TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

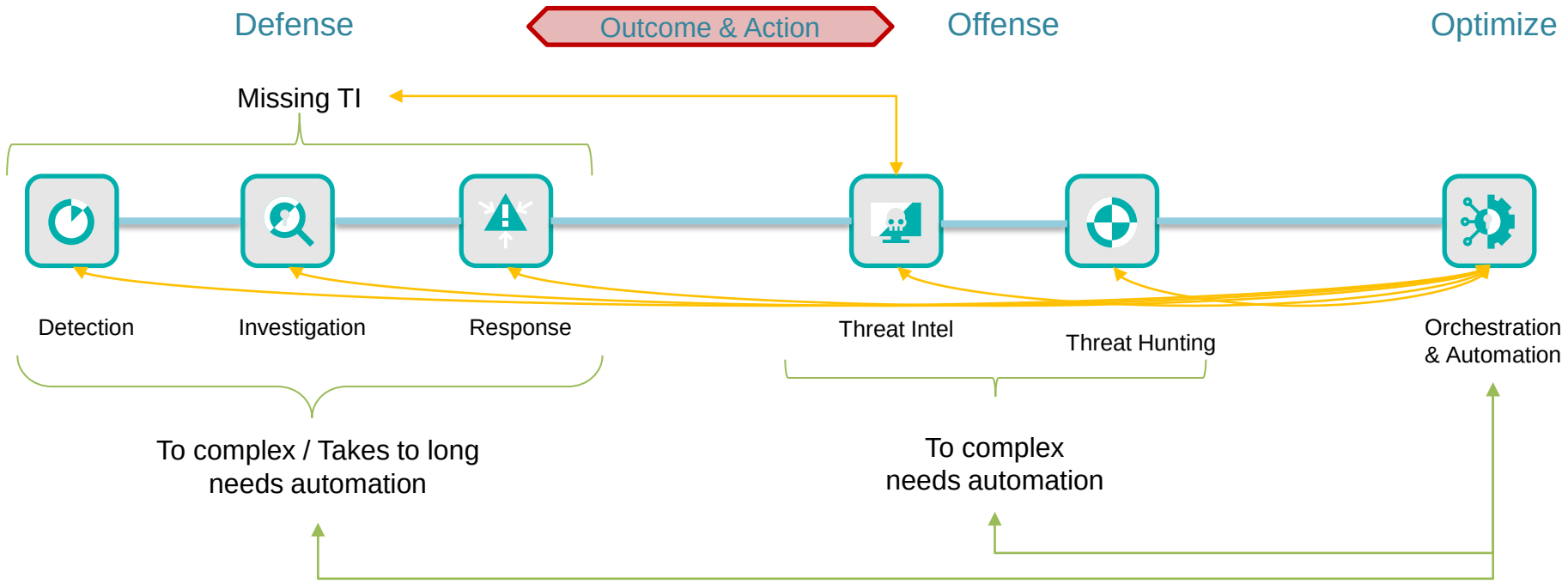
Berlin, 26. - 27.06.2024

"Sicherheitsautomatisierung"

