如何挑選“好”的資安產品

愈貴愈好

如何挑選“好”的資安產品

~~愈貴愈好~~

如何挑選“好”的資安產品

絕對不是愈貴愈好

Boik Su

chrO.ot's member

Programming lover 🤓

OWASP / ROOTCON / AVTokyo

qazbnm456

qazbnm456

Agenda

- 企業現況（大部分）
- 疲於奔命的 SIEM / SOC 小組
- 如何挑選“好”的資安產品

Agenda

- 企業現況（大部分）
- 疲於奔命的 SIEM / SOC 小組
- 如何挑選“好”的資安產品

企業現況（大部分）

- So many acronyms there in CSIRT. What organization you want to have in your company
    - CIRT, CSIRC, CIRC, CERT, IHT, IRC, IRT, SERT, SIRT …

企業現況（大部分）

- So many acronyms there in CSIRT. What organization you want to have in your company
    - CIRT, CSIRC, CIRC, CERT, IHT, IRC, IRT, SERT, SIRT …
- In fact, it’s not “what you want”, it should be “what are needed in order to fit” to the role your company plays

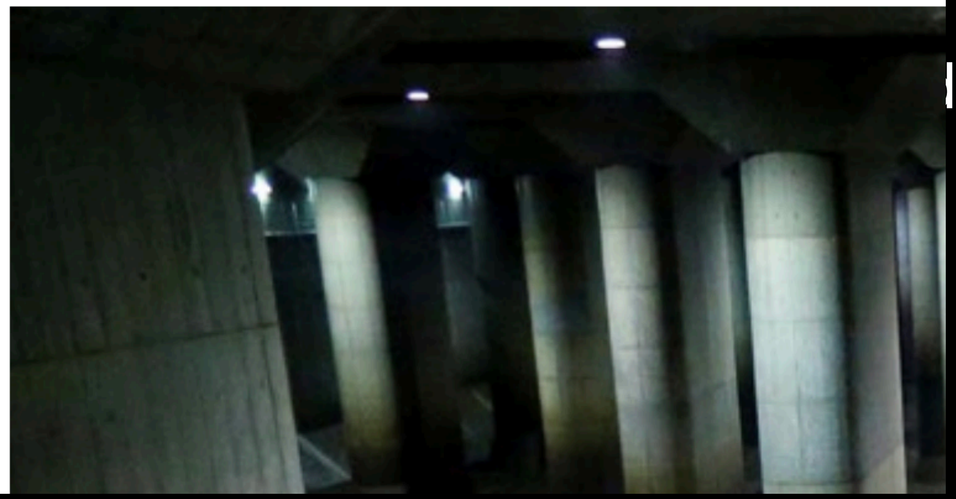
企業現況（大部分）

- So many acronyms there in CSIRT. What organization you want to have in your company
  -

East Asia and the Pacific

Top ten risks in East Asia and the Pacific

1. Natural catastrophes
2. Cyberattacks
3. Interstate conflict
4. Fiscal crises
5. Extreme weather events



- In fa ler to fit” t

企業現況（大部分）

- So many a … nt to have in your comp…
  - CIRT, …
- In fact, it's … d in order to fit" to the …

博通完成收購賽門鐵克企業安全業務！接收Symantec品牌　賣方更名續攻Norton防毒軟體

賽門鐵克（Symantec）昨（4）日宣布，博通公司以107億美元收購賽門鐵克企業安全業務已經完成。賽門鐵克也將品牌交給博通，並將公司名稱改為“Norton LifeLock Inc.”，立即生效。從明日（美國時間11月5日）開始，其普通股在納斯達克證券交易所將以「NLOK」代碼進行交易。

未來，賽門鐵克仍然保有消費性安全產品，包括身分防護服務LifeLock及諾頓（Norton）防毒軟體，也就是續攻一般消費者的防毒軟體市場。

博通是全球知名的晶片大廠，近年來開始擴向企業使用的雲端解決方案市場發展，透過收購方式取得企業安全防護軟體技術，比起自己建制團隊的成本來得更低。

企業現況（大部分）

- So many acronyms there in CSIRT. What organization you want to have in your company
    - CIRT, CSIRC, CIRC, CERT, IHT, IRC, IRT, SERT, SIRT …
- In fact, it’s not “what you want”, it should be “what are needed in order to fit” to the role your company plays
- Generally speaking, CSIRT, CIRT and CERT are relatively well-known among them

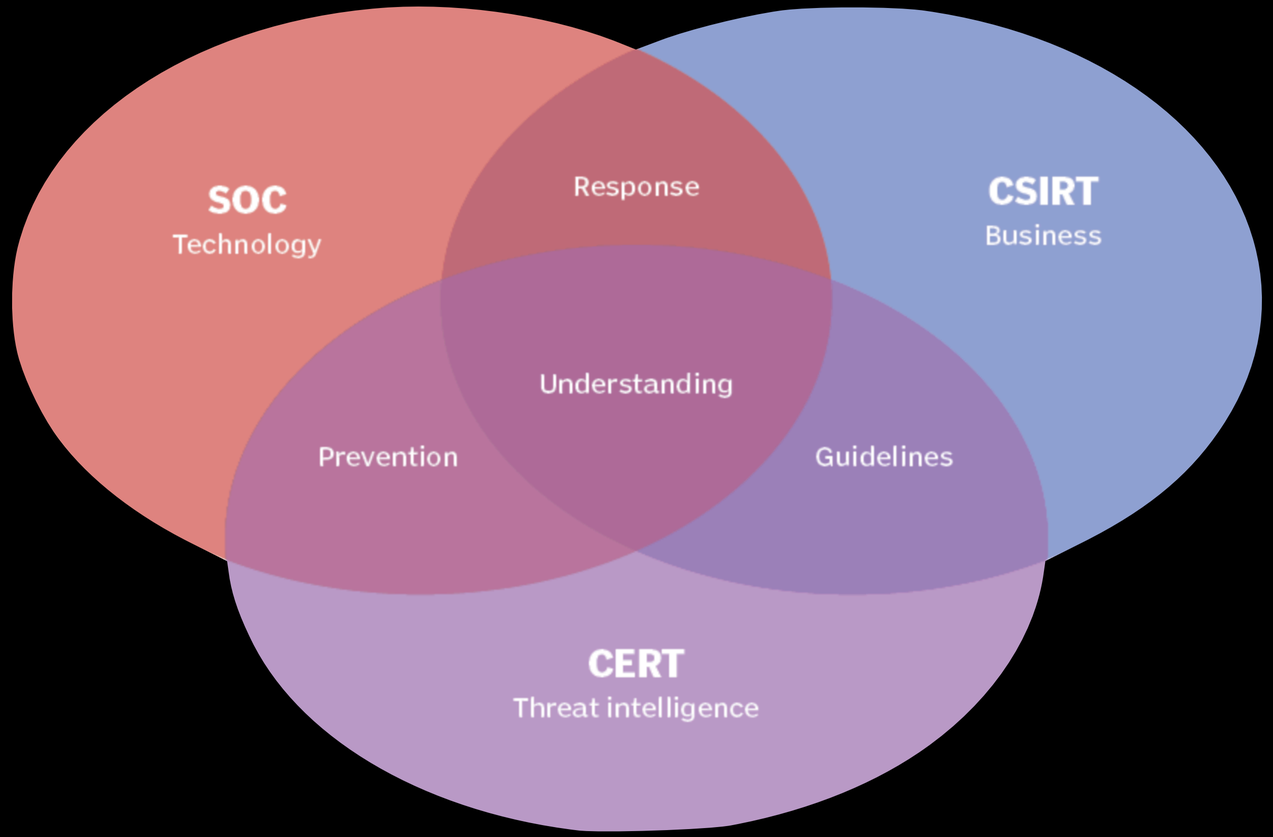
企業現況（大部分）

- So many acronyms there in CSIRT. What organization you want to have in your company
    - CIRT, CSIRC, CIRC, CERT, IHT, IRC, IRT, SERT, SIRT …
- In fact, it’s not “what you want”, it should be “what are needed in order to fit” to the role your company plays
- Generally speaking, CSIRT, CIRT and CERT are relatively well-known among them
- There’s another one called “PSIRT”, responsible for product security

- Besides, there is also another term, SOC, that you might hear of

- Besides, there is also another term, SOC, that you might hear of
- Which handles all things related to Information Security apart from IR

- Besides, there is also another term, SOC, that you might hear of
- Which handles all things related to Information Security apart from IR



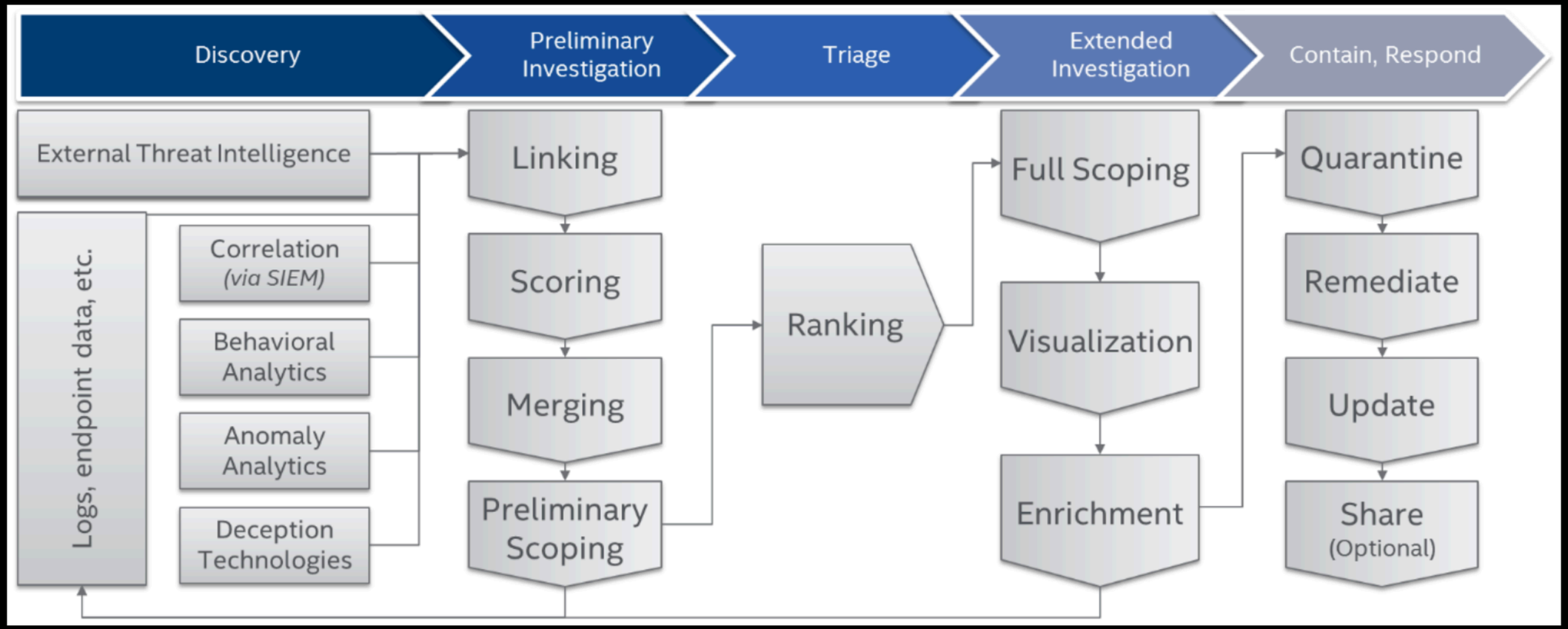
We have a security team

and then …?

