RSA® STRATEGY & ROADMAP FOR TARGETED ATTACK DEFENSE

Set a new course for today's threat environment

EXECUTIVE SUMMARY

Common constraints and pitfalls

This service is for organizations needing protection against cyber attacks. It reviews business priorities, risks and gaps to assess a security program and delivers roadmap recommendations needed to meet key security objectives.

Organizations continue to invest in security but still struggle with attacks that take advantage of less mature capabilities covering the spectrum of People, Process and Technology.

Personnel related constraints typically include:

- Inadequate resourcing and lack of specialization
- Outdated skills and training

While controls may be in place for threat prevention, incident response (IR) maturity levels are often low, with:

- Ad hoc processes and procedures
- Delays patching critical vulnerabilities

Gaps are compounded by technology limitations, with:

- Manual incident management workflows
- Fragmented monitoring and alerting
- Lack of proactive hunting and forensics analysis tools
- Uncorrelated and ineffective management of cyber threat intelligence data

Organizations need to have the right control mechanisms. The white noise and false positives must be filtered out. The technical solutions must be finely tuned by parsing, analyzing and prioritizing data for actionable intelligence.

While prevention is important, increased weight needs to be given to detection and response. Security practitioners accept that attackers can gain an initial foothold in an organization, but also understand that with the right systems in place, early detection and rapid response can prevent the adversaries from achieving their objectives.

TAKE THE FIRST STEP

RSA Strategy & Roadmap Service

By reviewing the controls required for today's threat environment, gaps can be identified and remediated to reach the desired state for targeted attack defense.

Delivered by RSA's® Advanced Cyber Defense (ACD) practice, the Strategy & Roadmap for Targeted Attack Defense Service includes an assessment of current capabilities, the identification of gaps, the comparison of maturity levels with peers and the development of a prioritized remediation roadmap for technical and operational controls. In particular, this means helping organizations identify whether they are investing in the right areas, as well as helping them to pivot their investments to better address any deficiencies.

THE RSA APPROACH

Covering eight core domains

This service focuses on assessing a combination of traditional defense mechanisms, as well as additional countermeasures needed for targeted attack defense.

The resulting report focuses on eight core domains, each representing key control areas which are reviewed for maturity.

For example, if there is risk to the organization's intellectual property, it should be monitoring the related high value assets with greater emphasis. To accomplish this controls may include the use of a traditional SIEM, but higher levels of maturity would also require the use of non-signature and non-rule based monitoring systems. Network-centric controls should include the ability to identify and inspect sessions between internal IT assets and external domains.

The eight core domains are described below and facilitate the implementation of a more robust model for targeted attack defense.

RSA

1. BUSINESS ALIGNMENT

Protect the organizational mission

Right-sizing a security strategy requires consensus, support and an acknowledgement of the threat environment by senior management. Incident and breach response need to be regarded more as an organizational competency than an IT-centric or security function.

In parallel, the security team needs to be adequately resourced to ensure that critical assets and business objectives are being monitored and given the level of protection they require.

Gaps in the organizational commitment to resourcing the right strategy can put the security program on the wrong foot and set the wrong expectations for targeted attack defense.

Key areas reviewed include:

- Organizational commitment and resourcing
- Allocation of responsibilities
- Policies, standards and guidelines

2. RISK ALIGNMENT

Allocate Scarce Resources Efficiently

Risks need to be remediated based on their severity level and the potential impact to the organization. By conducting periodic risk assessments, specifically designed to identify sophisticated threat actors, the organization will be able to balance the investment in security controls against the harm to the business resulting from security failures.

While many organizations conduct routine risk assessments, they are often based on more traditional attack vectors and defense mechanisms, resulting in over-allocation of resources to preventive measures and under-resourcing of detection and response capabilities

Key areas reviewed include:

- Risk Assessment process
- High value assets and data classification
- Cross functional team coordination

8 domains for targeted attack defense

3. CONTENT INTELLIGENCE

The right data, from the right sources

Due to the high rate of compromise at organizations relying on SIEM-centric monitoring strategies, security teams are looking to get past the deficiencies of SIEM and often need guidance and direction for the right approach.

Key additional sources of data include network packet capture systems, which can be reviewed for indicators of targeted attack activity.

Further valuable information can be derived from host-based threat detection and response systems, where unauthorized software modules and libraries provide early indicators that the organization may have been compromised and that an attack is underway.

