SOLUTION BRIEF

Armor SOC

Let our team of cybersecurity experts identify threats and guide remediation

Respond to threats with our Always-on SOC

Finding cybersecurity experts to add to your team is becoming near impossible. Armor's security operations center or "SOC" fills that gap with our own cybersecurity professionals (analysts, engineers, forensics experts, and support staff) who provide our customers with incident response, investigation, threat hunting capabilities and guidance.

Respond to threats around-the-clock

Armor managed detection and response (MDR) services includes investigating and responding to incidents as they arise. Armor continuously monitors your SIEM and analytics planes for :

- Alerts
- Compromise indicators
- Attack warnings

Hybrid threat surfaces require greater action

Armor constantly monitors new threats and attack vectors that might be missed and leverages intelligent automations throughout the threat hunting process including:

- Automated queries
- Jupyter notebooks
- Automated enrichment jobs

Predictively inform infrastructure reinforcement

Once hunting leads are validated, an investigation is launched and if active exploitation is discovered, an incident is created just as it would be if the exploit had been discovered by the SIEM.

Correlation rules and investigation steps into enrichment jobs can be reused to ensure the attack can be detected automatically in the future.

Why Armor SOC?

- Fill any gaps in your cybersecurity team instantly and cost effectively while keeping protection up to date
- Share licensing costs instead of organizational in-house SOCs bearing the full burden
- Offload alert analysis so your team can focus on what's important
- Create custom playbooks to respond quickly to known threats
- Rest assured with Armor expert certifications such as CISSP, and CISA

Full-service solution

Our SOC solution is only available as part of a full-service solution that complements the Armor extended detection and response (XDR) solution (collectively XDR+SOC). This is to ensure that our SOC can leverage all of the efficiencies provided by our XDR stack as well as safeguarding the quality of the data and insights produced by that stack.

Armor SOC is a key component of Armor's overall security portfolio

VAPT

Integration with release and runtime systems allows Armor to validate artefact integrity and monitor environment drift on an ongoing basis.

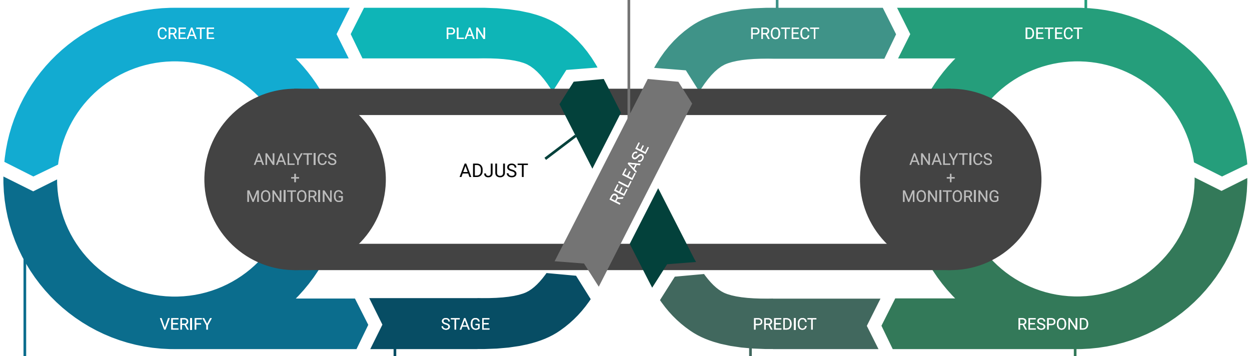
Armor's reporting APIs will feed remediation data into your product backlog for planning. Additionally, Armor's consulting services are available to inform strategy and prioritisation.

XDR

Armor offers runtime protection tools for various platforms or supports existing tools.

XDR

Armor XDR provides comprehensive cloud-native SIEM.



VAPT

Armor provides modern static and dynamic code analysis and dependency tree scanning to validate vulnerabilities aren't introduced.

VAPT

Armor's VAPT offering provides automated feedback on security posture regressions.

RISK MANAGEMENT

Integration with Armor's HITRUST vCISO offering will allow you to define risk-based, automated approval workflows with optional escalation for human compliance review.

SOC

Armor offers experienced SOC analysts, and advanced threat intelligence to predictively inform infrastructure reinforcement.

SOC

Armor's SOC includes SOAR playbooks to inform required changes.

Armor SOC features

INCIDENT NOTIFICATIONS

Near realtime notifications of incidents in your choice of mediums.

INCIDENT RESPONSE

The Professional and Enterprise plans include 24/7 incident response by our team of security experts.

THREAT REMEDIATION

Beyond documentation, our team of analysts and engineers will provide remediation guidance to help you mitigate threats faster and more effectively.

ADVANCED FORENSICS

In addition to remediation guidance, the Armor SOC will provide full deep-dive root cause analyzes (RCAs) to better inform recurrence prevention strategies.

THREAT HUNTING

Leverage out-of-the-box threat models to identify new threats in your environment.

BEST PRACTICES

Armor experts are constantly updating best practices among our other customers and in the industry to give you the highest level of secure operation.

About Armor

Armor is a global leader in cloud-native managed detection and response. As a trusted partner to more than 1,500 firms in over 40 countries, Armor offers cybersecurity and compliance consulting, professional services, and managed services. Armor's industry-leading experts leverage non-proprietary frameworks and a 24/7/365 SOC to be the de facto standard that cloud-centric customers trust with their risk.

Contact us

https://www.armor.com/company/contact

For a free cyber health check

https://www.armor.com/forms/cyber-health-check

For more information

(US) +1 877 262 3473 **(UK)** +44 800 500 3167