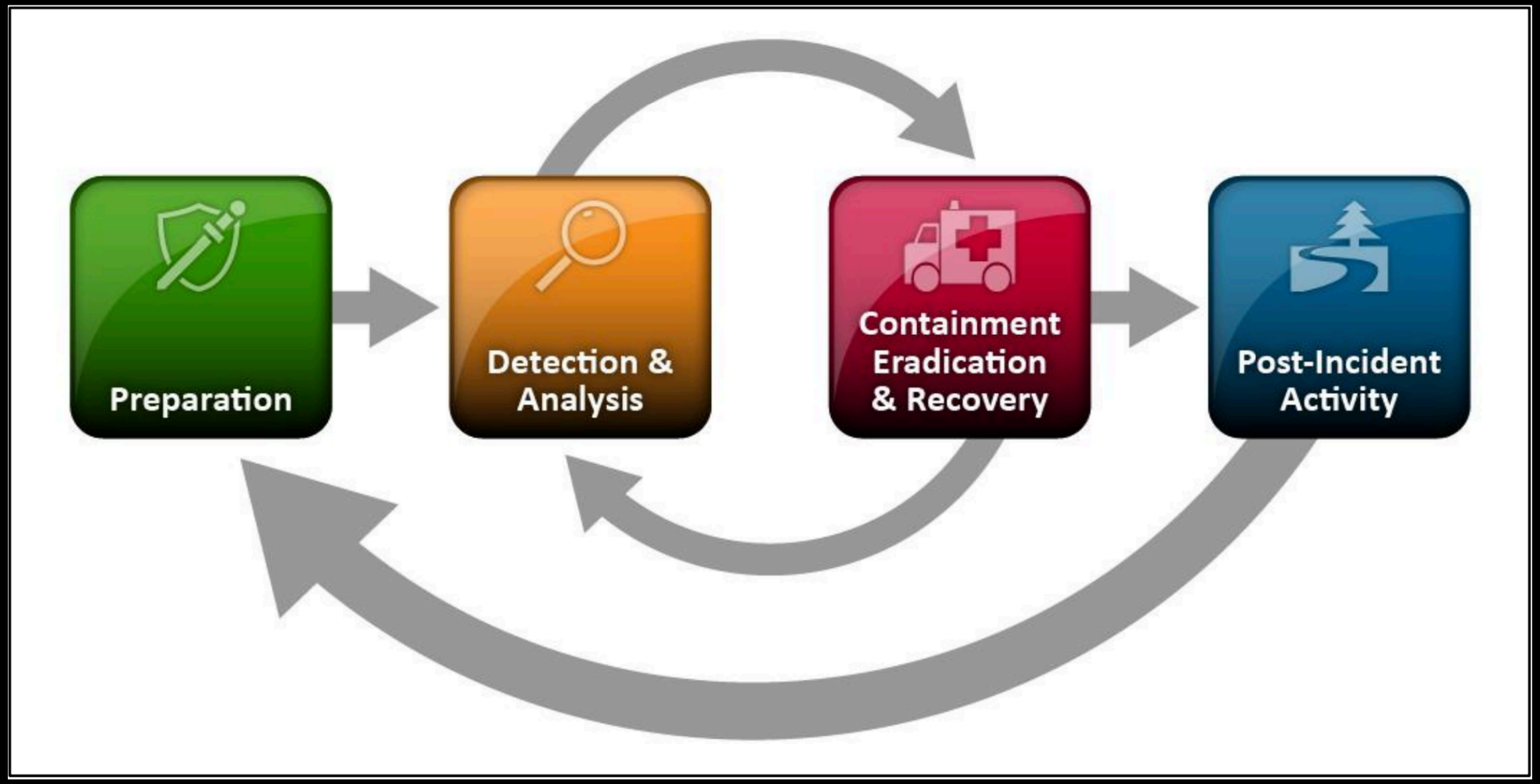
Critical Function

- Help enact security policies
- Set up security monitoring tools to receive raw security-relevant data
- Leverage logs to find suspicious or malicious activities by
    - Analyze alerts / warnings
    - Investigate IOCs, e.g., file hashes, certain patterns, etc
    - Review and Rectify detection / correlation rules
- Share findings and experiences with threat intelligence community

