Torq and OX Security

Integrate to automate AppSec triage and slash mean time to remediation

Business Challenge

Security teams face an unsustainable ratio of alerts to analysts. Vulnerability scanners generate massive volumes of risks across the software supply chain, but findings often arrive without the operational context needed to act. Critical flaws languish in backlogs while analysts manually hunt for code owners or struggle to assess business impact. Manual triage can't keep pace with modern development, and disconnected security operations and engineering workflows turn fixable risks into persistent vulnerabilities that block production.

Solution

Torq + OX Security eliminates remediation bottlenecks by merging application security with hyperautomation. OX validates critical risks across the SDLC using reachability and exploitability scoring to filter noise. Torq instantly triggers workflows that prioritize incidents, correlate with SOC data, and route remediation context directly to code owners — bridging the gap between AppSec detection and engineering action.

Value

With Torq and OX Security working together, AppSec moves from manual triage to automated orchestration. Alerts arrive validated through reachability and exploitability analysis, enriched with repository details, commit history, and root cause context. Remediation flows seamlessly to the right developer through existing channels — whether via Slack, Microsoft Teams, or Jira.

This approach reduces analyst fatigue by filtering out noise before it reaches the SOC, ensuring teams only work on validated, exploitable risks. It also accelerates remediation by routing findings with full context directly to the code owner who can fix them. Most importantly, it unifies security operations and AppSec, breaking down silos so findings flow from code repositories into operational workflows at machine speed.

Torq + OX Benefits

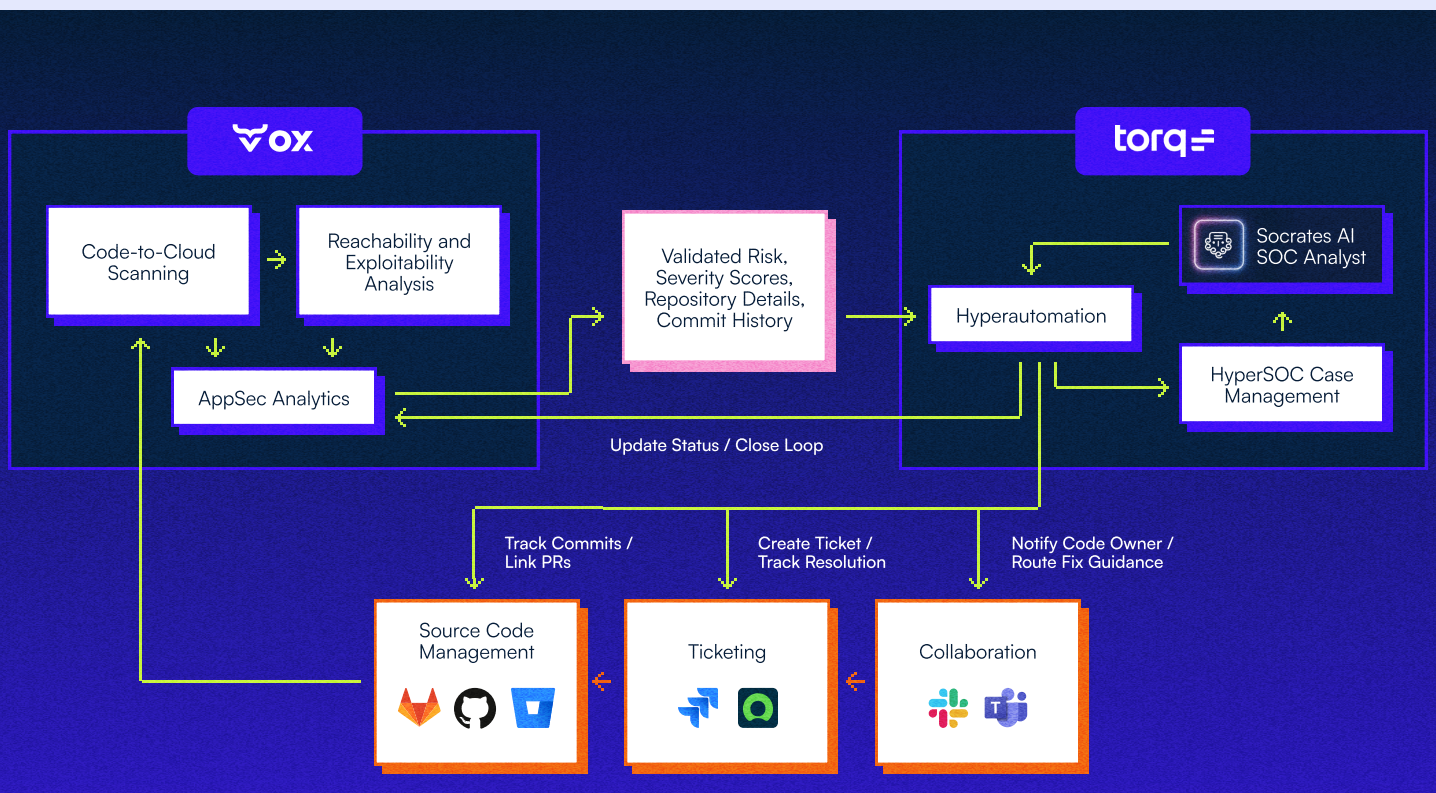
01. **Slash mean time to remediation**
Validated OX findings trigger Torq workflows instantly, turning detection into automated action and eliminating manual handoffs.

