ATAR®

RESPONSE ORCHESTRATION
& AUTOMATION
REDEFINED

atarlabs

Attacks Are Automated
Why Aren't Defenses?

State of Cyber Security Operations Today

ATAR Labs has been founded by a group of industry professionals who have been working in the SOC space for more than a decade. We have spent the last several years observing the consistent rise in attack speed and volumes while we, as defenders, started lagging behind.

ATAR Labs breaks down the challenges of a modern SOC into five distinct, but strongly interrelated areas:

Attack Speed

Attacks keep getting faster everyday. Modern attacks are almost entirely automated. By using purpose built malware, attackers can get in, do malice and get out of an organizational network in less than 15 minutes. We cannot even start an investigation in the same 15 minutes let alone stop it.

Lack of KPIs & Metrics

As most SOCs lack the practice of investigation and response, it is almost impossible to come up with relevant, easy-to-collect KPIs and metrics. Getting a grip on who needs more training, SLA adherence, incident backlog trends, etc. is difficult and intuitive-only.

No Single Pane of Glass

Most SOCs consolide alerts on a SIEM and manage all incidents on a an IT service desk software. There is no trail of investigation and response activities and there isn't a proper answer to "who is working on which case and doing what" at any point in time on the SOC floor.

Attack Volume

An average organization would get more than 300 cyber alerts per day (IDC). Investigating and responding to an alert would take around 8 full hours. Most SOCs do not have that much human resource to investigate and respond to every single alert.

Disparate Tools

SOC analysts use 15, up to 20 different tools throughout their daily jobs to investigate and respond to attack alerts. Not only do they need to know these tools inside out, but they also need admin privileges to be able to run them. SOCs do not embrace the idea of trusting admin passwords in the hands of junior analysts, hence the two-tier model of today; Tier-1 analysts are not able to investigate (and use the tools) and they are merely expensive human filters.

To conclude, it is not only the attack speed and volume that are hurting us, but also the lack of a unified investigations and response platform.

Automated Threat Analysis and Response (ATAR®) is a cyber security investigations and response platform.

ATAR® for Security Operations

Automate
Repetitive Activities

ATAR® features a full blown automation engine. Using the ATAR® robot, one can define arbitrary automation scenarios. Typically, SOCs generate investigation and response of their most frequent alerts, treating them according to the completely robotized playbooks. ATAR®'s rich library of integrations allows automated playbooks to fetch data, look up intelligence and even interrogate endpoints before running one or more actions designed to block or contain ongoing incidents.

Measure
KPIs and Metrics

As all incident investigation and response activities are conducted from the ATAR® platform, ATAR® collects metrics from everything happening on the platform. Incident backlog trends are collected among them (if it's the case to hire more resources or repurpose some of the existing ones), as well as SLA adherence, analyst case distribution and trends and analyst activity trends. ATAR® features some 25 ready-made dashlets showing different KPIs on dashboards. Feeding video walls with SOC data has never been easier.

Improve
Analyst Efficiency

ATAR®'s unified investigations interface allows service desk like case management features. With just one click of a button, analysts can use the interface - invoke data/evidence collection and actions, without even logging in and out of individual tools, greatly decreasing the total time required for investigations and response. This interface also builds an incident timeline which can help an entire team of analysts working on the same case, through building an interactive history of whatever modification has been done on the subject.

ATAR® can help improve the agility and efficiency of the modern SOC.

Automating
Repetitive Activities

When a new hire arrives at the SOC, (s)he is given playbooks describing what to do in the occurency of a particular type of incident. Playbooks defines a precise list of activities along with preconditions resembling a flowchart.