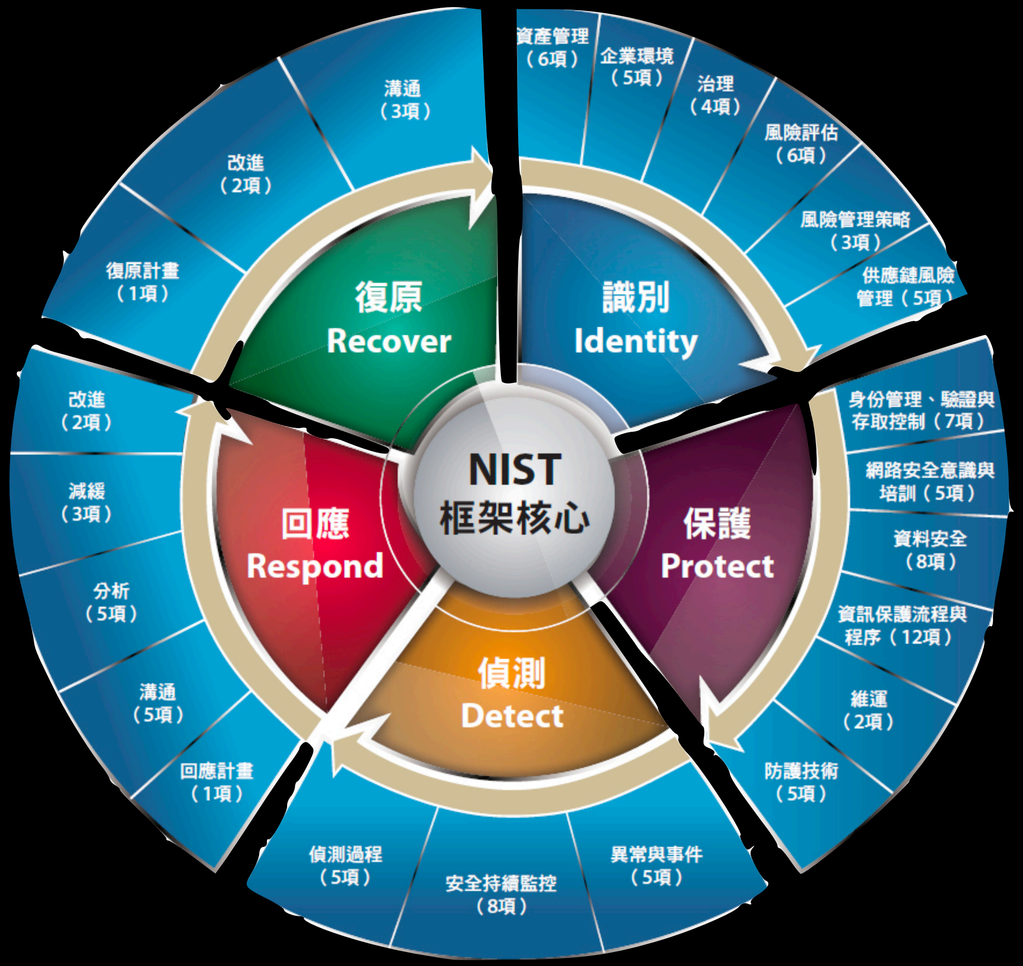
Critical Function



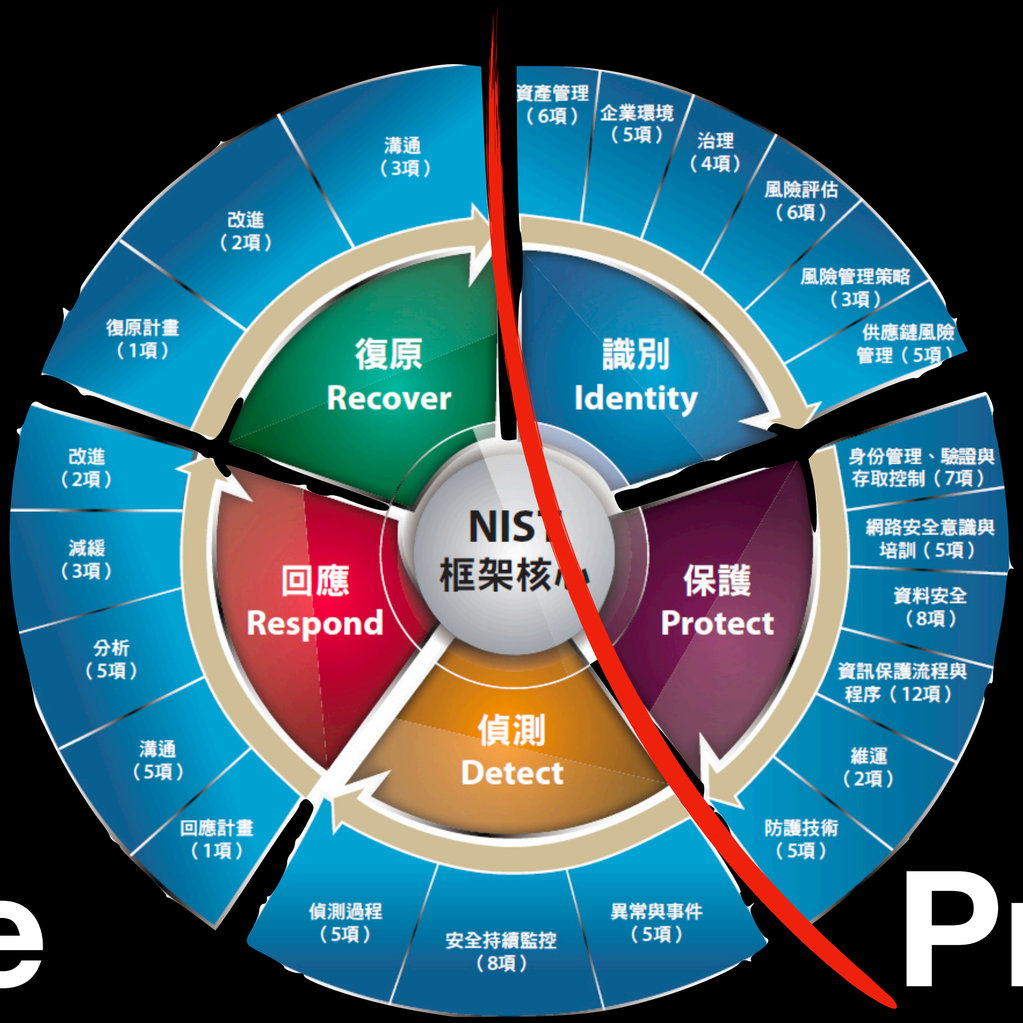
COMPUTER SECURITY INCIDENT HANDLING



NIST Cybersecurity Framework



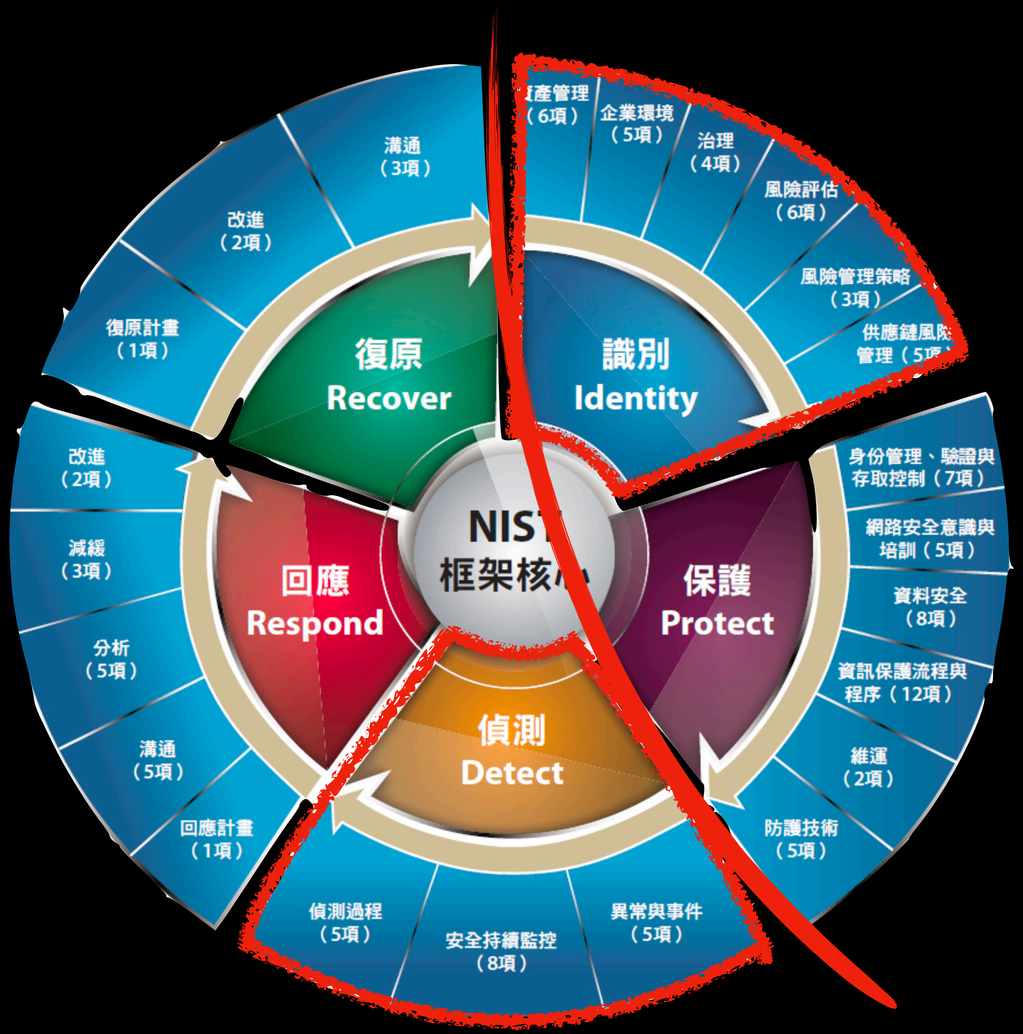
NIST Cybersecurity Framework



Incident Response

Preparation

NIST Cybersecurity Framework



辨識
Identity

- 資產管理
- 營運環境
- 治理
- 風險評估
- 風險管理策略
- 供應鏈風險管

偵測
Detect

- 異常偵測及事件管理
- 持續性安全監控
- 偵測流程

Asset Management

We do our “best” to identify all stuff and categorize them as

Asset Management

We do our “best” to identify all stuff and categorize them as

1. System: What systems do we have

Asset Management

We do our “best” to identify all stuff and categorize them as

1. System: What systems do we have
2. Personnel: How many employees in total

Asset Management

We do our “best” to identify all stuff and categorize them as

1. System: What systems do we have
2. Personnel: How many employees in total
3. Device: How many devices do we own

Asset Management

We do our “best” to identify all stuff and categorize them as

1. System: What systems do we have
2. Personnel: How many employees in total
3. Device: How many devices do we own
4. Data: What data do we have

Asset Management

We do our “best” to identify all stuff and categorize them as

1. System: What systems do we have
2. Personnel: How many employees in total
3. Device: How many devices do we own
4. Data: What data do we have
5. Capability: What capabilities do we have

資產盤點 & 風險評估

Log

We know logs are important, so we collect logs from

Log

We know logs are important, so we collect logs from

1. So many security devices that we've installed, e.g., firewalls, IPSs, etc

Log

We know logs are important, so we collect logs from

1. So many security devices that we've installed, e.g., firewalls, IPSs, etc
2. Host-based information, e.g., Windows EVT, AntiVirus, EDR, etc

Log

We know logs are important, so we collect logs from

1. So many security devices that we've installed, e.g., firewalls, IPSs, etc
2. Host-based information, e.g., Windows EVT, AntiVirus, EDR, etc
3. Web servers' logs

Log

We know logs are important, so we collect logs from

1. So many security devices that we've installed, e.g., firewalls, IPSs, etc
2. Host-based information, e.g., Windows EVT, AntiVirus, EDR, etc
3. Web servers' logs
4. Printers / Collaboration tools

Log

We know logs are important, so we collect logs from

1. So many security devices that we've installed, e.g., firewalls, IPSs, etc
2. Host-based information, e.g., Windows EVT, AntiVirus, EDR, etc
3. Web servers' logs
4. Printers / Collaboration tools
5. Others

主動偵測 & 資訊備查

SIEM

- Combine the functions of security information management (SIM) and security event management (SEM)
- A SIEM system has many capabilities and features. In many cases, these features add as much value to startups or SMBs as they do for big companies
    - Log management
    - Event correlation
    - Threat detection

Agenda

- 企業現況（大部分）
- 疲於奔命的 SIEM / SOC 小組
- 如何挑選“好”的資安產品

疲於奔命的 SIEM / SOC 小組

- We have various and robust logs from different sources, though

疲於奔命的 SIEM / SOC 小組

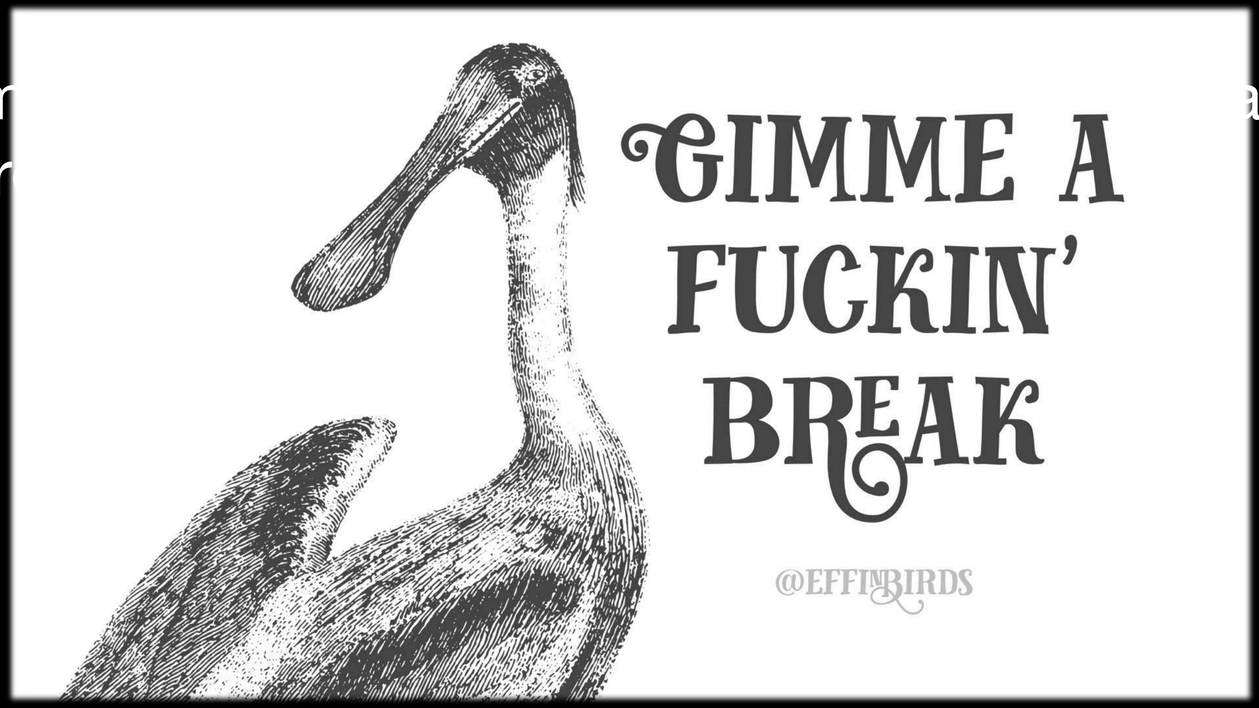
- We have various and robust logs from different sources, though
- SIEM / SOC teams can be inundated with security alerts on a regular basis

疲於奔命的 SIEM / SOC 小組

- We have various and robust logs from different sources, though
- SIEM / SOC teams can be inundated with security alerts on a regular basis
    - The volume of alerts generated is so huge, that available security admins are overwhelmed

疲於奔命的 SIEM / SOC 小組

- We have various and robust logs from different sources, though
- SIEM / SOC teams can be inundated with security alerts on a regular basis
  - The volum able security admins ar



疲於奔命的 SIEM / SOC 小組

- We have various and robust logs from different sources, though
- SIEM / SOC teams can be inundated with security alerts on a regular basis
    - The volume of alerts generated is so huge, that available security admins are overwhelmed
- This results all too often in situations where many alerts can't be investigated

疲於奔命的 SIEM / SOC 小組

- We have various and robust logs from different sources, though
- SIEM / SOC teams can be inundated with security alerts on a regular basis
    - The volume of alerts generated is so huge, that available security admins are overwhelmed
- This results all too often in situations where many alerts can't be investigated
    - Leaving the organization vulnerable to attacks that go unnoticed

疲於奔命的 SIEM / SOC 小組

- We have various an ces, though
- SIEM / SOC teams erts on a regular basis
  - The volume of available security admins are ove
- This results all too c erts can't be investigated
  - Leaving the org hat go unnoticed

疲於奔命的 SIEM / SOC 小組

- When a security incident happened …

疲於奔命的 SIEM / SOC 小組

- When a security incident happened …
- The manager rushed into the War Room and yelled
    - “How did this happen? Were there something being stolen?”