Andy Grzess, ReliaQuest

Cyber Classic Maturity Automation

Automation muss so früh wie möglich ein geplant werden



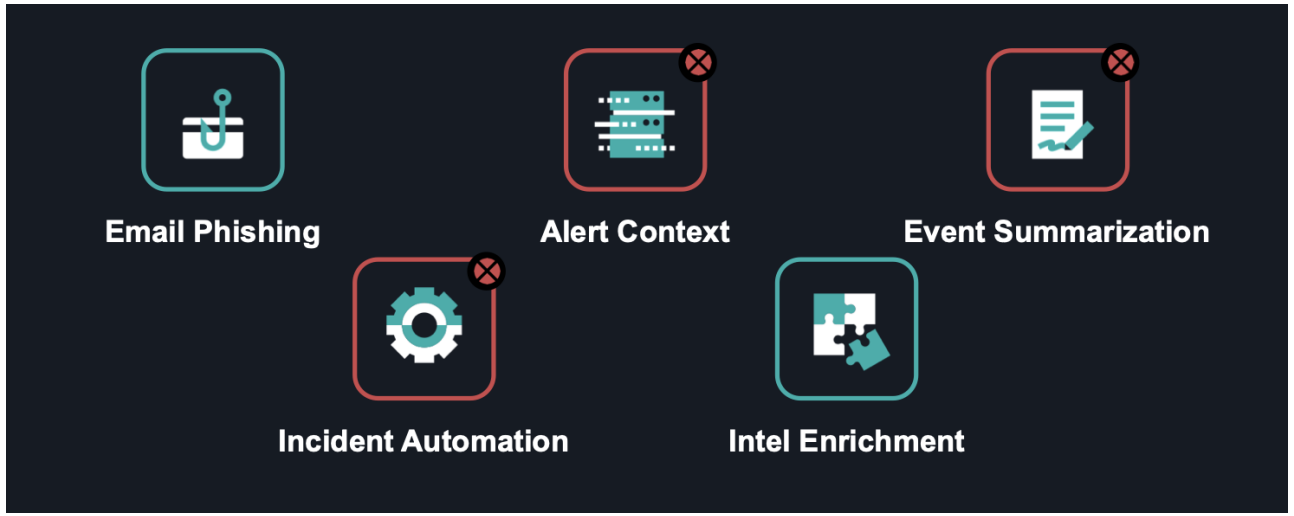
Sicherheitsautomation

Wenn alle Elemente des IR-Prozess abgedeckt werden können viele Attacken in den früh vereitelt werden.

Kosteneffiziente Automation muss früh eingebaut werden.

Bei der Auswahl des CSOC, MDR, XDR oder MSSP muss Automation eine Priorität sein.

Viel Automationsproject scheitern im ersten Jahr



Die meisten Organisationen kämpfen damit, mehr als 2 von 5 wesentlichen Automatisierungsanwendungsfällen im ersten Jahr ihrer SOAR-Integration umzusetzen. Viele werden niemals einen ROI erreichen, da sie aufgrund der Komplexität und fehlender Ressourcen die weitere Implementierung aufgeben.

Warum Automation Fallbeispiel (März 2020)

- 1. Tag Freitag mit 24/7 passive Respons MDR
  - 16:01 Enduser klickt link in einer Phishing-Email.
  - 16:02 RAT-Malware wurde heruntergeladen installiert.
  - 16:23 EDR kann RAT nicht entfernen.
  - 16:24 SIEM Alarm.
  - 16:36 SOC beantragt Isolation des Endpunkt und User Password reset.
  - 17:16 Angreifer nutzt Local-Admin um Rechte zu erweitern.
  - 21:46 Angreifer hat Zugriff auf AD mit AD-Admin.
- 2.Tag
  - 14:30 Nach 8 Eskalationsversuchen wurde der Endpunk. isoliert (3 Geolokationen)
  - 15:23 Anruf Direktor CSOC zum MDR “Es ist Passiert“
    - AD – encrypted
    - 25% Backups encrypted
    - AD-Admins disabled
  - 15:35 Worldwide network Shutdown.
- 2 Jaher Später → >12Million $ Schaden ….

Ursache:
Phishing wurde 90 Minuten früher gemeldet (Nach +20 fällen Schichtende mach ich Montag).

AbuseMailBox Usecase
Mit einer Automation hätte man die Attacke in 10 bis 15 Minuten eindämmen können

- Löschen des Phishing in allen Mailboxen
- IOC update auf für FW, EDR, Proxy, DNS, etc.
- Hunting in allen Systemen

Der Eskalationsprozess brach zusammen (COVID).

Mit einer Automation hätte man die Attacke in 10 bis 15 Minuten eindämmen können

Triage unter 10 min gefolgt von automatischer
- Enduser Session und Password reset
- Endpunkt Isolation
- IOC update auf für FW, EDR, Proxy, DNS, etc.
- Hunting in allen Systemen

MTTR Reaktion vorm Hauptvorfall

- 1. Tag Freitag mit 24/7 passive Respons MDR
  - 16:01 Enduser klickt link in einer Phishing-Email.
  - 16:02 RAT-Malware wurde heruntergeladen installiert.
  - 16:23 EDR kann RAT nicht entfernen.
  - 16:24 SIEM Alarm.
  - 16:36 SOC beantragt Isolation des Endpunkt und User Password reset.
  - 17:16 Angreifer nutzt Local-Admin um Rechte zu erweitern.
  - 21:46 Angreifer hat Zugriff auf AD mit AD-Admin.
- 2.Tag
  - 14:30 Nach 8 Eskalationsversuchen wurde der Endpunk. isoliert (3 Geolokationen)
  - 15:23 Anruf Direktor CSOC zum MDR “Es ist Passiert“
    - AD – encrypted
    - 25% Backups encrypted
    - AD-Admins disabled
  - 15:35 Worldwide network Shutdown.
- 2 Jaher Später → >12Million $ Schaden ….