SecurityScorecard

DATA SHEET

TITAN MAX

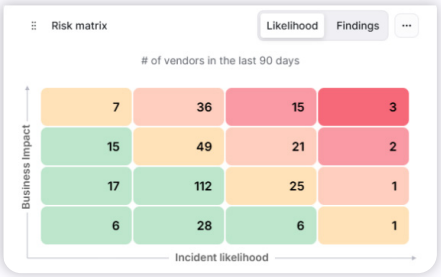
Managed Services for Cyber TPRM Outcomes

TITAN MAX is a TPRM force multiplier that injects people, process, and technology on behalf of customers.

Drawing on cyber risk management best practices from organizations such as NIST, MAX enables compliance, continuous cyber risk awareness, and focused risk reduction efforts for monitored vendors and organizations. This framework ensures that risk management teams can efficiently assess, monitor, and respond to risks across the entire vendor ecosystem.

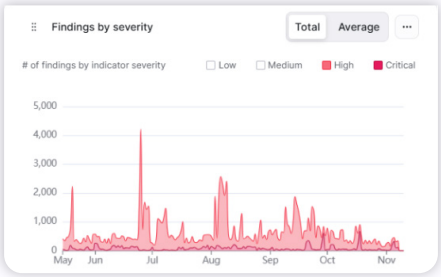
ASSESS

Identify gaps in a vendor's security program and the likelihood of the vendor encountering a serious cybersecurity incident



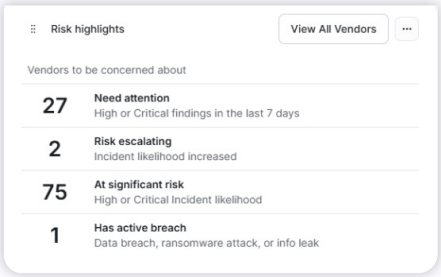
MONITOR

Leverage threat intelligence, trend data, and vendor attack surface assessments to gain a threat-informed and continuous view of third-party risks



RESPOND

Advise your teams and your vendors on how to enhance cybersecurity posture, reducing breach risks and preventing serious incidents



MAX Questionnaires

Meet compliance objectives with an augmented extension of your team

MAX Questionnaires is an end-to-end vendor cybersecurity questionnaire management service that evaluates a vendor's adherence to risk management standards. Questionnaire creation, distribution and response analysis is provided so that vendors can attest to the state of their security programs.

Deliverables	Questionnaires Ensure vendors meet risk management standards
Questionnaire design	✓
Questionnaire distribution	✓
Vendor questionnaire response support	✓
Vendor response analysis	✓
Documents gathering	✓
In-depth risk remediation recommendations	✓
Vendor risk assessment	✓
Consolidated findings report	✓

KEY DELIVERY SLAS

- Standard questionnaires are delivered within 48 hours of the customer request
- Vendor follow-up outreach occurs once and 72 hours after the initial outreach
- Questionnaire analysis is complete within one week of the vendor fully completing the questionnaire
- Quarterly reporting on vendor response progress and completion status

DELIVERABLE DEFINITIONS

Questionnaire design: Development of a SecurityScorecard platform questionnaire according to preferred security standards.

Questionnaire distribution: Questionnaire delivery, vendor progress reporting and follow-up for non-responsive vendors.

Vendor questionnaire response support: Assistance to vendors for completing questionnaires and setting up Trust Pages.

Vendor response analysis: Review of vendor attestations and validation using external security posture data from SecurityScorecard.

Documents gathering: Collection and validation of documents that act as evidence of the existence of required security policies or plans.

In-depth risk remediation recommendations: Tailored guidance for vendors that identifies control gaps and prioritized mitigation actions.

Vendor risk assessment: Vendor cybersecurity maturity analysis with an executive summary for stakeholders.

Consolidated findings report: Summary and analysis of an aggregated round of questionnaires sent to vendors.

MAX Monitor and MAX Respond

Drive proactive risk reduction with a threat-informed view of your supply chain risks

MAX Monitor and MAX Respond services provide a threat-informed view of risks within your supply chain. They identify the actionable insights needed to respond to changes in your supply chain risk exposure and deliver the resources to engage directly with vendors.

Deliverables	Monitor Arm in-house teams with actionable risk reduction insights	Respond Drive issue resolution without assigning in-house resources
MAX customer portal	✓	✓
Platform configuration	✓	✓
Incident likelihood assessments	✓	✓
Reactive findings reporting	✓	✓
Regular status reports	✓	✓
Vendor activation	✓	✓
Zero-day vulnerability exposure report	✓	✓
Vendor engagement		✓

KEY DELIVERY SLAS

- Incident likelihood assessments complete within 1 week of onboarding and quarterly afterwards
- Vendors onboarded within 48 hours of contact identification
- Findings report delivered within 8 hours of indicator detection
- Zero-day exposure delivered within 8 business hours of issue attribution for vendors in managed portfolios
- Vendor escalations initiated within 72 hours of trigger activity

DELIVERABLE DEFINITIONS

MAX customer portal: Dedicated SecurityScorecard platform site for reviewing supply chain risks and service delivery outcomes.

Platform configuration: Implementation and administration of the SecurityScorecard platform on behalf of the customer.

Incident likelihood assessments: Threat-informed analysis that identifies potential for security incidents and associated remediation plans.

Reactive findings reporting: Alerting of individual findings from continuously monitoring the customer's vendor ecosystem.

Regular status reports: Weekly and quarterly reporting of supply chain risk management program status and outcomes.

Vendor activation: Invitation of vendors to the SecurityScorecard platform to review their risk assessments and resolve their issues.

Zero-day vulnerability exposure report: Rapid identification of organizations impacted by high impact CVEs that are externally detectable.

Vendor engagement: Outreach, face-to-face discussions, and follow-up with vendors as part of proactive and reactive changes to risk exposures.