The combination of log, packet and host data provides a more comprehensive platform for accelerating detection and response. The addition of business context to this data also helps to categorize and prioritize incidents.

Key areas reviewed include:

- Alert aggregation and correlation
- Watchlists
- Managed Security Services

4. ANALYTIC INTELLIGENCE

Be the hunter

Since sophisticated threat actors tend not to trigger alerts, capabilities need to be in place for proactive anomaly detection at both the network and host level. Once suspect libraries and files are detected, they need to be analyzed in a safe manner, without posing risk to the rest of the organization while preserving the chain of custody.

Gaps in analytic detection capabilities remain some of the most significant barriers to targeted attack defense.

Key areas reviewed include:

- Proactive anomaly hunting
- Malware analysis
- Sandboxing and lab environment

5. THREAT INTELLIGENCE

Identify Attacker Tactics

Some attackers are very persistent in their efforts. Defensive countermeasures can include threat modeling and the enumeration of the tools and tactics used by the adversary, including domain and registrant names, IP addresses, file types, vulnerabilities exploited and related meta data.

Proactive techniques can be developed by harvesting attacker TTP's (Tools, Tactics and Procedures) from incident data, open source and subscription-based intelligence.

Key areas reviewed include:

- Threat modeling
- Vulnerability and patch management
- Open source threat research

6. INCIDENT RESPONSE OPERATIONS

Manage the incident lifecycle

The organization's Incident Response Policy should be supported with an Incident Response Plan, highlighting roles, responsibilities, service levels and required workflows. As an IT-centric function, this may differ from the Breach Response Plan, which requires broader cross-functional alignment with other stakeholders, such as within the lines-of-business, corporate communications, finance and legal.

While Incident Response tends to be an IT and security centric function, breach management needs to be regarded as more of an organizational competency, which in a breach situation need to work seamlessly together.

Key areas reviewed include:

- Roles and responsibilities
- Incident response planning
- Communications and Reporting

7. DEFENSE-IN-DEPTH

Leverage investments already made

Most organizations have built-up their portfolio of security solutions over time. It is important to take account of existing security controls and leverage investments already made.

A robust monitoring capability is built on a set of core security technologies including Firewall, Anti-virus, IDS/IPS (Intrusion Detection and Prevention Systems), e-mail and web gateway security, vulnerability and penetration testing. While many of these systems do not pose a barrier to more sophisticated actors, they do need to be in place for defense-in-depth and to mitigate more conventional threats.

Key areas reviewed include:

- Key security technologies
- Threat feeds
- Facilities and business continuity

8. REPORTING AND METRICS

Share metrics and performance data

Models such as VERIS (the Vocabulary for Event Recording and Incident Sharing) provide a basis for describing incidents in a structured and repeatable manner. This can be extended to include metrics for tracking the efficiency and effectiveness of the controls and to generate dashboards and reports for management consumption.

Key areas reviewed include:

- Maturity levels
- IR Metrics
- Dashboards and reporting

ENGAGEMENT AND DELIVERABLES

Findings Report and Presentation

During an engagement current capabilities are reviewed across the eight core domains just discussed. Gaps and remediation recommendations are documented in a Findings Report and accompanied by a presentation in which key findings are shared with the management team.

Key activities in the engagement include the following:

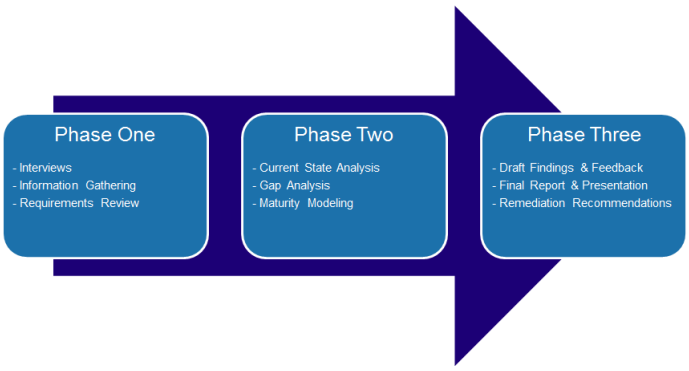
- Interactive and business-focused interviews addressing people, policy and process
- Technology review as key inputs to the Content, Analytic and Threat Intelligence domain analysis
- Security policies, standards, guidelines and related information
- Observation of current operational state for incident response and workflow management

While there is a strong emphasis on addressing the controls required for targeted attack defense, engagement activities also include a review of traditional defense-in-depth capabilities. This helps maximize investments already made, for example in SIEM which can be a valuable tool for detecting less sophisticated attacks and in helping to scope and extent of more sophisticated attacks.

