Datasheet

ADARMA Incident Simulation
Rehearse and test for confidence

Have confidence in your playbook and your resilience to threat

Questions about your ability to respond

The faster you can contain, respond, and remediate an attack, the less damage it can do to your organisation. Learning from mistakes can also be an expensive way to go. Attacks will happen, it is how you respond to them that matters. Therefore, having a cyber security incident response process that flows from detection, identification, investigation, containment through to remediation is the first step. Being fast, confident, and assured in how to use it and whether it works in relation to the threats you face is imperative.

Good incident simulation builds confidence in your playbook and your resilience to threat. Rehearsing time-pressured technical, process and individual decision making is a critical component of being prepared to respond. challenging the varied capabilities involved in an effective response. Confidence is delivered in answers to questions:

- Do you have the right technology to enable detection, hunting collaboration?
- Do you have the right mix of skills, attributes, and personnel, can they work together and communicate well?
- Do you have the right processes to support the flow of information to achieve the fastest possible outcome with the greatest confidence?
- What are the internal and external dependencies relating to responding to an incident?

Answers to give you confidence

Adarma's cyber incident simulation exercises take you beyond just checking if you have controls in place. The cyber threat landscape and the constantly changing TTPs (tactics, techniques, and procedures) leveraged by threat actors, renders static traditional compliance activity ineffective.

Adarma have designed a range of incident simulation exercises based on the most relevant threats currently impacting businesses and those on the horizon of becoming mainstream.

The Adarma incident simulation exercise leverages real world threat actor TTPs to develop realistic scenarios that security teams will be required to address. Our extensive experience in threat intelligence and our threat led approach towards implementing cyber security enables us to generate and replicate what business will face in the event of a cyber related incident.

WE HELP YOU

Validate or restore confidence in your Incident response process

Improve threat resillience across Protection, detection, containment investigation and response

Measure and improve SOC performance against real threats you will face

Design an improvement plan for ongoing security posture and governance

Focused on your outcome

The Adarma Incident simulation follows 4 steps:

Environment analysis
We Identify the areas of focus and agree on the rules of engagement. We understand current controls in place and the scope of the area of focus. We document your current organisational staffing model, third parties involved and key individuals that will need to participate.

Threat narrative development
We develop the threat narrative, setting the scene and context of the incident with you. We include context like first contact, discovery, detection, and actions. To ensure success is measured, we detail objectives to be achieved, processes and technology capabilities tested.

Wargaming scenario generation
We generate threat injects to support the threat narrative. The threat injects simulate threat actor TTPs and are used throughout to support each phase of the cyber kill chain. Wargaming puts your team in a simulated incident response footing. Throughout the wargaming phase, Adarma will provide immediate feedback with the team to ensure lessons learned can be used immediately.

Final report and feedback
We detail what went well/not and improvements and changes need to be made including:

- People - roles to be added to the security or incident response team, skills gaps, seniority of resources
- Processes - Increasing efficiency, removing overhead, ineffective steps in the process, and additional resources into the incident RACI.
- Technology - IOC inclusion, rule updates, repositioning of sensors, telemetry to collect

We are Adarma

Your strategic partner for effective cyber threat management, we exist to protect your promise of cyber threat resilience. Our expert team of threat management specialists guide and support you to confidently mitigate risk and maximise value of your cybersecurity. Working hand-in-hand with you and your team we provide advice, intelligence, technology and security services with complete visibility and transparency to ensure you are fully protected as you transform, innovate and grow. We help you deliver the security outcomes you need to make a difference.

How to Engage

For more details, discuss your needs with Adarma client Director or account manager today.

Threat-led	More than Tech	Just like you
Our injects are constantly updated to ensure the most relevant real world TTPs are used in our exercises. Our incident simulation is tailored to your threats and context.	Focused on technology, process, and people. Outcomes include improvements to your team structure and skill sets to improve effectiveness as well as technology and process	Delivered by security professionals. Our experienced delivery team has been where you are, we know your challenges and what it takes to help you achieve your goals

ADARMA

Contact Details T: 0333 0058535 | E: hello@adarma.com | W: www.adarma.com

3rd Floor, Quay 1, 133 Fountainbridge, Edinburgh, EH3 9QG

www.linkedin.com/company/adarma-security twitter.com/adarma_security