疲於奔命的 SIEM / SOC 小組

- When a security incident happened …
- The manager rushed into the War Room and yelled
  - “How did this happen? Were there something being stolen?”
  - “We’ve deployed all kinds of security devices to every corner. Why did it still happen?”

疲於奔命的 SIEM / SOC 小組

- When a securit
- The manager ru
  - “How did t stolen?”
  - “We’ve de y corner. Why did it still h

疲於奔命的 SIEM / SOC 小組

- When a security incident happened …
- The manager rushed into the War Room and yelled
    - “How did this happen? Were there something being stolen?”
    - “We’ve deployed all kinds of security devices to every corner. Why did it still happen?”
- People in the War Room are have no idea about the culprit, so every one just try to stop the threat immediately by pulling off the cable and killing those bad things

疲於奔命的 SIEM / SOC 小組

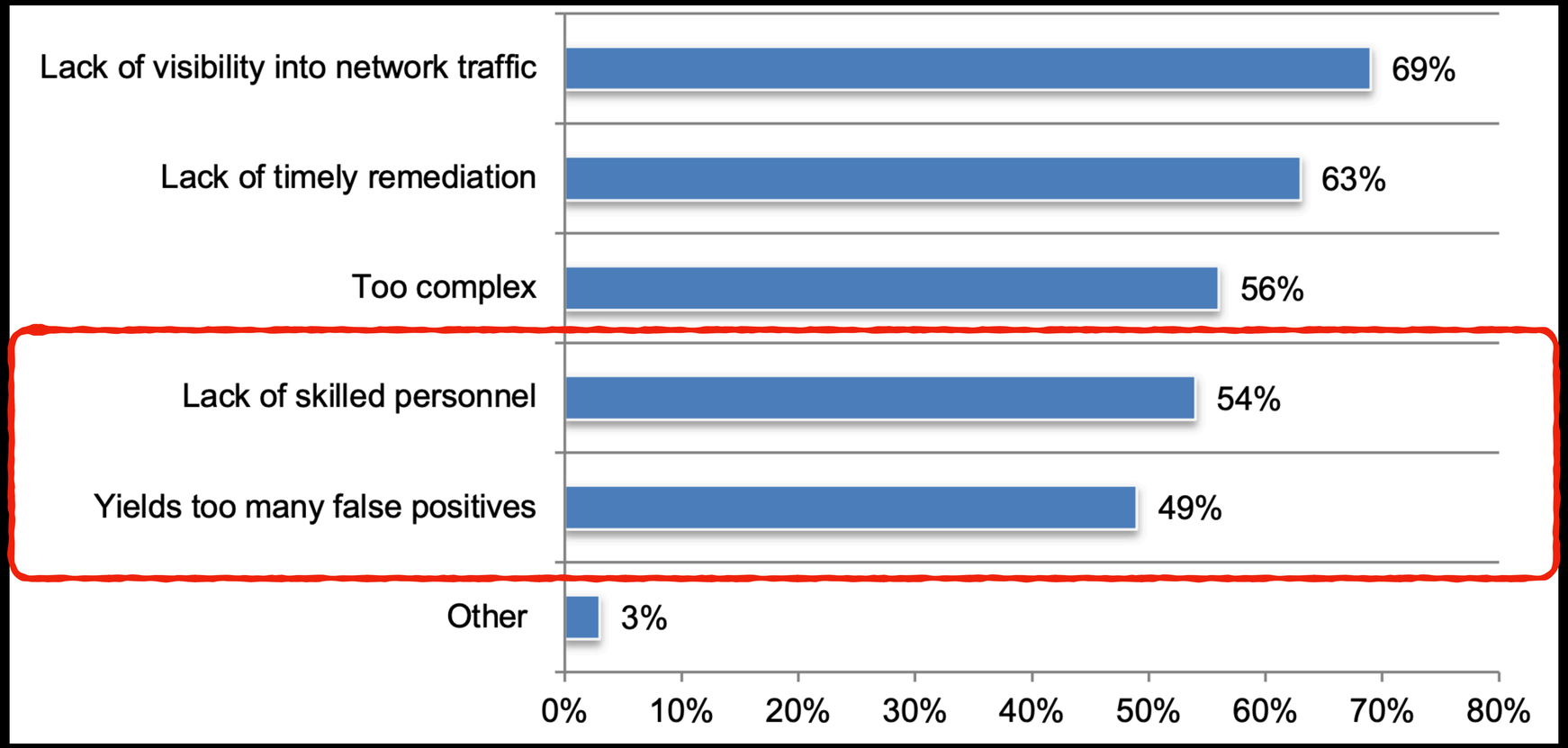
- When a security inc
- The manager rushe
  - “How did this h eing stolen?”
  - “We’ve deploy every corner. Why did it still happ
- People in the War R culprit, so every one just try to stop the t he cable and killing those bad things

企業正面對如何因應威脅的難題

SOC 成效不彰、工作痛苦

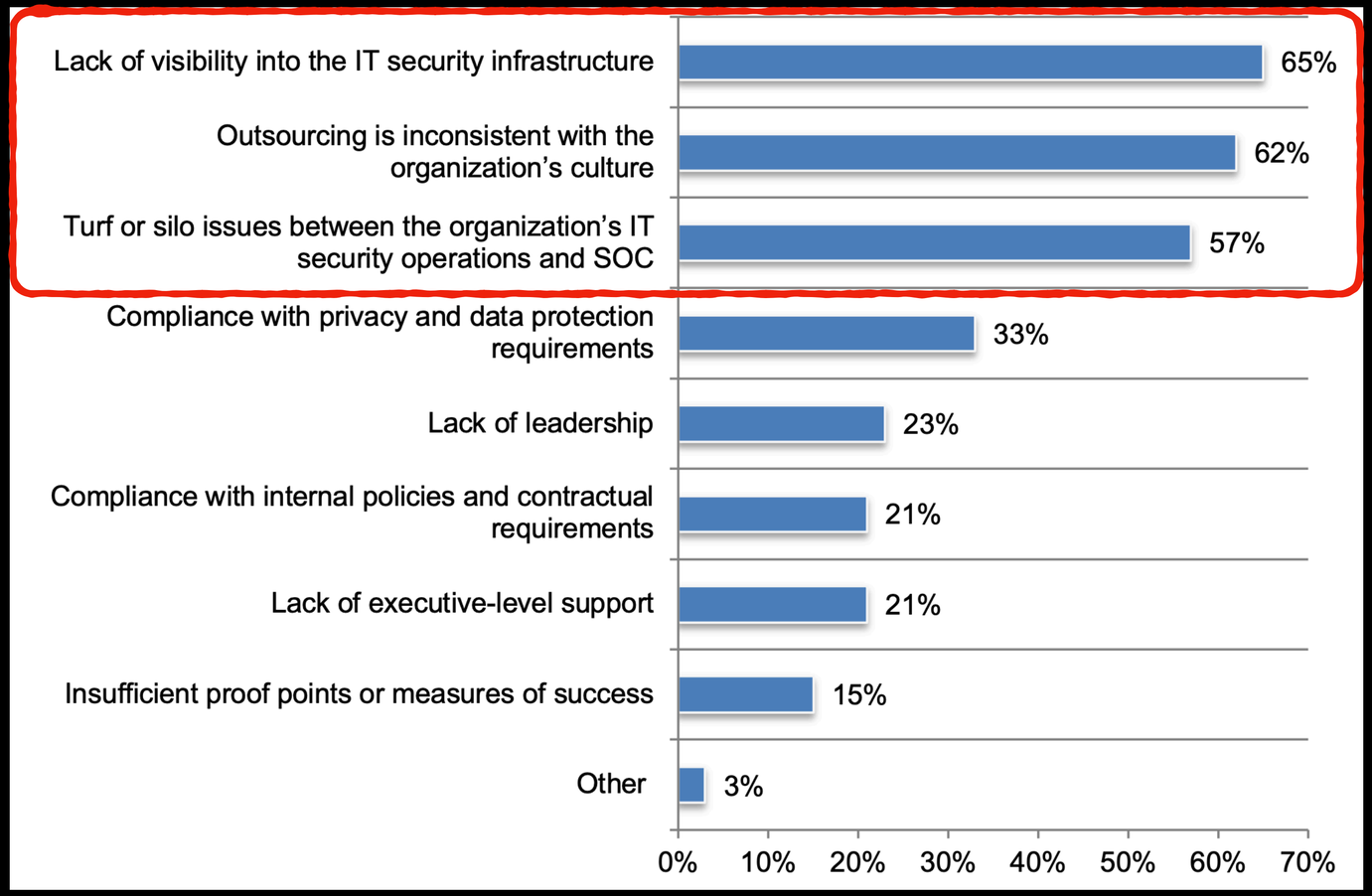
SOC 成效不彰

- What makes the SOC ineffective? (人的問題)



