RSA PROGRAM FOR ADVANCED SOC

Automate operations and provide actionable intelligence to protect the organization from targeted attacks

AT-A-GLANCE

The RSA ® Advanced Cyber Defense (ACD) Practice enables agile mitigation of targeted attack activities. Using an intelligence driven security model, the ACD team focuses on the protection of critical business assets by applying proven operational expertise to enable front-line cyber readiness, response and resilience.

EXECUTIVE SUMMARY

Security programs have evolved to address a range of use cases, typically resulting in a variety of point solutions deployed for defense-in-depth. Targeted attacks represent a more acute challenge, whereby adversaries establish an attack infrastructure consisting of tools, tactics, and procedures to bypass traditional security measures. What can organizations do to protect themselves? One approach is to enhance existing capabilities with additional countermeasures. RSA recommends the consolidation of these efforts under a holistic program for an Advanced Security Operations Center (SOC).

The RSA® Advanced Cyber Defense (ACD) practice enables organizations to deepen their defenses and limit the risk to critical assets resulting from targeted attacks. The RSA ACD Program for Advanced SOC provides organizations with the ability to leverage the investment in traditional security defense mechanisms and enhance those capabilities with the additional technical and operational components to defend against targeted attacks. This includes an assessment of the current state and gaps and the deployment of new solutions required to address remediation requirements, customized to each organization's unique needs.

The intelligence required to prevent and remediate targeted attacks is derived by enhancing analytic capabilities. The RSA Program for Advanced SOC facilitates actionable intelligence by focusing on three key technical areas:

– Aggregation and analysis of threat intelligence data
– Correlation of content intelligence data from throughout the organization
– Security solutions that provide advanced analytic intelligence capabilities

The scope of the incident-handling process extends to non-security practitioners throughout the organization. It also extends to third parties. As a result, workflow needs to be managed in a manner that minimizes overhead and maximizes efficiencies, while simultaneously reducing breach exposure time. The RSA Program for Advanced SOC includes the automation of incident-handling processes and procedures.

Benefits of the RSA Advanced SOC Program include the alignment of risk management and business priorities. This ensures that scarce resources are being allocated where they are needed most. By implementing a holistic approach to targeted attacks, organizations can ensure that incident response is not simply regarded as a security function but also as an organizational competency, ready for use when it is needed.

RSA

SOLUTION PORTFOLIO

RSA's broad portfolio of solutions enables organizations to formulate the strategy and tactics for Advanced Cyber Defense. The combination of services and technology provides an agile platform for the design of a risk intelligent operation that suits a wide range of security postures and risk propensity levels.

RSA SOLUTIONS FOR ADVANCED CYBER DEFENSE

- Advanced SOC Design & Implementation
- Security Operations Management
- Vulnerability & Risk Management
- Cyber & Counter Threat Intelligence
- Incident Response
- Security Strategy & Program Development

Readiness, Response & Resilience

TAKE THE NEXT STEP

To benefit from the RSA Advanced SOC Program, please contact your RSA services sales representative.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA®