Datasheet

Countermeasures Assessment

The Adarma Way

Detective controls, on platforms like Splunk and Splunk Enterprise Security (SIEM), are a critical component of countermeasure systems - your vanguard to identify malicious actors and actions.

They're often modelled and deployed at speed against a point in time target identified by VM and TI systems. But as time goes on, the risk created by this approach increases.

Time constraints result in use cases that may only be useful for a single threat at a single time, with deployed controls that don't meet best practice or deliver best results. These unknown control gaps create risk that can go unnoticed.

Effective risk mitigation depends on assessing both platform and implemented controls for maturity *at the same time* as you're evaluating the threat landscape - and the use cases you've developed to address it.

What challenges are addressed?

Our Countermeasures Assessment is a single product designed to perform these parallel assessments.

Beginning with a physical or virtual discovery workshop, over a typical two-week period we'll meet you where you are – managers, analysts, engineers – to assess your SOC and SIEM data sources, use cases, and controls. We'll go through them line by line, function by function, to ensure we understand your aims and needs.

The culmination is a Current State Report identifying gap areas and remediation recommendations, and a Future State Report outlining key next steps, both aligned to the MITRE ATT&CK framework.

A closure workshop communicates the findings and gives the opportunity to deep dive into the areas you find most compelling.

We'll resolve:

- **Hidden business risks** buried in use cases and controls that are ineffective, inefficient, and out of date.
- **Poor data quality**, data storage and ability to search, query, and analyse using the SIEM platform.
- **Uncertainty around platform health** – if your SIEM platform isn't at peak function, its controls provide no value.
- **Recommending process improvements** – making best use of CI/CD approaches to ensure new issues don't go unnoticed.

And we'll do it in a way that's concise, accurate, and actionable – combining rigorous analysis with our unique understanding of the threat landscape and experience managing SIEM platforms.

What are the advantages of Adarma's Countermeasures Assessment?

- **Deep use case and control analysis** – line by line, function by function, ensuring relevance and value.
- **High-level platform health analysis** - known issues, root causes, remediation requirements.
- **Reduce the most risk** – we outline key tactics and techniques.
- **Aligned to MITRE ATT&CK framework** - internationally recognised reference for IR present and future.
- **Clear and actionable feedback** - improve your use case development lifecycle, through workflow, process and governance.

Countermeasures Assessment

Why Adarma?

At Adarma we have been designing, developing, implementing and operating Splunk-based SIEM's for over 8 years.

Widely regarded as industry leaders, we're known for our deep Splunk knowledge and experience. Awarded Splunk's EMEA Partner of the Year 2019, we currently hold Elite partner status and are a Security Specialized Partner. We are often the first, and last, stop for Splunk expertise.

About Adarma

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

Our teams are a diverse group of customer-facing technical experts and business-facing 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.

We have the experience, proven track record, and recognition- as industry specialists to ensure our cyber security solutions are tailored to your needs.

Contact us to discuss your requirements enquiries@adarma.com