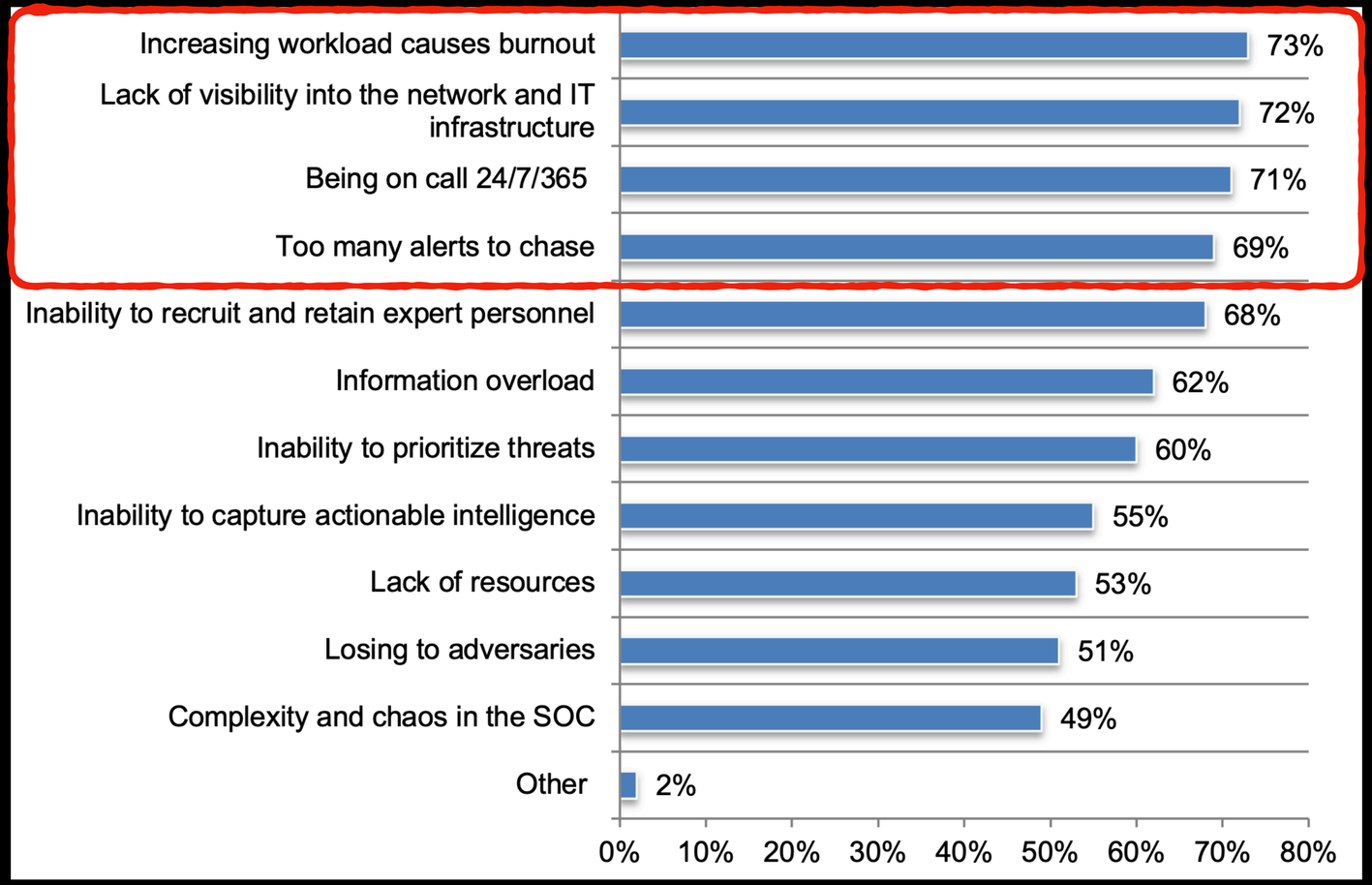
SOC 成效不彰

- Why operating a successful SOC is that hard? (大環境的問題)



SOC 工作痛苦

- What makes working in the SOC painful? （物的問題）



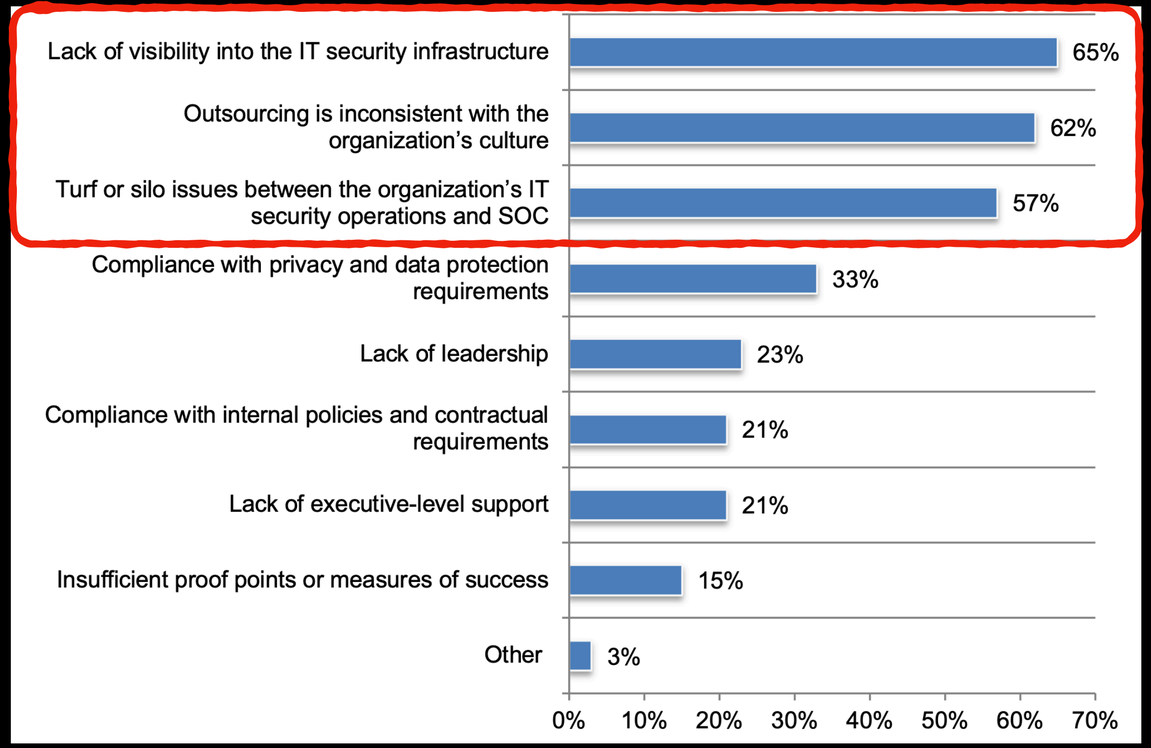
Agenda

- 企業現況（大部分）
- 疲於奔命的 SIEM / SOC 小組
- 如何挑選“好”的資安產品

應以人為出發點

SOC 成效不彰

- Why operating a successful SOC is that hard?
  - Lack of visibility into the IT security infrastructure
  - Outsourcing is inconsistent with the organization’s culture
  - Turf or silo issues between the organization’s IT security operations and SOC

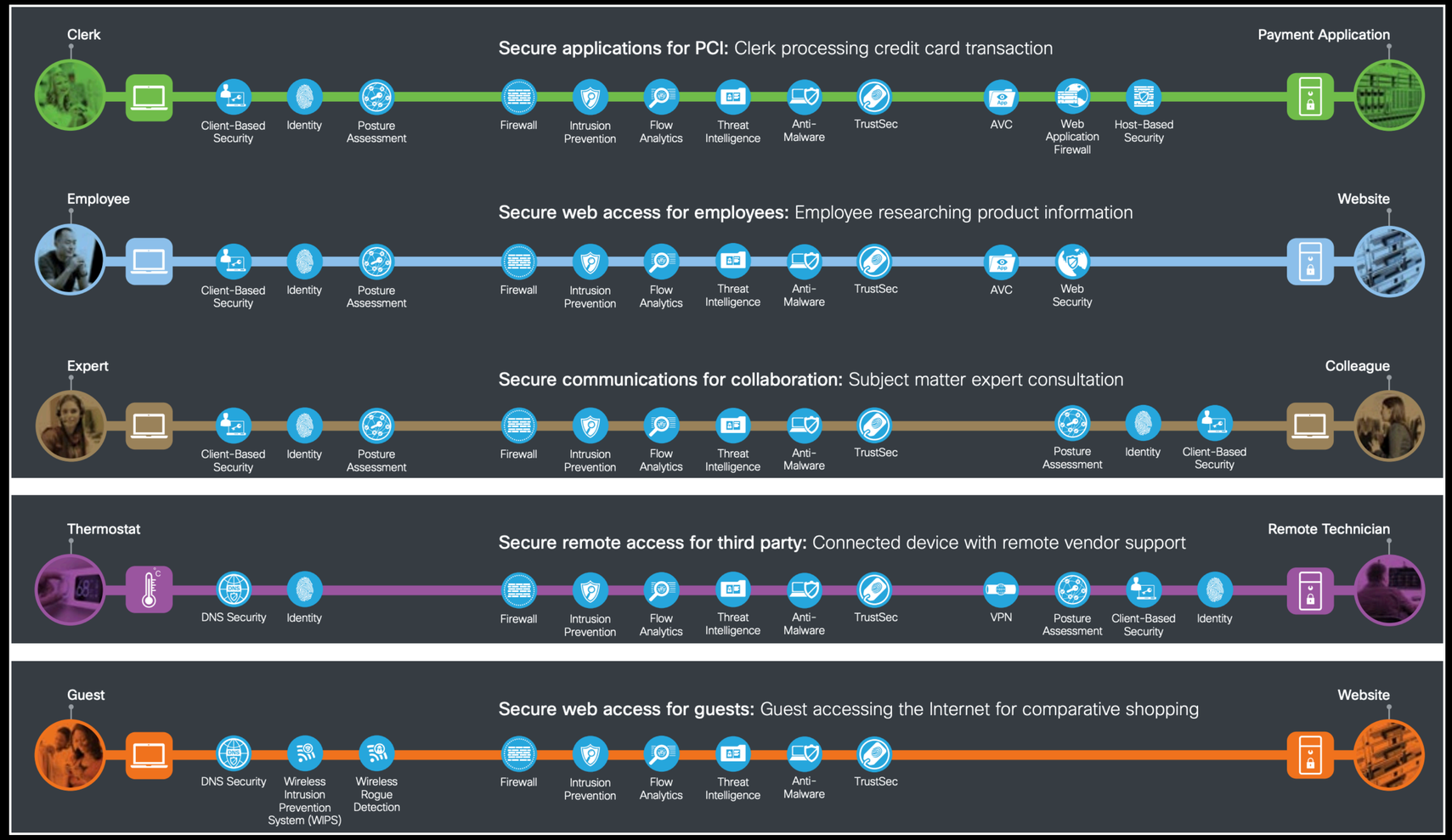


SOC 成效不彰

- Why operating a successful SOC is that hard?
  - Design and discuss with IT department and get involved
  - Think twice before deploying
  - Make a balance between IT & Security

