Datasheet

Managed Services Component:
Security Automation and Response – Phantom

SOC analysts spend a lot of time on high effort tasks that can be perceived as low on returned value.

Running queries on potential Indicators of Compromise (IOC) across multiple enrichment services to provide context is vital in ensuring false positives are closed down and true threats identified.

Unfortunately, the time taken in assessing, correlating, analysing and reporting information across multiple platforms and services, is time taken from identifying and neutralising the genuine threats.

Increasing analyst numbers in the SOC to cope isn't a realistic way to sustain operational efficiency: the numbers literally don't add up. But doing nothing to address the challenges of scale puts a managed service in the position of having to do more with less. And the only thing that increases is risk.

Adarma Responds: Security Orchestration Automation and Response

At Adarma, when we identify risk for our customers, we act. We took a new approach:

Use machine power to perform the many structured, predictable, repeatable, and time-consuming tasks - across multiple services and multiple platforms - at speeds unachievable by analysts.

And let analysts embrace uniquely human qualities and expertise: making decisions, exercising judgement, reaching solutions, guiding, monitoring, and reporting the results.

Multiple systems working together, machine and human operating in their domain of expertise: that's at the core of SOAR.

SOAR platforms **automate** to complete individual tasks and **orchestrate** to complete processes - sequences of tasks that may run across platforms, applications, or networks- without the need for manual intervention.

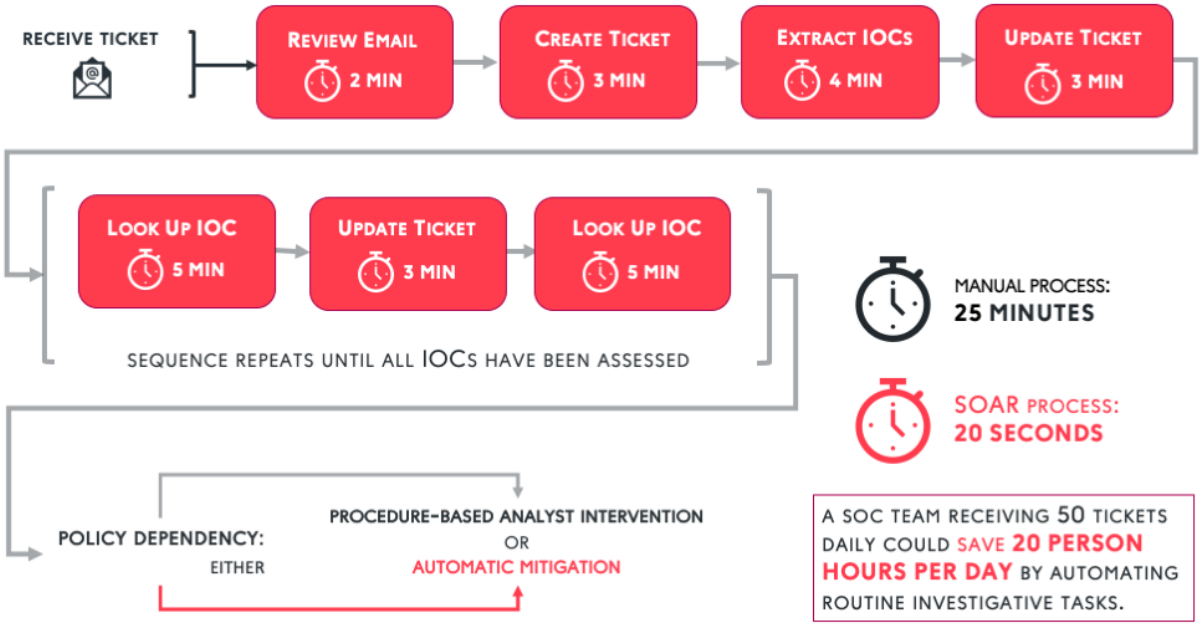
Tasks that might take an analyst minutes take place in seconds to correlate, enrich, and present information about potential IOCs, allowing analysts to make decisions about incident correlation, triage, and investigation.

Where analyst expertise is needed, automation and orchestration procedures request attention at key decision points and continue once it's been supplied.

