

A business case for OpenText SOAR



Contents

Cybersecurity today	3
What is OpenText SOAR?	3
OpenText SOAR adds value to security teams	4
Summary	6



Cybersecurity today

Cyberattacks are increasingly the No. 1 source of risk for all enterprises; every organization tries to ensure all attacks are defeated and the crown jewels are protected. Insider and external attackers are successfully stealing data, tampering with databases, forcing and stopping the execution of critical services. These attackers might be individual, organized crime syndicates, competing corporations, and even nation states.

Enterprises in all sectors are spending a lot to secure their data, computing environment, and services from such attacks. However, this is increasingly becoming a serious challenge for several reasons:

- **Attacks are super fast now.** Attackers use malicious software to attack which explains why we see attacks getting in, doing some harm and getting out in 15-20 minutes today.
- **Organizations are getting hundreds of cyber alerts a day.** Several hundreds of attack alerts a day are typical, if not more, and investigating and responding to all of these is impossible.
- **Existing security tools are not working together.** This lack of cooperation results in poor overall protection.
- **There are never enough cyber experts on the team.** In order to operate regardless of the security technologies we have, we always need more people.

Due to this, cybersecurity is increasingly being observed as an *unconquerable* problem. Attackers are having the upper hand and the situation is only getting worse. OpenText SOAR is here to change that.

What is OpenText SOAR?

A Security Orchestration, Automation, and Response platform, OpenText SOAR allows anything repetitive in the day-to-day security operations to be automated and provides a single unified pane of glass for all security team members to work on cybersecurity incidents.

By providing a unified operations environment OpenText SOAR allows security teams to be more agile and efficient and to defend their organizations. And OpenText SOAR is built so it will keep working even if you change security tools or add new ones.

By collecting more data, consolidation and understanding the root cause, OpenText SOAR can reveal whether an alert is genuine or false.

OpenText SOAR adds value to security teams

Below you will find four of OpenText SOAR's biggest benefits.

Automating alert triage and consolidation

OpenText SOAR can automatically prioritize which alerts are more important than others; sorting all alerts in priority order. This helps organizations to always start with the most important alert and carry on over to less important ones.

It can also analyze the alerts based on the organization's rules and consolidate multiple independent alerts into a smaller number of consolidated cyber incidents to investigate. This decreases the total volume of work for security operators significantly.

“Our manual alert triage is now mostly automated, requiring 90% less human resources, we’ll be reaching 95% soon. Also, in a typical day, [OpenText SOAR] consolidates 1,000 alerts into 250 cyber incidents. A 95% reduction on cyber incident cases to investigate decreases our efforts dramatically.”

Telco CISO

Eliminating false alerts

Security tools are not foolproof; we often receive false alerts. OpenText SOAR can eliminate such false alerts by automatically collecting additional data from systems and/or reaching out to employees and asking questions. By collecting more data, consolidation, and understanding the root cause, OpenText SOAR can reveal whether the alert is genuine or false.

“Since we started using [OpenText] SOAR, we put a special emphasis to eliminating false alerts. Today, in a typical month, [OpenText] SOAR eliminates some 60-70% of all false positives. In this way it saves us 1.6 full time employee effort per month.”

Bank CISO

OpenText SOAR can automatically collect all data and evidence an operator needs, even before the operator starts working on the case.

Automating alert investigation and response

If the investigation and response to a particular type of attack alert can be presented as instructions to a newly joining security staff member, it is possible to automate most (if not all) of those steps. This can help security teams offload whatever is repetitive, allowing them to focus on more complex issues.

“We automated the investigation and response processes of most of the monthly top-10 frequent alerts. Most are fully automated where some are still involving a security operator to confirm sensitive actions like taking a computer off the network. During the course of a full year, [OpenText] SOAR automation saved us 9.5 full-time employee effort.”

CIO of Government Agency

Increasing productivity

During an investigation, the security operator uses multiple tools. OpenText SOAR unifies all these different tools by providing a unified command and control interface.

This interface allows operators to do far more in less time. This greatly increases the productivity of the security operator.

OpenText SOAR can automatically collect all data and evidence an operator needs, even before the operator starts working on the case, saving a lot of precious time and allowing the operator to focus on resolution, not gathering data.

“We have very few security operators. [OpenText] SOAR’s unified command and control interface allows them to investigate more cases per day. We ramped up from 8–10 investigation cases a day to 100–120 a day; a 12x increase in operator productivity.”

Bank CISO

OpenText SOAR is a security operations platform that combines every security tool under one unified umbrella, helps them work in tandem, and helps your employees achieve far more to defend your organization.

Summary

Cybersecurity is a complex problem and attackers are far ahead of us. We need automation and automated assistance to scale our limited expertise and connect the dots among our independently operating security tools.

OpenText SOAR is a security operations platform that combines every security tool under one unified umbrella, helps them work in tandem, and helps your people achieve far more to defend your organization.

It provides a lot of additional benefits, such as driving down training costs for security operators, decreasing the ramp-up time to enable a new hire in sensitive day-to-day security operations, and reducing the risk of security operator mistakes and misbehavior.