02. **Context-rich prioritization**
OX's reachability and exploitability scoring filters noise, so Torq workflows only fire on real, actionable risk.

03. **Automated code owner routing**
Torq identifies the responsible developer and delivers remediation context directly to them via Slack, Teams, or Jira.

04. **Reduced analyst fatigue**
Validated risk signals replace raw alert volumes, freeing analysts to focus on higher-value investigations.

05. **Unified AppSec and SecOps**
Findings flow seamlessly from code repositories into SOC workflows, treating AppSec alerts with runtime-level urgency.



How it Works

OX Security continuously identifies critical security risks across the SDLC, applying reachability and exploitability scoring to validate real, actionable threats and filter out noise. Torq periodically polls OX for new validated findings matching specific risk policies, pulling in deep context including repository, commit history, and the vulnerability's root cause.

Torq ingests the findings, automatically triages them with HyperAgents and Socrates, and prioritizes incidents based on OX's severity signals while correlating with broader SOC data. From there, Torq identifies the code owner and orchestrates remediation — routing findings directly to developers via Slack, Microsoft Teams, or Jira with full remediation guidance.

Finally, Torq closes the loop by tracking resolution status, ensuring validated risks are not only identified but fully remediated at machine speed.

Torq + OX Use Cases

Automated triage & prioritization

Torq polls OX for validated critical risks and automatically creates and prioritizes tickets in Jira or ServiceNow, eliminating manual sorting.

Direct-to-developer remediation

Torq routes OX findings with full remediation context directly to the responsible developer via Slack or Teams, removing the security team as a bottleneck.

Unified security operations

Automated handoffs between detection and response break down SOC and AppSec silos, slashing MTTR by treating AppSec alerts with runtime-level urgency.

About OX Security

OX Security is a code-to-cloud application security platform that provides complete visibility across the software supply chain. Using reachability and exploitability analysis, it validates real risk across the SDLC — filtering noise so security teams can focus on threats that actually matter. OX bridges AppSec and DevOps by delivering prioritized, actionable findings with full remediation context.

For more information, visit ox.security.

About Torq

Torq is the autonomous SecOps platform transforming how enterprises manage risk. Using adaptive agentic reasoning and automation, Torq identifies, prioritizes, and remediates critical threats at machine speed, slashing MTTI and MTTR while amplifying productivity. Global leaders like PepsiCo, Procter & Gamble, Siemens, Telefónica, and Virgin Atlantic trust Torq to power the next generation of AI-driven security operations.

For more information, visit torq.io.