AUTOMATING SECURITY RESPONSE

DAVID WILLIAMSON

DIRECTOR, CISCO CUSTOMER EXPERIENCE

What is SOAR?

- Security Orchestration, Automation and Response
- Per Gartner (#325580), the core components of SOAR are:
  - Workflow engine
  - Case and Ticket management
  - Orchestration and Automation
  - Threat Intelligence Management
- SOAR is more than a product
  - Processes + software platform + integrations across your infrastructure and systems for both inputs and controls to mitigate

Why would we want to implement automation?

- The volume of incidents seen in a SOC that have to be dealt with by analysts, especially L1, is overwhelming
  - Repetitive, high workload, leading to burn-out and retention issues
  - Easy to miss a serious attack in the noise of the obvious – even if there are no false positives
- Our goal is to automate this workload wherever possible
  - Free analysts' time for more interesting work, reducing churn and burn-out
    - Including threat hunting based on escalations from the SOAR platform
  - Reduce response times
  - Drive consistency of execution for metrics and machine learning

We need to reduce the response time!

- Actors have automation too!
  - Actors use tooling to scan, probe, exploit, mutate and expand faster than human defenders can react, so your ability to respond in the same or better timescale is critical
- As defenders we need to improve response time, lowering latency between detection and mitigation
  - Automation is key to this, through automated application of controls for mitigation and/or activating supporting controls to slow down the attacker
- Don’t bring people to a software fight, you’ll be outgunned!

Building your default risk profile

- What is your default risk profile, or “block if…”?
  - Expressed as a n-tuple workflow with logical connectives which can be expressed in natural or formal language
- Various factors influence the risk profile for a given target
  - Time, target criticality, target posture, etc.
- And also for the identified risk based on IoCs
  - Identified actor, known bad source domain, geolocation, traffic path, Kill Chain™ stage, indicator history, IoC quality, number of IoC sources, time since published, access via a proxy server, has touched a honeypot, etc.
- Risk profile and tolerance is different for each organisation

Why do people hesitate to automate?

- Automation has vastly lower OpEx, so why doesn't everyone do it?
  - Mostly because they fear that it'll go wrong and cause unintended, serious consequences on their network and systems – due to bad input data, failure of automated process or failure of automated controls
- But, you already automate!
  - You rely on vendors and tools such as Microsoft SCCM, SolarWinds, ManageEngine etc. to patch your end-points, on anti-malware vendors to update their software and signatures etc.
- So the challenge is often to overcome this hesitancy

Overcoming that hesitancy

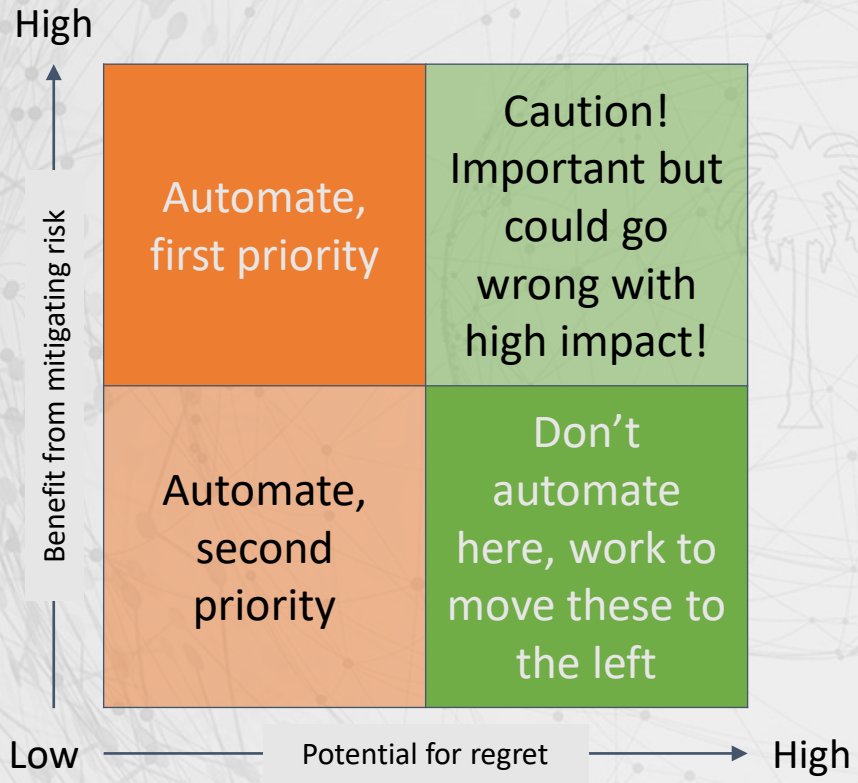
- What could be done to eliminate hesitancy?
  - We need a quantified and lower risk of negative consequences – to reduce or even eradicate the risk of a bad outcome to an automated application of a control
- To do this we need
  - Increased confidence in the decision making, specifically in
    - Input data to the process
    - The process itself
    - If the process results in an action, the application of the control
  - Limited or acceptable consequences if the mitigation is erroneous or the application somehow fails

The principle of low regret

- A model devised at the John Hopkins Advanced Physics Laboratory
- Low potential or likelihood of regretting the outcome of the application of a control to mitigate an event per the detected IoCs
  - If we mitigate an identified attack that subsequently proves to be a false positive, or the application of the automated control fails, the consequences of that erroneous mitigation have trivial or acceptable negative impact on the organisation's operations and data integrity
- If we can calculate the potential for regret against the benefit of mitigating risk via application of a control, then we can decide what we can automate and what we can't

What to automate?

- Categorise mitigation processes
  - Prioritise what has greatest benefit at least potential for regret, then work down
  - With each quartile, prioritise according to the complexity of automating – focus on quick to implement, leave the hardest things in each quartile to later – and not the things with the perceived highest benefit or reduction in analyst workload
- If more sophistication is desired, add a 3rd dimension for confidence
  - Confidence in risk rating, intelligence and the controls used to mitigate



Improving confidence

- A risk scoring mechanism is required so that scores can be compared to risk profile thresholds to trigger action
  - A numeric value to compare against the default risk profile
- Inform the mechanism using threat intelligence
  - Using ThreatQuotient* or similar, fed by OSINT and commercial feeds such as Flashpoint*, Intel 471, SenseCy, Terbium Labs, Sixgill etc.
  - ThreatQ has a customisable scoring system based on source name or type, attributes, adversary and indicator type

* Cisco Investments portfolio companies

Technical components to a SOAR solution

- A SOAR tool to provide workflow orchestration and automation
  - CyberSponse, Phantom, Demisto, Resilient, Siemplify, D3, Swimlane, etc.
- Increase confidence using threat intelligence, complementing raw IoC feeds with more sophisticated interrogative APIs
  - e.g. Cisco OpenDNS Investigate API, Cisco Threat Grid API
- Apply technical controls natively in the SOAR platform, by raising an ITSM ticket for application by another team or tool, or via Cisco NSO

What else can my SOAR tool do for me?

- SOAR provides automation of processes and playbooks in software for faster, predictable and consistent outcomes
  - Case management is the centre of the analyst workflow, the core functionality of a SOAR tool
- However, as it is the central point of coordination and workflow it is typically also a powerful source of information about SOC operations
  - Data from the SOAR tool can populate native dashboard applications such as Tableau or Panaseer* providing near real-time metrics on queue, responses and cases

* A Cisco Investments portfolio company


CISCO