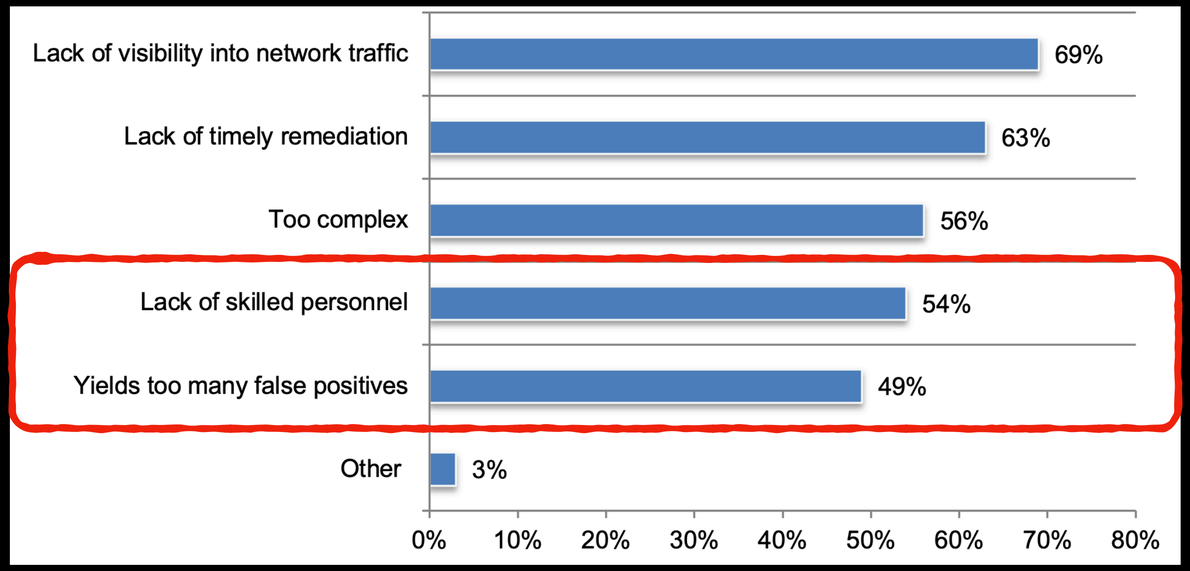
SOC 成效不彰

Know the business flows to simplify the identification of threats



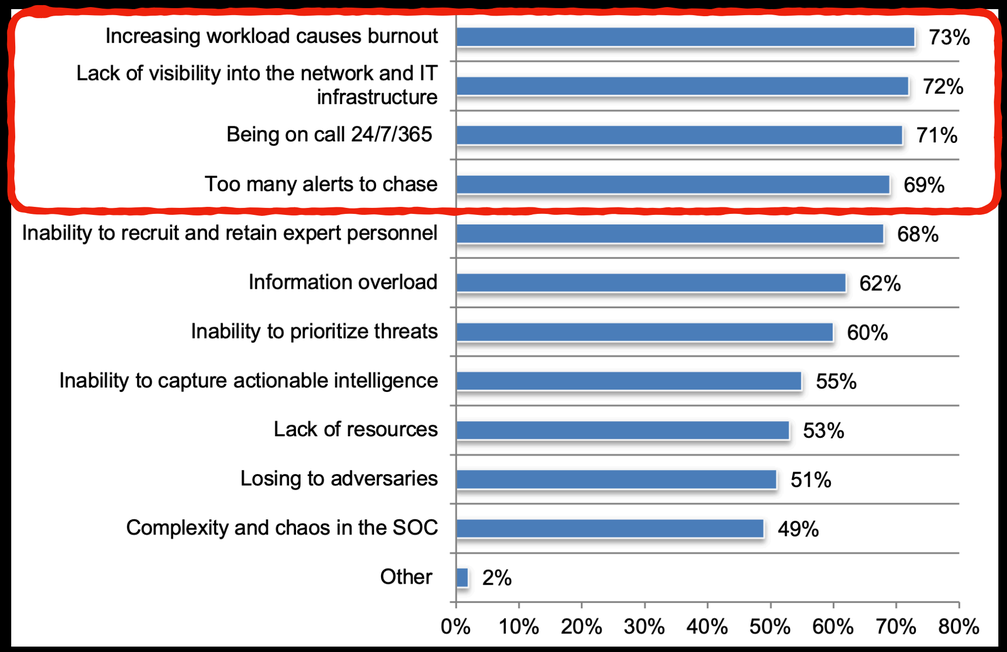
SOC 工作痛苦

- What makes SOC ineffective and working in it painful?
  - Lack of skilled personnel
  - Yield too many false positives



SOC 工作痛苦

- What makes SOC ineffective and working in it painful?
  - Lack of skilled personnel
  - Yield too many false positives
  - Lack of visibility into the network and IT infrastructure
  - Increasing workload causes burnout
  - Too many alerts to chase



SOC 工作痛苦

- What makes SOC ineffective and working in it painful?
  - Lack of skilled personnel
  - Yield too many false positives
  - Lack of visibility into the network and IT infrastructure
  - Increasing workload causes burnout
  - Too many alerts to chase

SOC 工作痛苦

- What makes SOC ineffective and working in it painful?
    - Lack of professionals that can lead and prioritize alerts / threats
    - Lack of proactive threat hunting that can correlate events and reduce false positives

SOC 工作痛苦

- What makes SOC ineffective and working in it painful?
    - Lack of professionals that can lead and prioritize alerts / threats
    - Lack of proactive threat hunting that can correlate events and reduce false positives
- Let human do humane things
- Let machines do the routine jobs
- Let’s play a win-win game between human beings and machines

SOC 工作不痛苦

- What makes SOC not ineffective and working in it not painful?
  - Not lack of professionals that can lead and prioritize alerts / threats
  - Not lack of proactive threat hunting that can correlate events and reduce false positives

SOC 工作不痛苦

- What makes SOC not ineffective and working in it not painful?
  - Not lack of professionals that can lead and prioritize alerts / threats
    - Recruit professionals and treat them well, or train the members
  - Not lack of proactive threat hunting that can correlate events and reduce false positives

Recruit professionals / Train the members

- Skilled personnel are also valuable properties
- A Tier 2 Analyst often requires such professional skill set
    - Review trouble tickets
    - Leverage asset management and threat intelligence to identify affected systems and the scope of the attack
    - Determine and direct remediation and recovery efforts

SOC 工作不痛苦

- What makes SOC not ineffective and working in it not painful?
  - Not lack of professionals that can lead and prioritize alerts / threats
    - Recruit professionals and treat them well, or train the members
    - Hold internal / cross-department technical meeting
  - Not lack of proactive threat hunting that can correlate events and reduce false positives

Internal / cross-department technical meeting

- Share sharp techniques or findings
- Give advises on approaches or methodology
- Know better on others work

SOC 工作不痛苦

- What makes SOC not ineffective and working in it not painful?
  - Not lack of professionals that can lead and prioritize alerts / threats
    - Recruit professionals and treat them well, or train the members
    - Hold internal / cross-department technical meeting
  - Not lack of proactive threat hunting that can correlate events and reduce false positives
    - Participate and engage in the Threat Intelligence community

Engage in the Threat Intelligence community

- FIRST - Forum of Incident Response and Security Teams
- APCERT - Asia Pacific Computer Emergency Response Team
- G-ISAC - Government Information Sharing and Analysis Center

Engage in the Threat Intelligence community

- Squid’s static buffer overflow
- Google Chrome: CVE-2019-13720 & CVE-2019-13721
- BlueKeep: CVE-2019-0708
- Emotet & MegaCortex
- GlobeImposter

Misguided Threat Intelligence

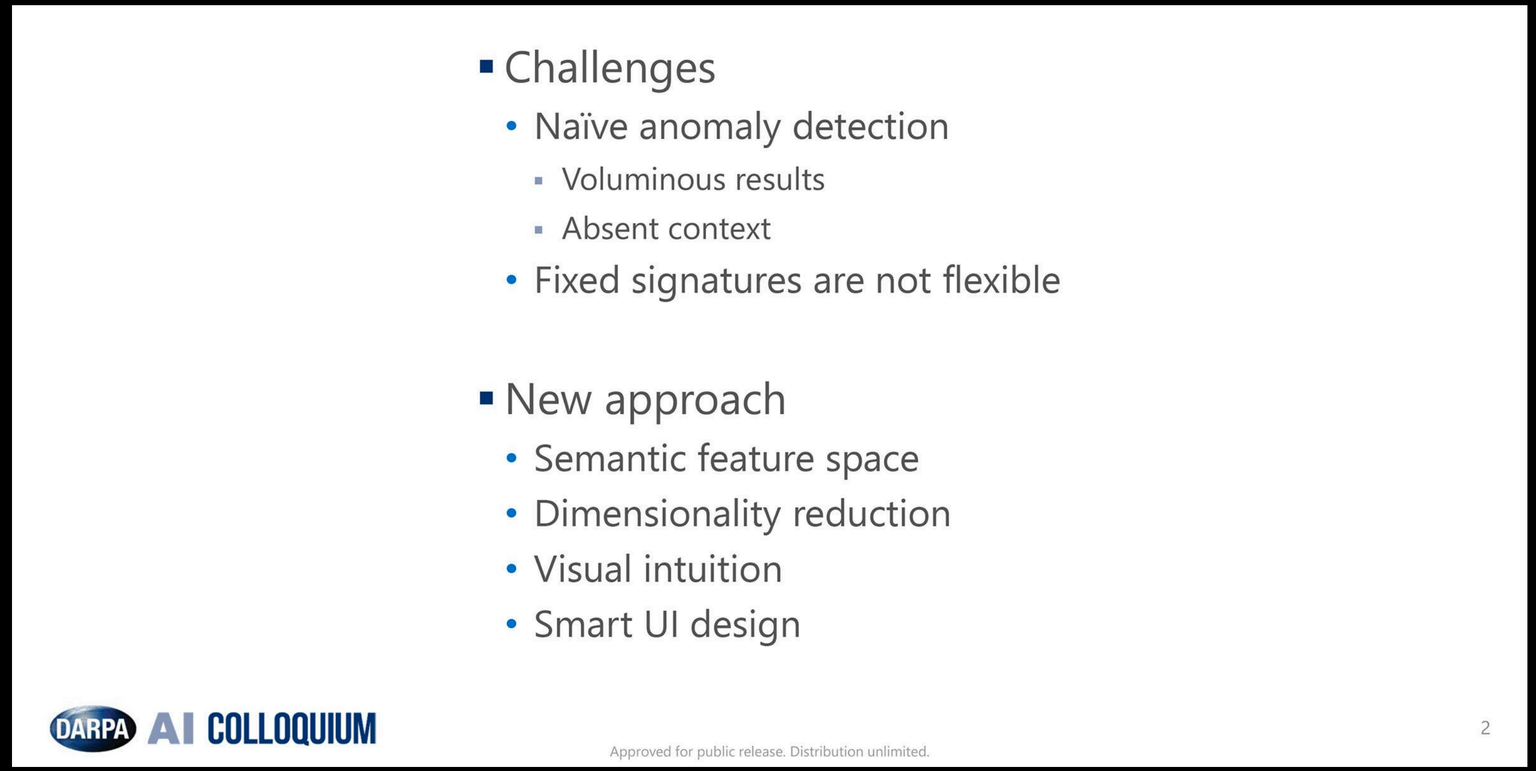
- Can lead to problems
- Verify with multiple sources
- Call out vendors

