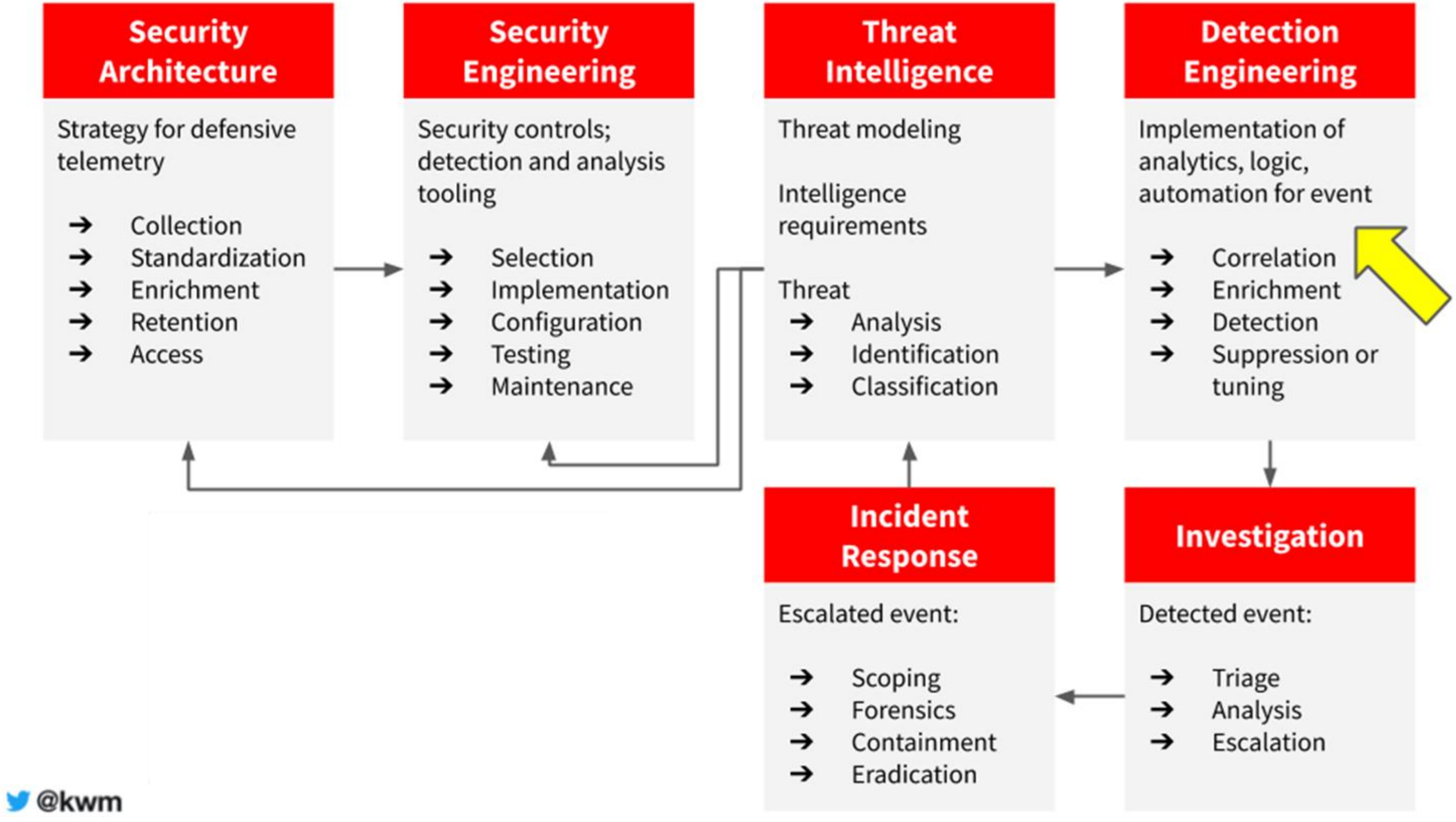
- Implement Technical Controls
- Security Monitoring
- Incident Triage
- Incident Response
- Outsourcing IS marginally effective

Blue Team

Defense

MEASURES the success PB Development

Modern Threat Analysis, Detection, and Response



Security Architecture

Strategy for defensive telemetry

- ➔ Collection
- ➔ Standardization
- ➔ Enrichment
- ➔ Retention
- ➔ Access

Security Engineering

Security controls; detection and analysis tooling

- ➔ Selection
- ➔ Implementation
- ➔ Configuration
- ➔ Testing
- ➔ Maintenance

Threat Intelligence

Threat modeling

Intelligence requirements

Threat

- ➔ Analysis
- ➔ Identification
- ➔ Classification

Detection Engineering

Implementation of analytics, logic, automation for event

- ➔ Correlation
- ➔ Enrichment
- ➔ Detection
- ➔ Suppression or tuning

Incident Response

Escalated event:

