Data Sheet

Attack Detective

SaaS for Advanced Threat Detection & Hunting

Attack Detective powered by SOC Prime Platform is the industry-first SaaS solution that connects real-time threat surface visibility and existing security data with Detection-as-Code content, MITRE ATT&CK®, and CTI to quickly identify and tackle cyber threats before they escalate. It provides real-time data and content audits for comprehensive threat visibility and improved detection coverage, equips security teams with low-noise and high-quality rules for alerting, and enables automated threat hunting.

Highlights

- **Fortify your SIEM Posture**
  - Run an automated content audit mapping your rules & queries to MITRE ATT&CK® to gain a comprehensive assessment of your detection coverage in real time
  - Automatically analyze log sources collected in your SIEM to eliminate existing blind spots with an actionable plan that maps data to MITRE ATT&CK
- **Enable High-Fidelity Alerting**
  - Enable low-noise, high-value alerting with detection rules set selected based on your SIEM posture audit
  - Reduce false positives (and negatives) rate
- **Automate Threat Hunting**
  - Quickly identify and tackle cyber threats before they escalate by delivering real-time, researched, and packaged threat hunting capability to your organization
  - Tune detections to perfectly match your threat hunting goals and tech stack in use

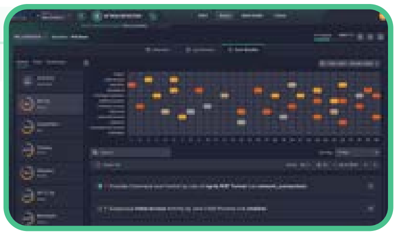
Content Audit

Improve threat visibility by automatically mapping your rules & queries to MITRE ATT&CK with AI that does not leak your code.

Data Audit

Address threat detection blind spots with an actionable plan generated by mapping the data collected in your SIEM to MITRE ATT&CK.

Rules for Alerting



Discover the best detection rules for your SIEM, seamlessly configure them and deploy to generate low-noise, high-value alerts

Threat Hunting

Act faster than attackers by automating routine threat hunting tasks, correlating findings with ATT&CK and the latest CTI.

Attack Detective Workflow

1 step

Content Audit

- Choose your Data Plane to enable Attack Detective to perform a Content Audit based on a dataset saved in a custom repo.
- Obtain the list of detections mapped to ATT&CK backed by AI recommendations on mapping improvement.
- Open and update the chosen rules using Uncoder AI to match your current security needs.
- Save updated detections to your custom repo or deploy directly to your SIEM, EDR, or Data Lake environment.

2 step

Data Audit

- Get automatically analyzed log data collected in your Data Planes to assess MITRE ATT&CK® coverage and identify potential cyber defense blind spots:
  - Attack Detective sends audit queries to your Data Plane (SIEM, EDR, or Data Lake) via API (with read-only privileges) to collect the aggregated statistics on the number of accounts and assets (without their values)
  - Attack Detective maps log sources to MITRE ATT&CK, identifies potential gaps according to its dictionaries, and chooses detection content relevant to your log data.
- Obtain an actionable plan to maximize threat visibility and address detection coverage gaps.

3 step

Scanning

- Scanning starts by querying your Data Plane via API (with read-only privileges) to determine log sources and events collected.
- Check if the needed fields are not empty, and count unique assets and accounts in the system.

