RSA

DATA SHEET

RSA® Advanced Cyber Defense

Controlled attack & response exercise

Executive summary

Incident lifecycle management

The RSA Controlled Attack & Response Exercise is for organizations that want to assess and enhance their maturity levels for threat detection and re-sponse. Preparations for real-world cyber attacks are best met by reviewing both technical and opera-tional capabilities for end-to-end incident lifecycle management.

Organizations seeking to extend capabilities beyond penetration testing and red teaming so that incident response becomes a broader organizational compe-tency can avail of consulting from the RSA Advanced Cyber Defense Practice, with tailored services to ac-commodate discrete customer needs.

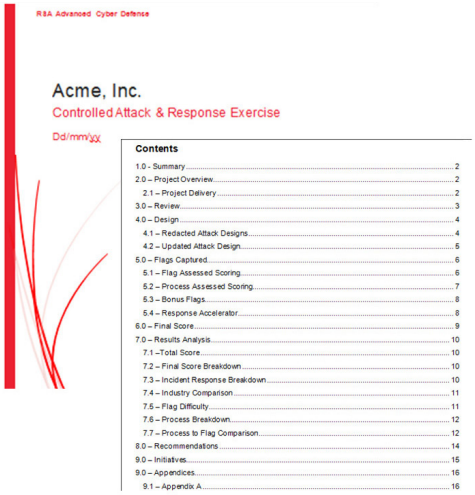
Cyber risk management

Reducing breach exposure

The business risks associated with cyber attacks have raised expectations with regard to incident re-sponse readiness. Organizations are increasingly being held to account to ensure that critical assets are being adequately protected. The emphasis for security practitioners has broadened from a tradi-tional focus on preventative measures. The scope has widened to include the detection of attacks as early as possible in the incident lifecycle. This can prevent an initial compromise from resulting in a larger breach.

The RSA Controlled Attack & Response Exercise pro-vides a number of benefits including:

- Objective benchmarking of the effectiveness of both the technical and operational functions for incident response.
- An end-to-end review of the incident manage-ment lifecycle, from initial triage to detection, remediation and response.
- Identification of strengths and priority areas for improvement to ensure that existing capabilities are being maximized.


RSA Advanced Cyber Defense

Acme, Inc.

Controlled Attack & Response Exercise

Dd/mm/yy

Contents

RSA controlled attack & response exercise

The Finding Report scores the technical and operational capabilities for Incident Response based on a “capture-the-flag” methodology.

The controlled attack addresses various threat elements such as phishing, command and control of predetermined host systems and ex-filtration of staged data. The engagement approach and remediation recommendations are represented in a Findings Report and Executive Presentation, with time and emphasis also given to knowledge transfer.

Engagement approach

Practicing for real-world scenarios

By testing current capabilities, the organization is able to determine how it would respond to a cyber attack and whether existing controls are being implemented to their fullest potential. The service delivery framework ensures that a highly consultative and interactive engagement is conducted:

- Review of EXISTING CAPABILITIES—this includes interviews, documentation review and observation of the current incident response process.
- Controlled Attack Design—one or more attacks are designed while ensuring that confidential data and production systems are not impacted.
- Controlled Attack Delivery—the attacks are conducted to ensure that the current technical and operational capabilities for incident response are rigorously tested.
- Findings Review—the scoring is reviewed to identify strengths and weaknesses, conduct knowledge transfer and prioritize areas for enhancing overall readiness for incident response.

Flags are set for various phases of the incident handling process, including Triage, Identification, Containment, Eradication and Remediation.

The scoring of results is based on the number of flags captured, the related difficulty level and the degree to which the incident response processes and procedures have been adhered to.

Bonus flags ensure that the exercise is also challenging for more mature incident response teams. As there is a narrow window of opportunity in preventing an initial compromise from resulting in a breach, multipliers are also used to reward accelerated response timelines.

With the RSA Controlled Attack & Response Exercise, incident response teams can obtain an objective measure of the effectiveness of the IR function, which helps ensure that scarce resources are being effectively allocated to protect critical assets.

Flags	Description	Difficulty	Pts	Flag Captured	Pts Awarded	Category	Attack
1	Recipient of email from E-Domain 2	Easy	1	Y	1	Triage	3
Attack #3 is the first identified attack							
2	Record Incident in SecOps	Easy	1	Y	1	Triage	3
3	Assign Priority	Medium	2	Y	2	Triage	3
4	Escalate To L2	Easy	1	Y	1	Triage	3
5	Communication	Easy	1	Y	1	Triage	3
6	Classified as Crisis (meets criteria)	Medium	2	N	0	Triage	3
7	Hostname of Host 3	Medium	2	N	0	Identification	3
8	Contained Host 3	Hard	3	N	0	Containment	3
9	Disabled Account (H3)	Easy	1	N	0	Containment	3
10	Removed Malware from Host 3	Hard	3	N	0	Eradication	3
11	Restored Host 3 to Production	Hard	3	N	0	Remediation	3
12	Identify W-domain 2	Medium	2	Y	2	Identification	2, 3

Technical controls and flag capture

Existing controls are reviewed and scored based on difficulty levels.

Flags	Description	Process	Pts	Category	Attack
1	Recipient of email from E-Domain 2	-	-	Triage	3
Attack #3 is the first identified attack					
2	Record Incident in SecOps	SOP - Creating Incident Manually	3	Triage	3
3	Assign Priority	SOP - Archer SecOps Alert	3	Triage	3
4	Escalate To L2	SOP - Escalate_Incident_from_L1_to_L2 Security Incident Management Process v1_0 20150519	2	Triage	3
5	Communication	Communication Process GSOC_023	3	Triage	3
6	Classified as Crisis (meets criteria)	Crisis Management Process GSOC_024	1	Triage	3
7	Hostname of Host 3	SOP - Network_Investigation_Guide	1	Identification	3
8	Contained Host 3	-	-	Containment	3
9	Disabled Account (H3)	-	-	Containment	3
10	Removed Malware from Host 3	-	-	Eradication	3
11	Restored Host 3 to Production	Security Incident Management Process v1_0 20150519	1	Remediation	3
12	Identify W-domain 2	Host Investigation Guide - Host Indicator V0.2	3	Identification	2, 3

Operational controls and flag capture

Existing processes and procedures are reviewed and scored based on the level of adherence to the prescribed IR plan.

About RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA award-winning products, organizations effectively detect, investigate and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud and cybercrime.

RSA Advanced Cyber Defense and Incident Response Practices are part of RSA Risk & Cybersecurity Practice. RSA Global Services organization also provides Professional Services in support of RSA product platforms, education services from RSA University and 24x7x365 product maintenance services from RSA Customer Support.

For more information, go to **rsa.com**.