SOC 工作不痛苦

- What makes SOC not ineffective and working in it not painful?
  - Not lack of professionals that can lead and prioritize alerts / threats
    - Recruit professionals and treat them well, or train the members
    - Hold internal / cross-department technical meeting
  - Not lack of proactive threat hunting that can correlate events and reduce false positives
    - Participate and engage in the Threat Intelligence community
    - Deploy MDR / EDR with MSSP or SOAR with playbooks

Context matters

- Even DARPA points out “It’s very difficult to detect cyber threats across large enterprise networks”
- Not to mention “the variability of malicious activities”



Context matters

- Even DARPA points out “It’s very difficult to detect cyber threats across large enterprise networks”
- Not to mention “the variability of malicious activities”
- What we need is a “Adaptive Security Architecture”

Context matters

- Even DARPA points out “It’s very difficult to detect cyber threats across large enterprise networks”
- Not to mention “the variability of malicious activities”
- What we need is a “Adaptive Security Architecture”
    - Traditional “prevent and detect” approaches are inadequate due to
        - Increasing adoption of cloud-based systems
        - Open application programming interfaces (APIs)

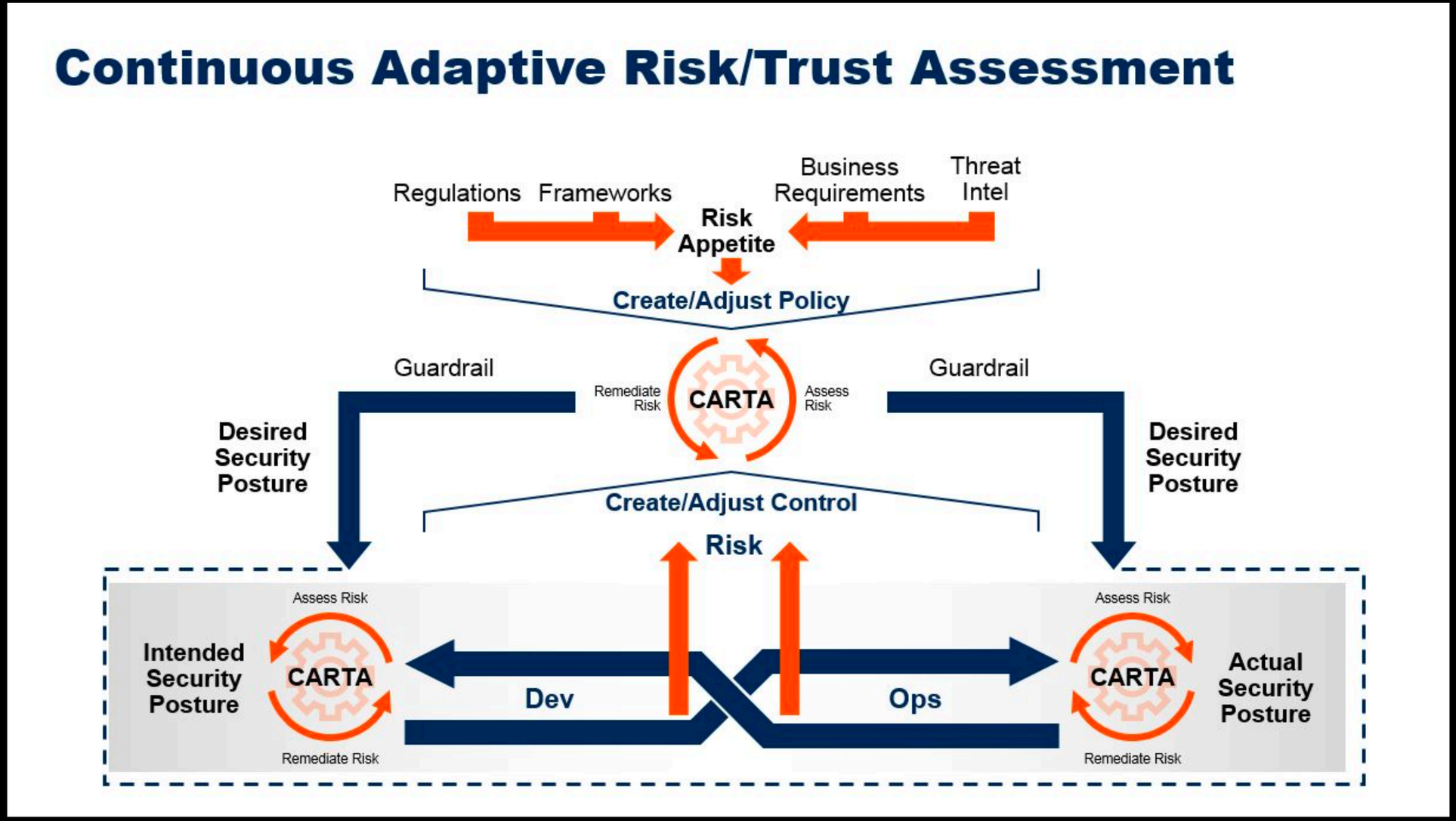
Context matters

- Even DARPA points out “It’s very difficult to detect cyber threats across large enterprise networks”
- Not to mention “the variability of malicious activities”
- What we need is a “Adaptive Security Architecture”
    - Traditional “prevent and detect” approaches are inadequate due to
        - Increasing adoption of cloud-based systems
        - Open application programming interfaces (APIs)
    - The network perimeter is gone (or extended and now exists everywhere)

CARTA

The Gartner Continuous Adaptive Risk and Trust Assessment

CARTA


Continuous Adaptive Risk/Trust Assessment
Regulations
Frameworks
Business Requirements
Threat Intel
Risk Appetite
Create/Adjust Policy
Guardrail
Guardrail
Remediate Risk
CARTA
Assess Risk
Desired Security Posture
Desired Security Posture
Create/Adjust Control
Risk
Assess Risk
Assess Risk
Intended Security Posture
CARTA
Dev
Ops
CARTA
Actual Security Posture
Remediate Risk
Remediate Risk

CARTA

研究顯示美國醫療保健系統歧視黑人病患

美國醫療照護系統的演算法僅以保險與醫療費用資料，來衡量民眾的健康狀況，未考量到黑人在存取醫療照護資源時通常有其限制，導致在症狀同樣嚴重的白人與黑人之間，白人通常會相對容易得到應有的醫療資源

文/ 陳曉莉 | 2019-10-29 發表

Photo by Marcelo Leal on https://unsplash.com/photos/6pcGTJDuf6M

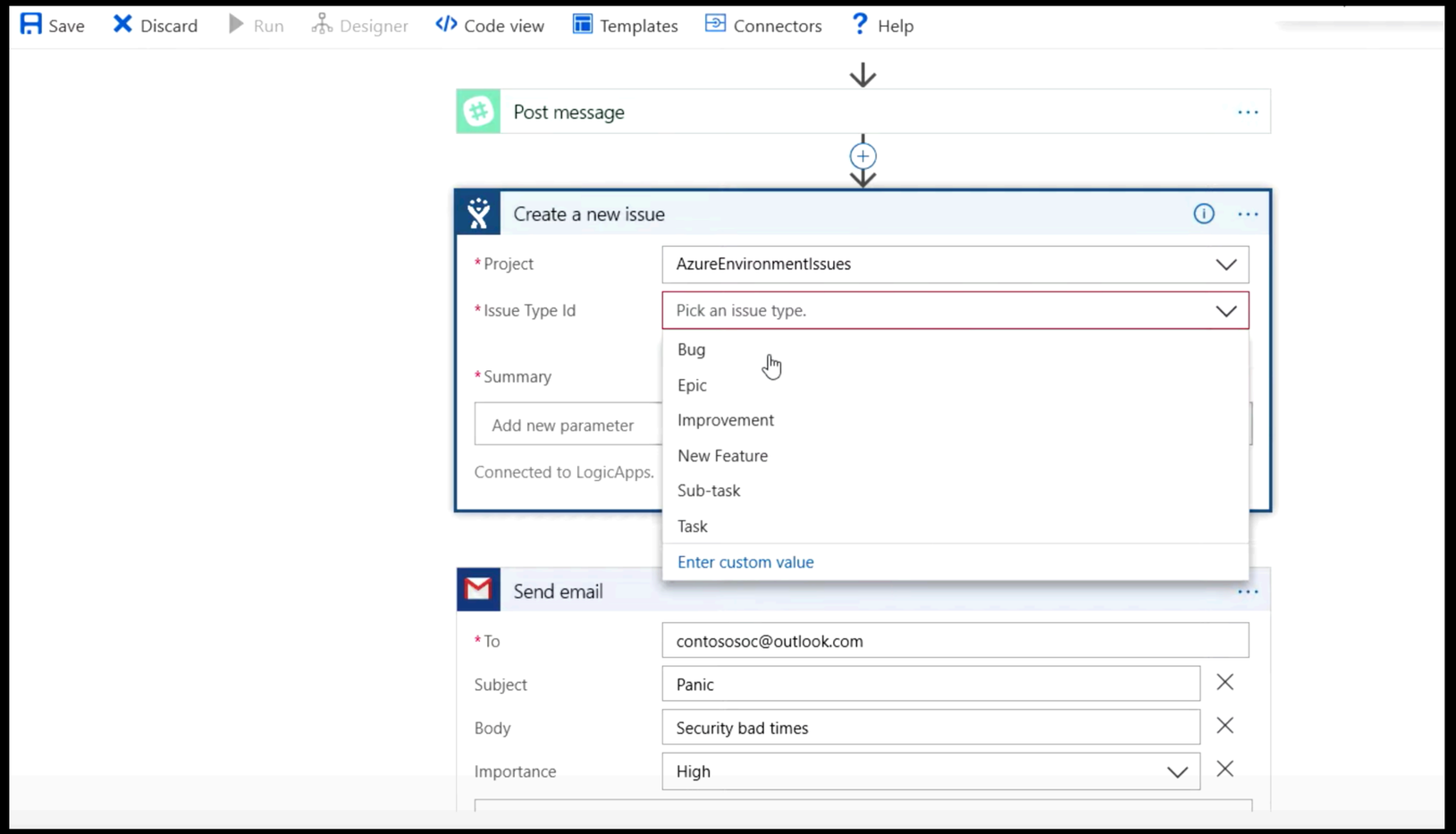
CARTA

1. 將一次性的資安把關機制，替換成具有情境感知能力、能夠自適應且具有可程式化特性的資安平臺
2. 持續主動和被動地挖掘、監測、評估風險，並排定優先順序
3. 在數位商業計畫初期即進行風險和信任評估
4. 建立基礎架構時應具有完整且全方位的風險能見度，包括敏感資料的處理方案
5. 使用分析技術、人工智慧、自動化和調度編配（Orchestration），以加速偵測及回應的時間，並和擴大影響力
6. 將資安防護建構成整合的自適應可程式化系統，而非形成資料孤島
7. 將資料驅動的風險決策和風險所有權，交到業務單位和產品負責人手中

