Purple Teams & Defense Metrics Programs

OBJECTIVES

- Operate a Purple Teams & Defense Metrics Program including attack simulations, content development and metrics
- Support decision-making for controls improvement and resources for NIST CSF Protect and Detect controls

OUTCOMES

- VECTR™ (vectr.io) platform for security test case management and Defense Metrics reporting
- Calendarized attack simulation events focused on defenses validation, improvement and Red/Blue knowledge-sharing
- Cumulative MITRE ATT&CK alignment and reporting
- Content development quick wins & custom content

SRA develops and publishes the free VECTR™ platform, the emerging industry standard for Purple and Red team documentation, metrics and content sharing.

PRICING

Test Cases	Cost	Duration
25	$25k	1 week
75	$75k	2 weeks
150	$130k	3 weeks

Content Dev
$300/hr

HIGH LEVEL ACTIVITES

1 Program Setup (one time)

- Establish goals, roles, attack sim process, and reporting procedures and deliverables
- Configure VECTR™ platform and first test cases

2 Attack Simulation Events (on cadence)

- Conduct pre-simulation workshop to set goals including mix of new test cases and repeat test cases (for showing improvements)
- Provide mix of Red and Blue leadership to guide simulations in a workshop format
- Identify and provide quick wins for content development

3 Reporting (on cadence)

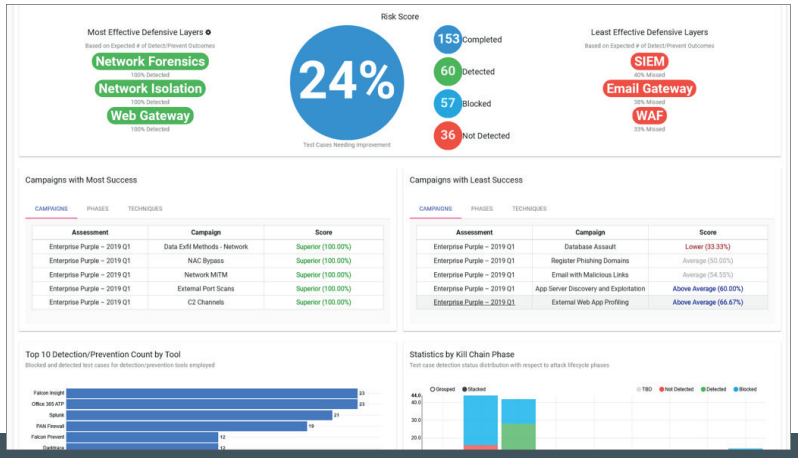
- Document cumulative defense success metrics and ATT&CK coverage
- Generate Engineering and Executive reports showing improvements, priorities and resource needs

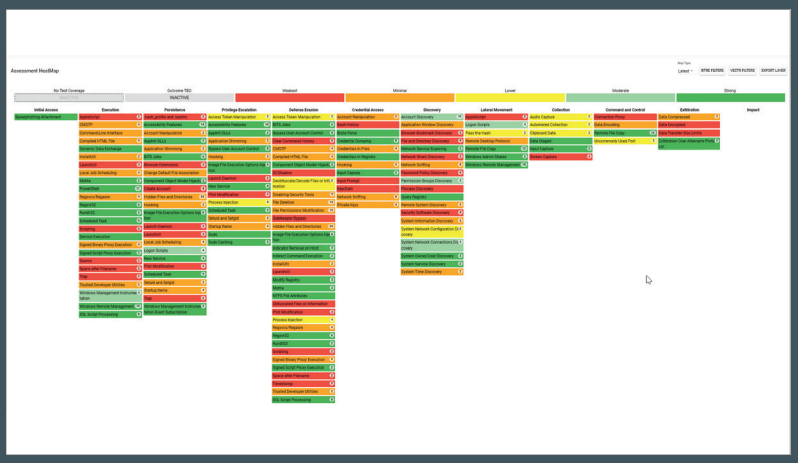
4 Content Development (on demand)

