Datasheet

Managed Services Component:
Adarma Countermeasures Management Platform

Trustworthy threat intelligence is vital to your cyber defence. What new threats are trending? Are older threats re-emerging with new dangers? What can you use to determine if you're at risk of compromise?

Failing to keep your intelligence up-to-date increases your risk by increasing the chances an attacker will slip unrecognised past your security measures, but effective defence doesn't rely on threat intelligence alone.

To shut down threats as quickly as possible before damage is done needs the ability to understand like the enemy: to think like an attacker, to anticipate what they're doing *right now* and predict the steps they'll take next.

Crafting that sort of response isn't simple. Countermeasures that are effective in reducing your risk requires the kind of judgement that only comes with experience combined with deep technical expertise – the ability to deconstruct adversarial tactics and techniques to model them as a logical series of detective rules.

Delivering that in a way that's sensitive to the unique needs of your organisation – that's a challenge.

Adarma has the experience and expertise to meet and exceed it.

Adarma's Managed Services

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.

Our analysts are cyber security professionals with combined decades of experience in SOC management and operations. Our SOAR capabilities make us fast and efficient in incident correlation and triage, IOC enrichment, and reporting.

Our threat intelligence platform identifies and tracks emerging IOCs, and our vulnerability management solution lets us identify, contextualise, track, and prioritise remediation recommendations to reduce risk in a managed and intelligence-driven way.

The partnership and transparency we offer is unequalled, customising our products and their operation to your unique needs, with tools and dashboards to let you see just how effectively they're performing.

Adarma Countermeasures Management Platform

Supported by these capabilities, the Adarma Countermeasures Management Platform (CMMP) is a proprietary platform for countermeasure design and deployment. It's a library of potential attack patterns, modelling each step from reconnaissance to final compromise – and providing the rules for your SIEM to detect them.

We chose to use the MITRE ATT&CK framework as the foundation of our platform. A living framework widely adopted by cyber security experts around the world, it provides a standardised way of describing attacker methodology.

Unlike other security frameworks focussing on risk management or identifying at what stage of comprise a system might find itself in, the ATT&CK framework focusses strongly on adversarial thinking to aid detection: what type of attack is this? How is it deployed? How does it move through systems and what artefacts does it leave as it goes?

Aligning to standards eliminates the uncontrolled risk that can otherwise compromise countermeasure employment and design – particularly in organisations with a wide variation in systems, technologies, and reporting methods.

Managed Services Component:
Adarma Countermeasures Management Platform

Key Platform Features

The Adarma CMMP identifies, models, and prioritises the stages of potential compromises in a standards-based, intelligence-driven way, giving you rapid warning of actual and potential attacks - and the recommended actions to effectively prevent or remediate them.

We model the *logic* of the countermeasure as a first step rather creating something specific to a single platform. Before deployment, it's translated into the platform's native format – like Splunk's SPL – as required. If there's ever a need to move platforms, your countermeasures can follow.

Harmonised, standard-based approach to modelling and managing countermeasures.

Increases SOC efficiency by decreasing time spend on rules management

Reduces risk in deployment – RESTful push-button process.

Auditable and reversible – multi-stage approval process with full commit history available.

CI/CD best practices are used in rule updates to integrate and deploy.

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 Countermeasures Management requirements
enquiries@adarma.com

www.adarma.com