OTRS Spotlight: Corporate Security 2024

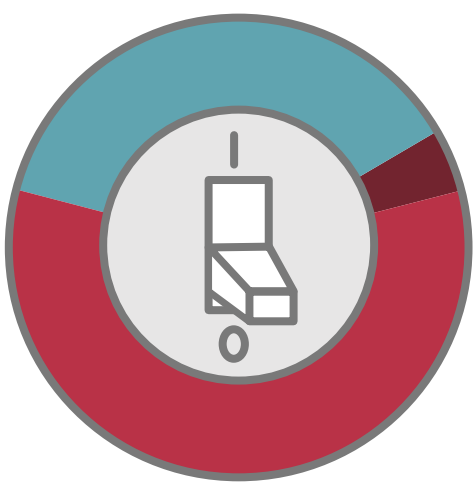
Part 1: The CrowdStrike Aftermath

93 %

After the CrowdStrike incident, 93 % of the companies surveyed increased their security precautions.

- **45 %** diversified their IT and software landscape to be less dependent on a single software provider.
- **40 %** implemented advanced real-time monitoring and alerting systems.
- **39 %** introduced additional testing for new patches and updates.
- **39 %** implemented or updated their incident response plan.
- **36 %** implemented or updated their disaster recovery and backup plans.
- **26 %** switched to staged/phased rollouts for patches and updates.
- **24 %** implemented Unified Endpoint Management (UEM).
- **17 %** disabled automatic updates for all of their software.
- **4 %** did not take any action and **3 %** don't know.

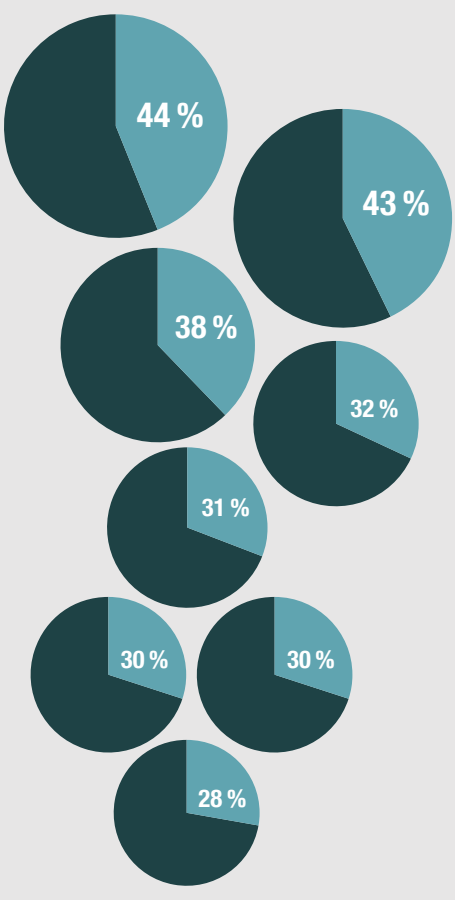
While not all organizations were directly affected by the CrowdStrike incident, it was a wake-up call for most to step up their IT security game.



Were any of the systems in your organization affected by the IT outage caused by the defective update rolled out by CrowdStrike in July 2024?

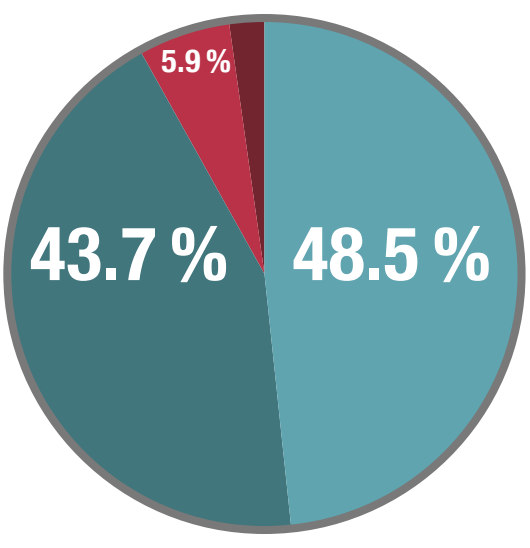
- **58.2 %** Yes.
- **37.4 %** No.
- **4.4 %** I don't know.

Only a few of those directly affected were prepared to mitigate the impact of the CrowdStrike incident using their own resources.



- **44 %** followed the **remediation steps as outlined by CrowdStrike** as soon as they were available.
- **43 %** installed the **fix deployed by CrowdStrike** as soon as it was available.
- **38 %** use **advanced real-time monitoring and alerting systems**, which enabled them to quickly intervene.
- **32 %** have robust **rollback mechanisms, disaster recovery and backups** in place in place which allowed them to quickly revert their systems to a stable version.
- **31 %** use **Unified Endpoint Management,** which allowed them to quickly identify affected systems and initiate appropriate measures to mitigate the impact (remotely).
- **30 %** have a **robust incident response plan** in place that helped them quickly identify, isolate and resolve the issue.
- **30 %** generally do **pre-deployment testing for new patches and updates**, which allowed them to detect the defect and to quickly intervene.
- **28 %** generally do **staged/phased rollouts**, which meant only a few systems were affected by the incident.