SOCs consolidate detection activities on a SIEM; all alerts from other detection systems are generally consolidated on the SIEM. Additional SIEM works as a detection system itself through analysys of the collected logs and traffic. Incidents do occur on other channels as well, channels such as as e-mails, phone calls, etc., but a great majority comes through alerts generated by the SIEM in charge. ATAR can also receive and manage alerts coming from systems not connected

Automate the bulky part

If one tallies up all the incidents handled at a SOC by monthly frequency, the top-5 most frequently reported incident types account for 50% of all the incidents that happened during the mentioned timeframe. Keeping this in mind, ATAR®'s goal is to automate the most frequent 3-5 playbooks if possible, offloading 30-40% of all incidents to automation.

Semi-automation is possible

When full automation is not possible because the SOC needs human intelligence for certain analysys, etc., defining semi-automation with ATAR® still stands. When a particular incident is triggered, ATAR® can start an automated investigation, collect some data, some evidence and can even stop there, when handing the case over to an analyst. Automation can still help, even when you can not fully automate a playbook.

Approve critical actions

ATAR® has ready-made integrations with over 85 different technologies from some 20+ different IT vendors. These integrations allow ATAR® to reach out to different platforms and collect additional data and evidence, as well as connect to a particular device to change configurations or take specific actions. In this respect, ATAR® allows Software Defined Security; it is possible to change security posture by triggering certain automation playbooks.

Technology integrations

ATAR® automation can be completely autonomous, running a playbook from end to end. When full automation is not desirable, ATAR® has an option to ask for approvals before critical activities. For example, ATAR® can run an investigation in a mostly automated manner, but would ask for approvals before blocking a particular IP address on the border firewall. Most SOCs start using the ATAR® automation with as many approval points, but they remove such approvals as soon as they start building their confidence in the automated playbooks.

Improving
Analyst Efficiency

Using ATAR® automation, SOCs observe that 30-40% of their incidents have been taken care of. Still, there is a large volume of attacks to be investigated, lacking response from analysts in a SOC. ATAR® provides an investigations console and several associated tools to help analysts streamline their work and handle incidents far more efficiently.

ATAR® delivers a specialized service desk for incident investigations. SIEMs, other technological sources, analysts can create incidents on ATAR®. Using dispatch rules, SOCs can direct incidents to specific analysts based on roles, groups, shifts, etc. ATAR® comes with a pack of functions meant to improve analyst efficiency by using automation in various forms.

Speed up investigations

When using the ATAR® service desk, analysts can see their assigned incidents, with all the details, SLAs, including the incident timeline, among others. ATAR®'s interface works as an investigation cockpit; ATAR®'s main functionality lies in the set of buttons on the user interface. Therefore, without switching between applications and logging on and off, analysts can click certain buttons, making ATAR® fetch in additional data or evidence, and they can even trigger counteractions with the click of one single button. These one click data collection and counteractions speed up investigation 10 to 15-fold.

Foster collaborations

Incident timeline is particularly important, as it allows collaborative investigations. When one analyst either hands over the incident to a colleague or asks his team to jump in, incident timeline steps in as activity coordinator. As all the investigative activities are listed along with all the data collected in chronological order, the incident timeline allows collaborative work.

Optimize Available Skillsets

Most SOCs employ more Tier-1 and less Tier-2 analysts. In most cases, Tier-1 analysts are nothing more than expensive human filters; they review the alert and only and uniquely try to eliminate false positives. Empowering Tier-1s would have been possible if there wouldn't be any risk of them causing faults. Giving them admin access to Active Directory or the border firewall for their investigation would only be advised if the risks of them making a mistake and crashing the whole infrastructure could be prevented.

ATAR® addresses this problem and allows Tier-1s to handle a bigger portion of investigative activities. The one-click evidence collection and one-click action buttons seem to ease the technical complexity of a particular activity; the junior analyst could look up particular data on a particular system by hitting only one button, without necessarily knowing how the system looks under the hood. Such abstraction of investigative data requests and the technical data gathering mechanisms, combined with extremely strong and granular access control, allows Tier-1s to do a lot of investigative activities without any risk of wrongdoings and perhaps typos. Such junior analyst activities can still handle action approvals by device owners.