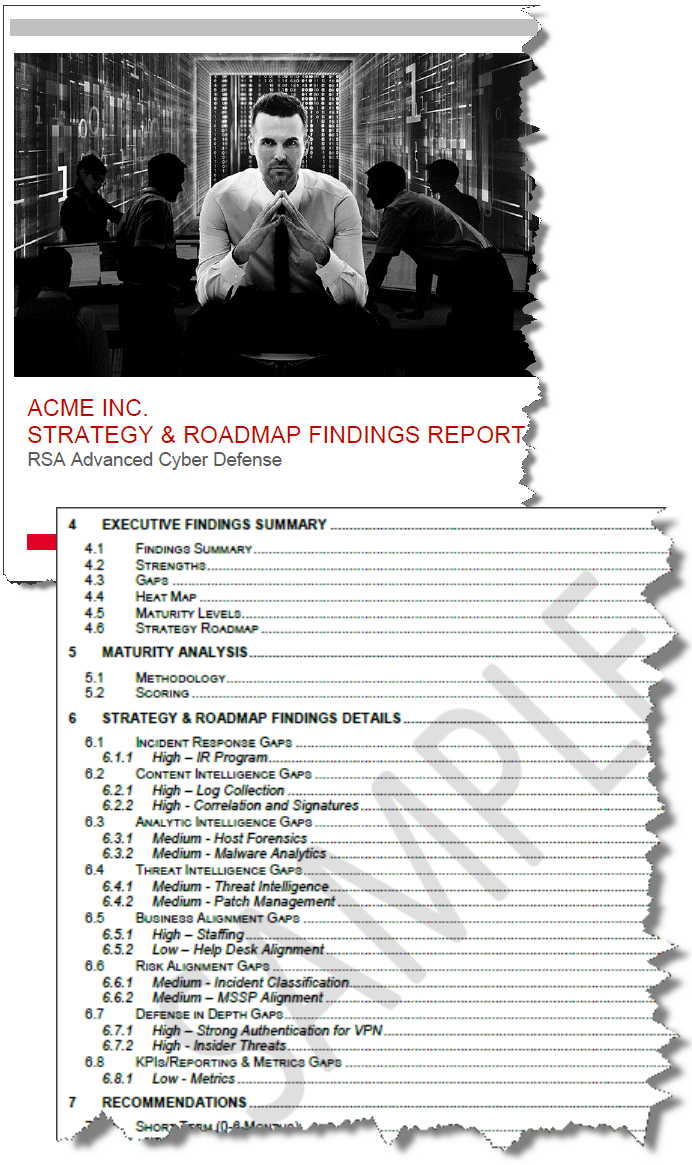
The approach of this service assumes that the attacker operates in stealth mode and is diligent at not triggering alerts. As a result, strong emphasis is placed on the review of capabilities for proactive hunting and advanced threat detection. Reducing exposure time helps prevent an incident from becoming a breach. While attackers may be able to gain an initial foothold there is a critical window of opportunity to prevent them from achieving their objectives.

The growth in the complexity of the threat environment is reflected in the trend towards outsourced security services. During the engagement consideration is given to the potential role of managed services providers and the degree to which it addresses the needs for targeted attack defense.

While many aspects of threat detection and response can be outsourced, breach management will continue to be an organizational responsibility. As outsourcing and cloud computing continues to grow a balance must be struck so that the organization retains visibility and control over the breach management process.



Phased Engagement Approach



Findings Report Table of Contents

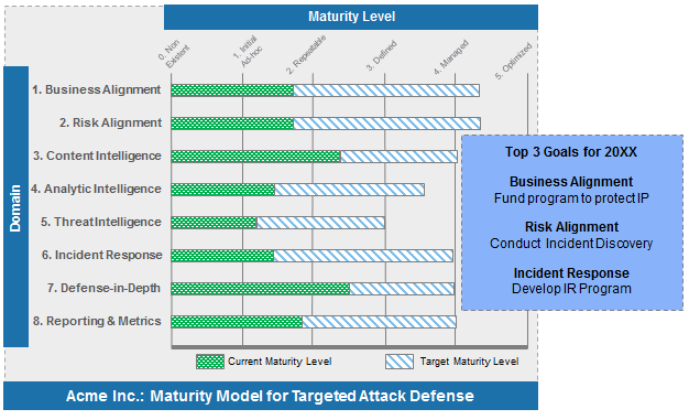
MATURITY SCORECARD

Current and target state analysis

Risk can be hard to measure and quantify, making it more difficult to prioritize the investment in mitigating controls. Such challenges can be addressed by adopting a more objective model to measure gaps and identify remediation requirements.