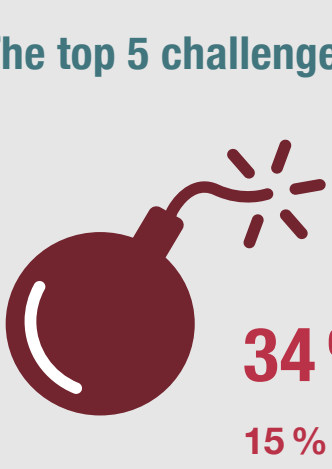
A feast for attackers: Half of all security teams do not deem their organization optimally prepared for security incidents.



How well prepared is your company in the event of a security incident?

- **48.5 %** Optimally.
- **43.7 %** Acceptably.
- **5.9 %** Not sufficiently.
- **1.9 %** I don't know.

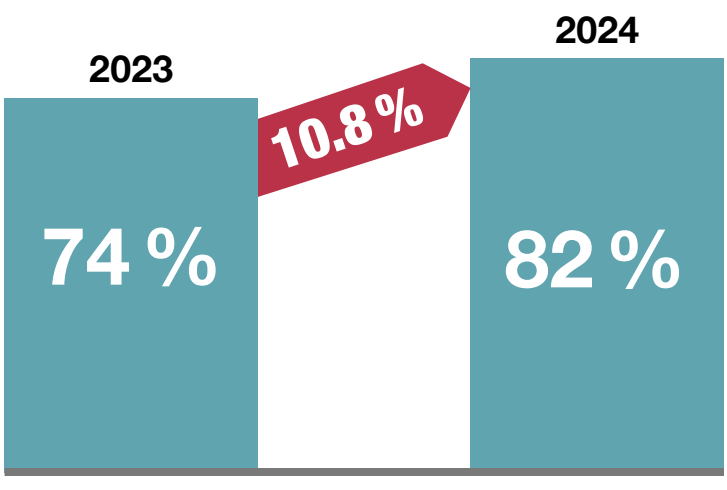
The top 5 challenges security teams face during incident response:



34 % Rapidly evolving threats

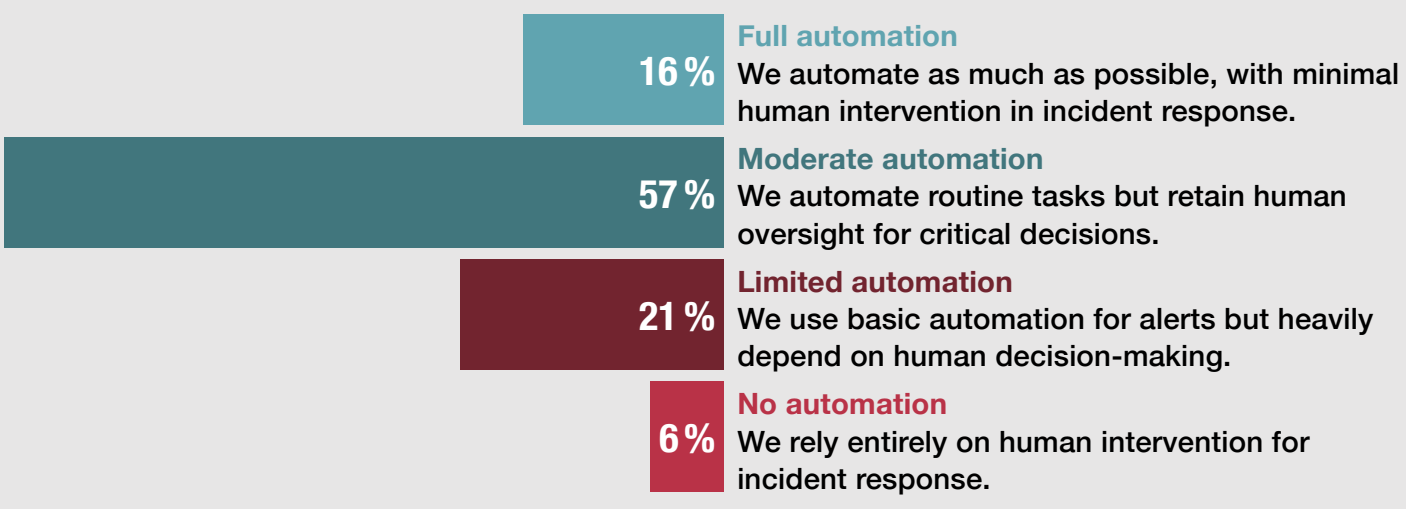
- **15 %** Conducting comprehensive post-incident reviews
- **12 %** Lack of skilled personnel
- **12 %** Timely and appropriate communication with the public
- **12 %** Lack of integration between tools

The number of security incidents increases every year, making it difficult for security teams to keep up with the attackers.



"Yes, we have seen an increase in security incidents."

By automating their incident response processes, security teams stand a better chance to keep pace with rapidly evolving threats.



The data used is based on an online survey conducted by Pollfish Inc. on behalf of OTRS AG, in which 476 IT und cyber security professionals in the U.S., Germany, Brazil, Mexico, Australia and Malaysia participated between August 22 and September 17, 2024. Unless otherwise indicated, all figures refer to the average of all countries surveyed.

OTRS