- ➔ Scoping
- ➔ Forensics
- ➔ Containment
- ➔ Eradication

Investigation

Detected event:

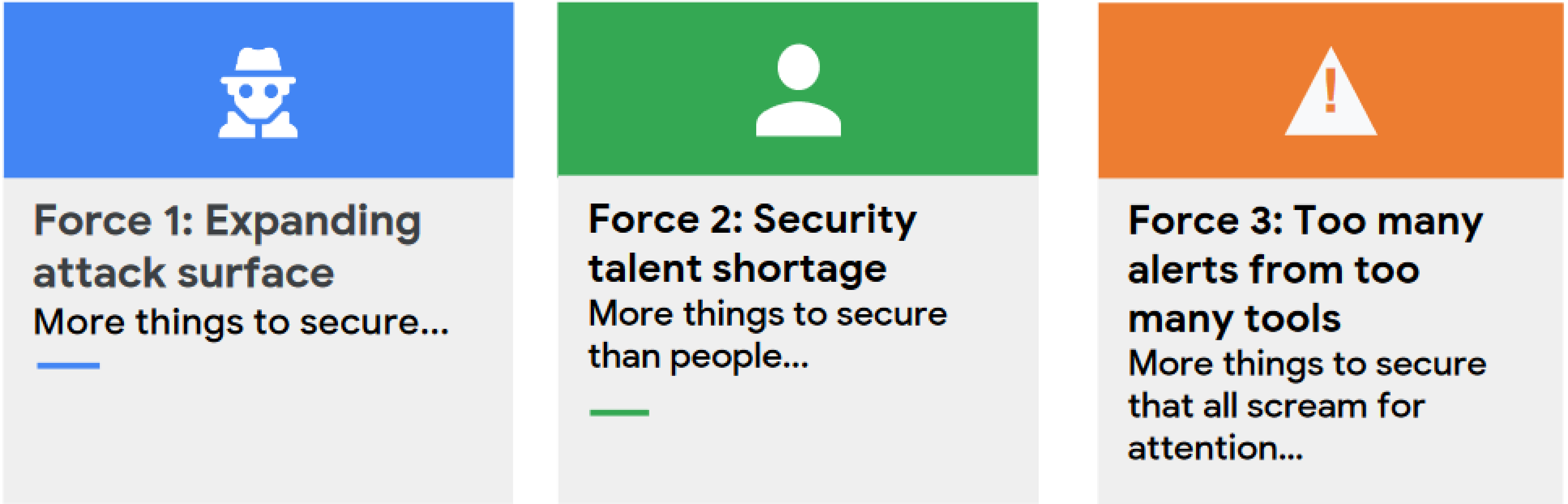
- ➔ Triage
- ➔ Analysis
- ➔ Escalation

@kwm

https://x.com/kwm/status/1260599938590797824

Challenges in SOC

SOC Challenges



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 :
* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-deloitte-google-cloud-alliance-future-of-the-SOC-whitepaper.pdf
* **Anton Chuvakin : Can You Really 10x the SOC – SANS Blue Team Summit 2021** https://www.slideshare.net/anton_chuvakin/10x-soc-sans-blue-summit-keynote-2021-anton-chuvakin

SOC is More Than Just Protection, Detection, and Response

- A Security Operations Center (SOC) is not only a defensive shield against cyber threats.
- It acts as a **strategic enabler** for organizations **undergoing digital transformation.**
- By providing a **strong security foundation**, the **SOC builds trust with customers, partners, and regulators**, making digital transformation sustainable.
- It provides the **confidence to adopt new technologies** such as cloud, AI, and automation **while minimizing risks.**

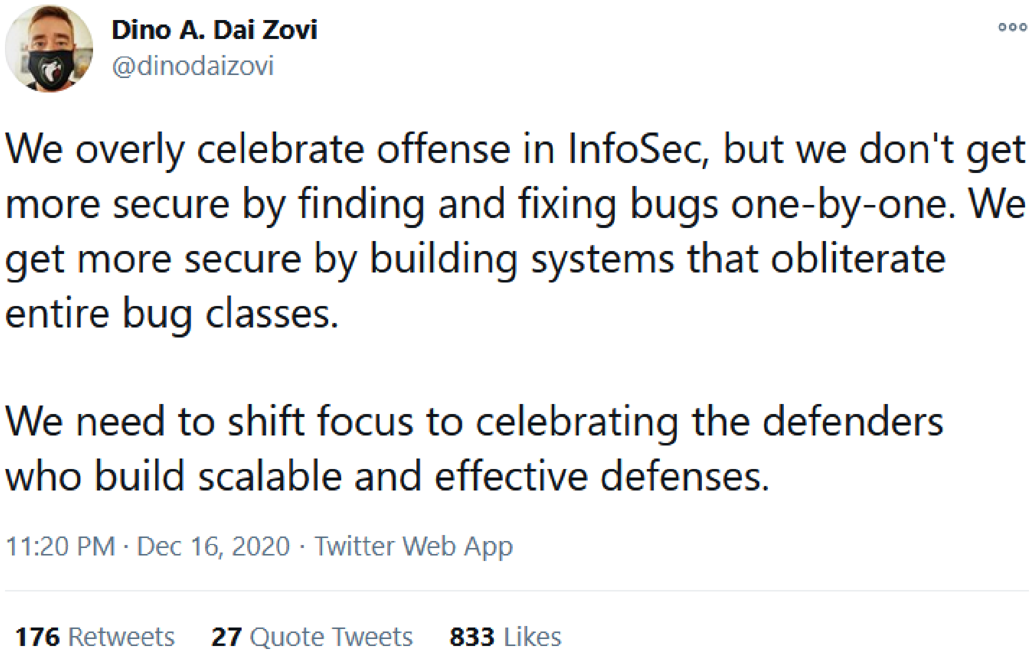
SOC for Driving Secure Digital Transformation