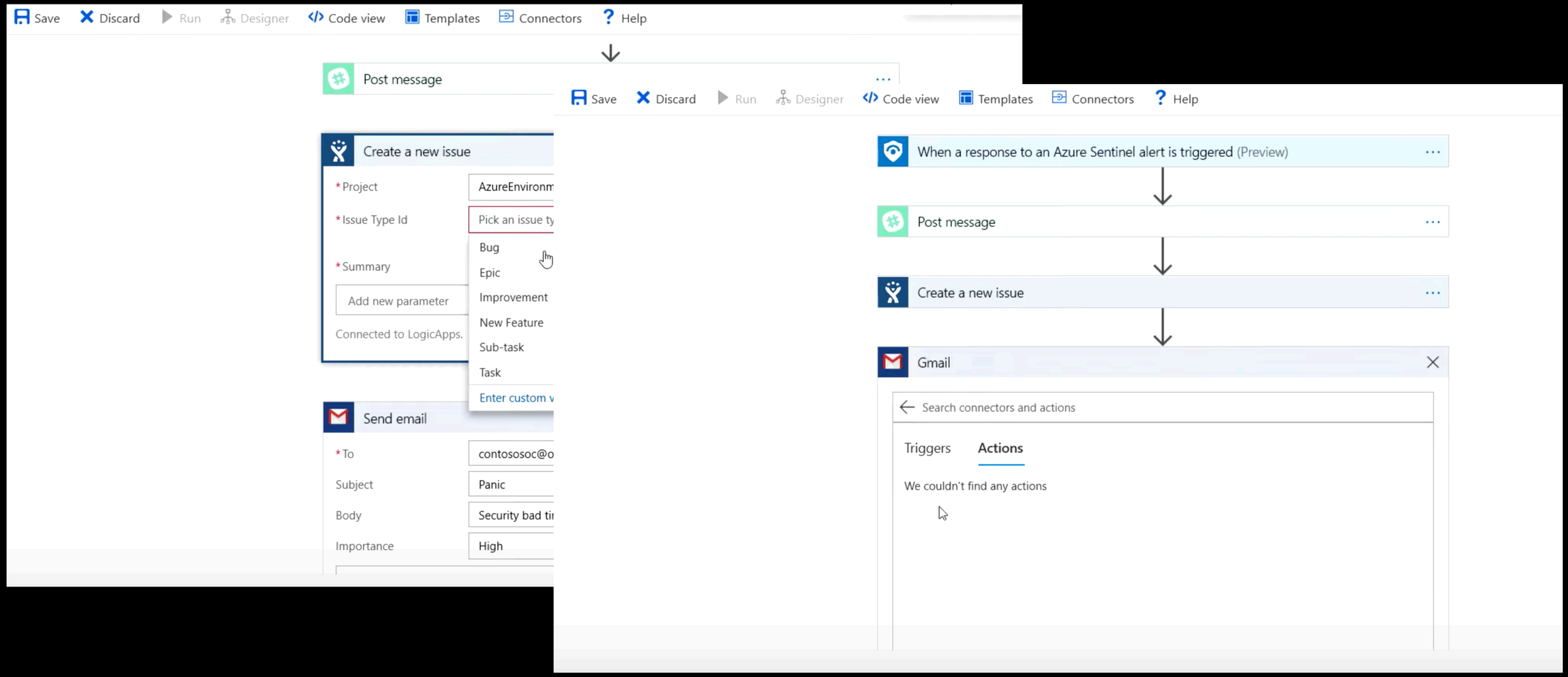
CARTA

1. **ZERO TRUST NETWORK**
2. **THREAT HUNTING**
3. 在數位商業計畫初期即進行風險和信任評估
4. 建立基礎架構時應具有完整且全方位的風險能見度，包括敏感資料的處理方案
5. **SECURITY ORCHESTRATION AUTOMATION & RESPONSE**
6. **CONTINUOUS ADAPTIVE RISK AND TRUST ASSESSMENT**
7. 將資料驅動的風險決策和風險所有權，交到業務單位和產品負責人手中

SOAR

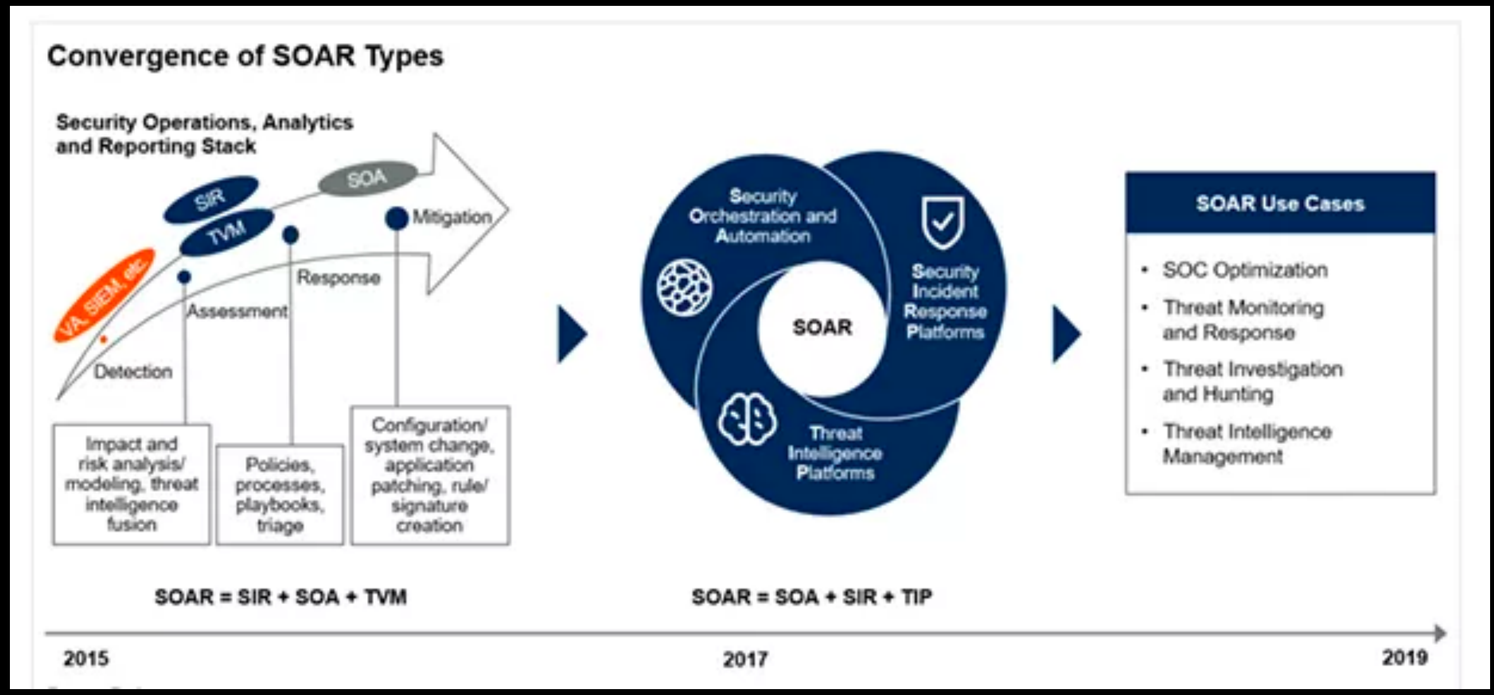

Save
Discard
Run
Designer
Code view
Templates
Connectors
Help
Post message
Create a new issue
* Project
AzureEnvironmentIssues
* Issue Type Id
Pick an issue type.
Bug
Epic
Improvement
New Feature
Sub-task
Task
Enter custom value
* Summary
Add new parameter
Connected to LogicApps.
Send email
* To
contososoc@outlook.com
Subject
Panic
Body
Security bad times
Importance
High

SOAR


Save
Discard
Run
Designer
Code view
Templates
Connectors
Help
Post message
Create a new issue
* Project
AzureEnvironm
* Issue Type Id
Pick an issue ty
* Summary
Add new parameter
Connected to LogicApps.
Bug
Epic
Improvement
New Feature
Sub-task
Task
Enter custom v
Send email
* To
contososoc@o
Subject
Panic
Body
Security bad ti
Importance
High
Save
Discard
Run
Designer
Code view
Templates
Connectors
Help
When a response to an Azure Sentinel alert is triggered (Preview)
Post message
Create a new issue
Gmail
Search connectors and actions
Triggers
Actions
We couldn't find any actions

SOAR

- Do I Need a SIEM if I Have SOAR?
  - It depends on what you mean “SIEM”
  - Short answer is “Not necessarily”, if SIEM is only for log repository



Closing Remarks

- The defense line has been pulled back to the end points again due to undetected attacks and the imbalance between defender and attacker
    - It was end-point at first (AV), then went to the front line (Firewall / WAF/ IPS), and moved back to the end-point again
- Besides that, Zero Trust Network has become more and more important
    - Web / Browser Isolation, VDI
    - CDR / URL replacement

There’s no killer products

Only the products fit the company, the environments, the teams which make them “good”

You have to

- Make sure you really need the products
- Give them a UAT to PoC
    - Aggressive detecting capability
        - Lockheed Martin Cyber Kill Chain / MITRE ATT&CK Evaluations
        - Red Team Assessments
    - Adaptive response capability
        - SOAR
        - Containers / Kubernetes / Microservices

References

1. Regional Risks for Doing Business 2019
2. SIEM for startups: why should you care?
3. CERT vs. CSIRT vs. SOC: What's the difference?
4. NIST Cybersecurity Framework 概覽
5. Improving the Effectiveness of the Security Operations Center
6. SAFE
7. Cisco Design Zone for Security
8. 新技术洞见：安全编排、自动化及响应（SOAR）解决方案
9. Do I Need a SIEM if I Have SOAR?

Thank you ☺️

Question?