Security weaknesses can be mitigated by putting the right controls in place. A review of these controls, combined with a measurement of relative maturity levels (capability maturity modeling) enables the organization to represent their security strategy and gaps in a manner that can be shared more broadly across the organization. This promotes an understanding of the security strategy and drives consensus and better decision making.

Maturity levels can also be tracked over time so that targets can be set and measured.



Maturity Scorecard

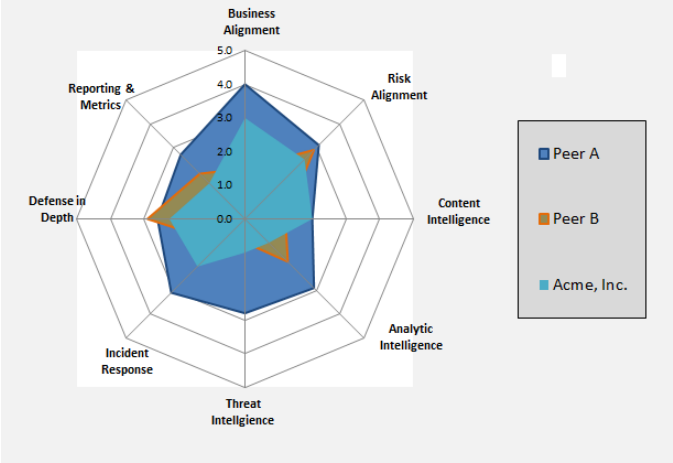
MATURITY BENCHMARKING

Comparison against peers

Budget constraints assure that investments are prioritized towards mitigating the risk levels associated with more important business initiatives. Risk elements may be both technical (e.g. systems criticality) and non-technical (e.g. brand protection and breach disclosure regulations).

As organizations struggle with a seemingly endless number of threats it can be difficult to quantify additional investment requirements. Benchmarking maturity levels against peers is a useful mechanism for communicating gaps to decision makers, helping them to identify opportunities for enhancing the security posture of the organization.

Key performance metrics are important to making good business decisions. Security managers face obstacles in trying to develop a coherent strategy because they are faced with unknown variables (such as zero day exploits), which are also required to calculate risk. Faced with such challenges, maturity modeling provides a basis for the development of metrics relating to the organizations security strategy in a format suitable for sharing with senior management.



Maturity Benchmarking

BENEFITS

Protecting the business

The benefits of RSA's Strategy & Roadmap for Targeted Attack Defense includes the alignment of risk management and business priorities. This ensures that scarce security resources are being allocated where they are needed most. By developing a holistic strategy, organizations can adopt a more proactive approach to security and protect sensitive information from getting into the wrong hands.

HOW WE DIFFER

Technical and Operational Expertise

RSA's ACD practice represents a team of professionals who have built and managed SOC's around the world, sharing resources and preferred practices with EMC's Critical Incident Response Center, protecting over 60,000 employees in over 100 countries. The ACD practice includes our Incident Response team which has worked with customers across industry verticals and specializes in technical forensic analysis for targeted attack defense and remediation.

INCIDENT DISCOVERY

Advanced threat detection

RSA also offers an Incident Discovery service, which closely complements this strategic security service and is delivered by our Incident Response team using RSA NetWitness® Packets and RSA NetWitness Endpoint to capture data and conduct a technical review of network and host systems to identify indicators of attack activity. The Incident Discovery Service helps organizations to find "the needle in the haystack" in complex systems environments.

LEARN MORE

RSA's portfolio of ACD services enables organizations to evolve from "being the hunted" to "be the hunter" and develop the strategies required to navigate the new terrain of targeted attacks.

For more information on the RSA's ACD capabilities, which are available on a global basis, please visit the web site https://www.rsa.com.

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's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. For more information, go to https://www.rsa.com.