- **Cloud adoption**: SOC ensures secure migration and continuous monitoring of workloads.
- **IoT & Edge technologies**: Provides security oversight for devices that expand attack surfaces.
- **Remote and hybrid workforce**: Enables secure access management, monitoring, and threat detection across distributed environments.
- **Regulatory compliance**: Supports frameworks such **as UU PDP, BI / OJK Regulation, ISO 27001, PCI-DSS** and industry-specific requirements, ensuring that transformation aligns with legal and contractual obligations.
- **Data protection:** Safeguards intellectual property, sensitive customer data, and operational information critical to digital trust.
- **Reputation and trust:** Ensures that security incidents do not derail customer confidence, protecting long-term brand value.

Summary and Takeaways

- Modern SOC development needed by organization to combat latest cyber security threat and expanding attack surface in cybersecurity
- Visibility in modern SOC is important and should become priorities
- Designing adversary simulation / emulation for building better use case detection and evaluation your cyber defense capability
- Talent shortage is real and company need to build a program for hiring and develop the skillset and knowledge to filling the gaps between SOC teams

Thought



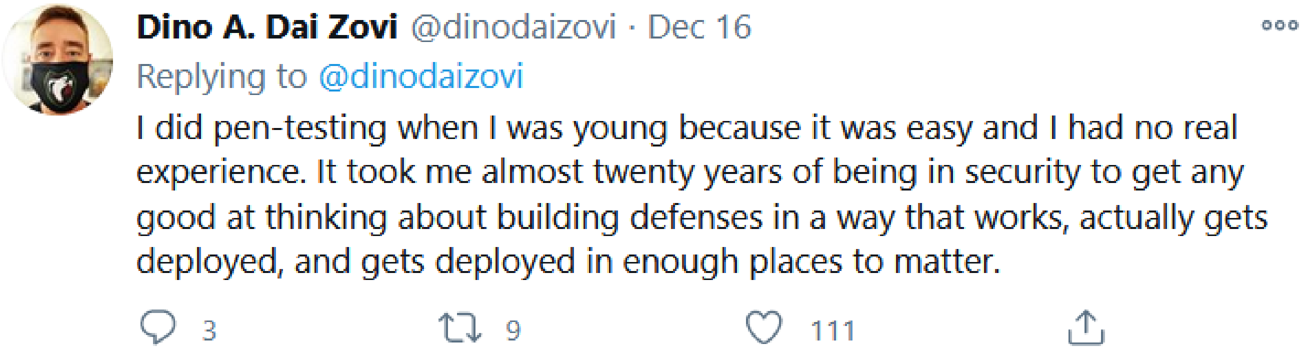
Dino A. Dai Zovi
@dinodaizovi

We overly celebrate offense in InfoSec, but we don't get more secure by finding and fixing bugs one-by-one. We get more secure by building systems that obliterate entire bug classes.

We need to shift focus to celebrating the defenders who build scalable and effective defenses.

11:20 PM · Dec 16, 2020 · Twitter Web App

176 Retweets **27** Quote Tweets **833** Likes



Dino A. Dai Zovi @dinodaizovi · Dec 16
Replying to @dinodaizovi

I did pen-testing when I was young because it was easy and I had no real experience. It took me almost twenty years of being in security to get any good at thinking about building defenses in a way that works, actually gets deployed, and gets deployed in enough places to matter.

3 9 ♡ 111

Further Reading References

- https://www.slideshare.net/anton_chuvakin/10x-soc-sans-blue-summit-keynote-2021-anton-chuvakin
- https://redcanary.com/blog/enabling-modern-security-operations-center/
- https://redcanary.com/blog/modern-security-operations-center/
- https://redcanary.com/blog/testing-validation-security-operations-center/
- https://www.slideshare.net/anton_chuvakin/10x-soc-sans-blue-summit-keynote-2021-anton-chuvakin

THANK YOU
Q & A