Attack Detective Workflow

4 step

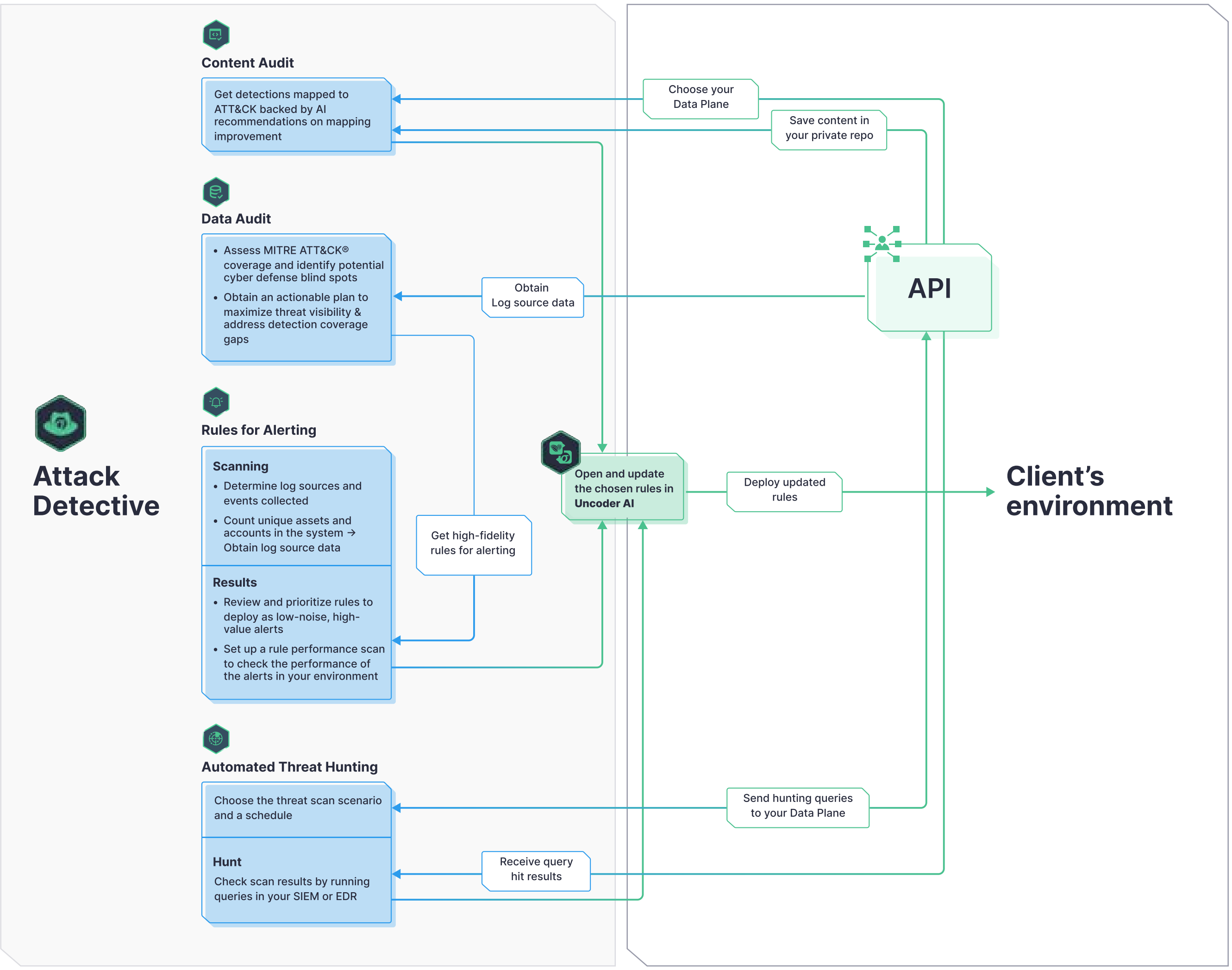
Rules for Alerting

- Obtain prioritized rules for high-fidelity alerting based on the scan results.
- Review and update chosen rules in Uncoder AI to match your current security needs.
- Save rules in your custom repo to make sure those rules are excluded from further threat scans since they are marked as verified alerts running in your environment.
- Set up a rule performance scan to check the performance of the alerts in your environment.

5 step

Automated Threat Hunting

- Choose the threat scan scenario and a schedule (a full scan is suggested by default). Run an actor-based threat scan to preempt attacks by specific adversaries most challenging your business.
- Attack Detective sends hunting queries to your Data Plane via API (with read-only privileges) to retrieve aggregated data on hits.
- To verify and further investigate any hit, launch hunting queries using the Hunt option. The queries are passed to the URL to instantly run in your SIEM, EDR, or Data Lake instance.
- Tune the chosen detections to perfectly match your threat hunting goals in Uncoder AI.
- Save and manage verified hunting queries in your custom repo to have all Detection-as-Code projects at hand and in sync.


Attack Detective
Client's environment
API
Choose your Data Plane
Save content in your private repo
Obtain Log source data
Get high-fidelity rules for alerting
Deploy updated rules
Send hunting queries to your Data Plane
Receive query hit results
Open and update the chosen rules in Uncoder AI

Content Audit

Get detections mapped to ATT&CK backed by AI recommendations on mapping improvement

Data Audit

- Assess MITRE ATT&CK® coverage and identify potential cyber defense blind spots
- Obtain an actionable plan to maximize threat visibility & address detection coverage gaps

Rules for Alerting

Scanning

- Determine log sources and events collected
- Count unique assets and accounts in the system → Obtain log source data

Results

- Review and prioritize rules to deploy as low-noise, high-value alerts
- Set up a rule performance scan to check the performance of the alerts in your environment

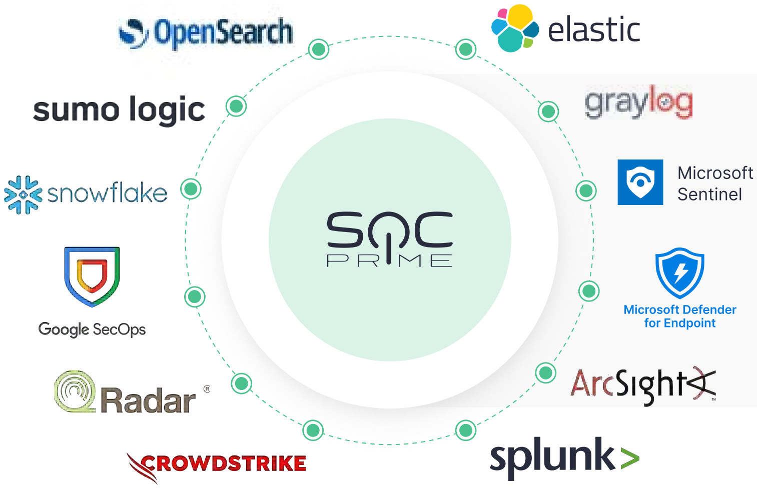
Automated Threat Hunting

Choose the threat scan scenario and a schedule

Hunt

Check scan results by running queries in your SIEM or EDR

Figure 1. Attack Detective Workflow



Supported Technologies

Attack Detective connects industry-leading SIEM, EDR, and Data Lake solutions in a single place to maximize threat visibility, eliminate blind spots in your defense, and prioritize risk reduction within your environment.

Privacy

SOC Prime infrastructure is SOC 2 Type II certified, which ensures that appropriate access restrictions to the databases for the infrastructure administrators are in place.

Attack Detective stores only aggregated information about the triggered rules, like hit count grouped by 1-hour bins and unique hashes (SHA256) for usernames and hostnames to show asset and account counts in the triggered queries. No SIEM log source data is collected or stored in Attack Detective.

To protect user data and handle privacy challenges, Attack Detective sticks to the following best security practices:

- **Read-only access to your data**
- **Keeping the data where it lives**
- **Microservice-based architecture**
- **Amazon AWS hosting**
- **Retrieved data are encrypted at rest in AES-256**
- **Data is transferred via a secure HTTPS channel, TLS v1.2**