Measure
KPIs and Metrics

In many SOC settings today, the activities taking place during an investigation are not logged and it is impossible to keep a trail of previous actions, whatever the results and timings. When such critical information is missing, it is almost impossible to collect detailed metrics on the investigation processes, hence come up with essential KPIs. This does not only adversely impact the SOC governance, but it also leads to consequences for auditability.

Metrics collection

All activities done by ATAR® automation and the analysts using the ATAR® interface are logged at all times. Such trail of activities are used for metrics collections. A typical SOC can answer the following questions with ease:

- Are we able to hit our SLAs?
- What is the breakdown of incident types that we analyze?
- Can we see the analyst's workload distribution in real time?
- Is our incident backlog growing or shrinking?

ATAR® collects these answers and many others responding to 20+ other questions key indicators and allows them to be shown on operational dashboards.

Dashboards and video walls

ATAR® comes with a pre-package of 25 different dashlets visualizing different aspects of SOCs distilled in metrics. These dashlets can be mixed and matched to build multiple different dashboards; a SOC analyst can see his or her stats, whereas a SOC Manager can see the big picture of things.

ATAR® comes with a pre-package of 25 different dashlets visualizing different aspects of SOCs distilled in metrics. These dashlets can be mixed and matched to build multiple different dashboards; a SOC analyst can see his or her stats, whereas a SOC Manager can see the big picture of things.

Simplify Audits

ATAR® stores all investigation activities, collected data and artifacts (e.g. malware samples) in its database. Auditors love ATAR®, as there is a complete history for all incident investigations, even for the ongoing ones.

An internal or 3rd party auditor can randomly pick a group of incidents, only to find a perfect review: how did the incident occur, who handled the triage, who was in charge of the investigation or how long did every single individual activity take. Individual accountability has never been so easy in SOCs.

ATAR®
Business Value

ATAR® helps SOCs become, more vigilant, measurable and auditable by assisting them, from several different, but interrelated angles:

ATAR® helps SOCs **investigate and respond faster**

Using playbook automation a lot of repetitive activities can be handed off to ATAR® automation; this means that 30 to 40% of all incidents are responded at machine speed.

One-click evidence collection and one-click actions allow analysts to investigate and respond 10 to 15 times faster. The net result is the significant growth in incident response.

ATAR® helps SOCs **offload repetitive activities**

Use of ATAR® helps your analysts focused on importanr cases and work in the SOC, instead of entangling them in repetitive mundane tasks. This does not only increase rates for SLAs, but more importantly, it increases job satisfaction for SOC analysts. Analysts are happier when work challenges their engineering curiosity; the life span of an analyst in a SOC cumulates to only 1-1.5 years of work. Take them off the mundane tasks and let them focus on real investigations which stir curiosity, leading to satisfaction and a longer life span in this line of work.

ATAR® helps SOCs **decrease costs**

Use of ATAR® helps analysts achieve more; SOCs can do more with less resources. ATAR® does not only help decrease the total number of analysts handling the investigation workload, but it also enables Tier-1 analysts to do more work. Than can explain the obvious shift from employment of more expensive and hardly found Tier-2s, to cheaper and easier Tier-1s. Overall, ATAR® improves SOCs costs efficiency, while ensuring no single incident is missed.

About
ATAR Labs®

ATAR Labs® builds next generation Cyber Security Operations Center (CSOC) platforms. Our flagship product ATAR® helps CSOC teams improve their efficiency in responding to cyber attacks using various and diverse forms of automation. ATAR® also helps SOC managers better govern their business by providing insight and accountability to SOC processes.

ATAR®
Awards

2017 **TechAnkara** Ankara Development Agency
Best Project of the Year

2016 **IT Architecture Awards**
Best Datacenter Project of the Year

2016 **TOBB StartupIstanbul**
2nd Best Startup Company

ATAR®
Integrations

(80+ Today)

Today's attacks are automated. Why aren't defenses?

www.**atarlabs**.io

info@atarlabs.io

atar_labs

atarlabs