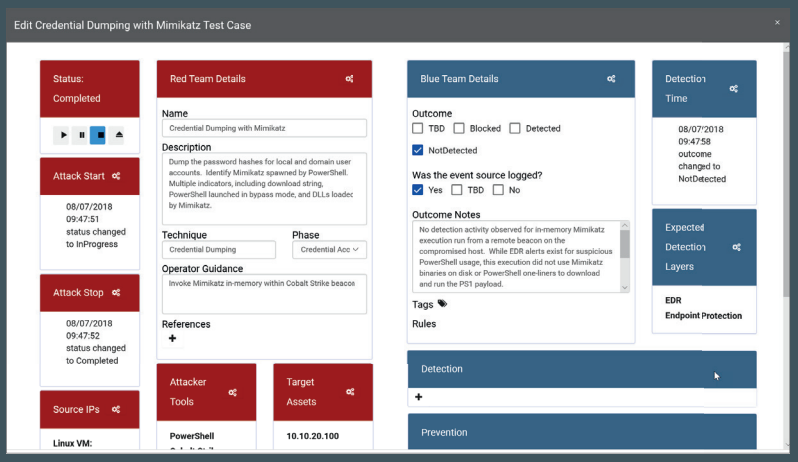
- Assist in engineering event source ingestion (if needed) and designing customized detection rules to augment your team and improve pace of remediation

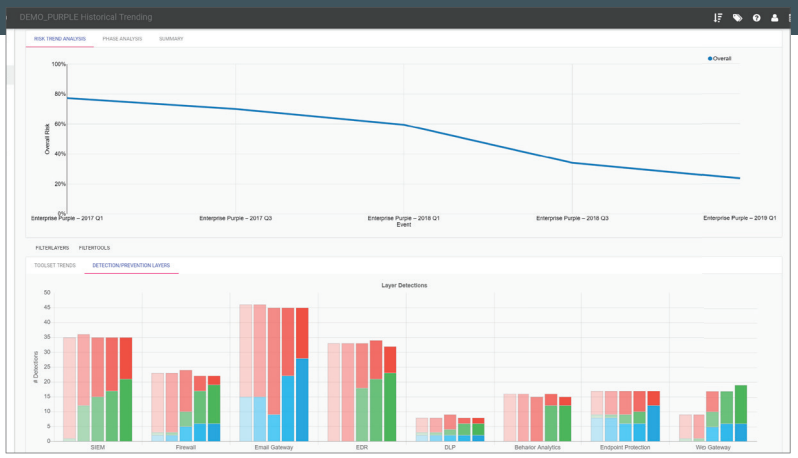
SecurityRisk ADVISORS

215.867.9051
info@securityriskadvisors.com
sra.io | vectr.io









VECTR

THREAT SIMULATION ◦ REPORTING & ANALYSIS

Collaborate.
Quantify.
Improve.

We believe in Purple Teams as the best way to assess and improve technical cybersecurity defenses.

Purple Teams through VECTR™ generates success defense metrics and helps align Red and Blue Teams towards the same mission: protecting the organization by discovering and plugging detection gaps. If you are scratching your head on how to adopt and align to the MITRE ATT&CK Framework, this is for you.

VECTR™ is the only free platform of its kind. It has STIX/TAXII functionality to support content updates and community sharing. VECTR™ is not available for purchase, it is available only as freeware.

VECTR™ Capabilities

- Document TTPs used in Purple and Red teams so test cases can be repeated until detection rules are made successful
- Light up a MITRE ATT&CK heatmap to show your teams' mutual success and needs
- Show how far you've come with historical trending of your metrics
- Evaluate and report the effectiveness of your tools investments
- Prioritize tuning and remediation activities
- Report defensive capability at each phase in the kill chain
- Import test cases using STIX 2.0 and TAXII

Reporting

VECTR™ offers detailed graphical reporting that will allow Analysts and Managers to drill down into successful attack methods, while also highlighting toolset performance and improvement over time at an Executive and Board level.

Learn more at **VECTR.io**
and download for free on our GitHub,
github.com/securityriskadvisors