Machine Expertise	Human Expertise
Regular, consistent analysis at volume and pace – no intuitive judgement	Analysis involving experience/instinct in making judgement
Displays minimal bias (any bias tends to be introduced by author of use case or framework)	Decisions requiring outside framework
Speedy and effective in following process and branching, logical decisions	Less rapid, tendency towards bias (training, beliefs, etc) – but flexible, effective, efficient

© 2020 Adarma Ltd

Managed Services Component:
Security Automation and Response – Phantom



SOARing Benefits

In the diagram above, illustrating the workflow for assessing a potential phishing attack, the timings (via Forrester) demonstrate the efficiency gains possibly for the number of routine analyst tasks.

With good modelling, SOAR can consult multiple services in parallel in around 20 seconds and a judgement request made to an analyst – with the results already formatted and ready for reporting.

When integrated with existing security tools, particularly SIEM, mean time to resolution (MTTR) is greatly lowered. Analysts spend less of their day on high time, low skill tasks and can focus skills on proactive threat detection and critical investigations, helping deliver increased value from your current security investment.

Using SOAR capabilities and Adarma engineering, we've delivered SOC performance efficiencies of up to 40% and beyond.

Achieving this kind of result is not quite as simple "use case=process". Poor modelling can drastically undermine SOAR's effectiveness – and value to you.

At Adarma, we have decades of combined experience in modelling, designing, managing, and implementing the processes that make up a SOC.

And we're here to help.

Adarma's SOAR Managed Service

Adarma was founded to make the world a safer place to do business, and our managed service products are designed to assure our customers of the best possible cyber defence. The partnership and transparency we offer is unequalled .

Our analysts have combined decades of experience in SOC management and operations.

Our threat intelligence platform keeps you informed of potential compromises - and our analysts alert to detect them.

© 2020 Adarma Ltd

Managed Services Component:
Security Automation and Response – Phantom

Our vulnerability management solution lets us identify, contextualise, track, and prioritise remediation recommendations to reduce risk in a managed and intelligence-driven way.

And our Phantom engineering and consultancy practices are led by the only Splunk Phantom accredited trainer and consultant in the United Kingdom. We've been instrumental in the majority of Phantom deployments in the UK, and our automation use case library can dramatically accelerate your time to value.

Adarma's SOAR capabilities are vital to our service. We've chosen Splunk Phantom to supply them because we believe it provides the most powerful SOAR tooling coupled with response and reporting mechanisms so efficient they've already made JIRA obsolete for many customers.

It's modular, scalable, provides tools to allow rapid prototyping as well as in-depth development, and it integrates simply and easily with major SIEM platforms out of the box.

Our SOAR capabilities reduce false positives, reduce investigation times, reduce alert numbers. SOAR knits together processes, procedures, platforms, and services to become a force multiplier for the team – concentrating analyst time and attention on the critical tasks that protect your assets and reduce your risks.

Phantom Key Features

We make full use of the best features of Phantom to keep increasing efficiency and effectiveness, driven by the desire to deliver value to you.

Modular: the orchestration and automation capabilities of Phantom aren't just task lists. They're modular and reusable actions, decisions, and interactions driven by analyst input to stay flexible, adaptable, and maintainable.

Scalable: tasks run concurrently and in parallel.

Rapid development: many tasks snap together like building blocks via an extensive GUI, no coding time required. Python scripting is available for advanced development.

Seamless SIEM integration: Phantom integrates directly with Splunk to allow deep diving into your service data, analysing Phantom and SOC performance as well as threats information. Phantom can even use Splunk data to detect that things aren't working as expected and take action to amend - no intervention required!

About Adarma

We're one of the largest independent security services companies in the UK. As a business formed and run by experienced senior security leaders, we know security and how to deliver real value in the real world. This is why our clients are successful FTSE 350 organisations from all industry sectors.

Adarma delivers innovative tailored solutions for some of the world's biggest companies. Our teams are a diverse group of technical experts and consultants, all with the same objective and united by the same goal: to help our clients prepare for attack and stand side-by-side with them when it happens.

Helping make the world a safer place.

Contact us to discuss your Managed Service or SOAR requirements enquiries@adarma.com

www.adarma.com

© 2020 Adarma Ltd

ADARMA