binalyze!

The Future of Incident Response: **Are You Ready?**

In cybersecurity, the saying goes that it's not if but rather when a company will suffer a breach or cyber attack. A robust Incident Response (IR) plan and strategy are among the most critical factors in ensuring your organization is ready in case of a devastating event.

Once a breach is discovered or an attack is launched against an organization, your IR team will have its plan to put into action – but it can still be an overwhelming and stressful process to manage and ultimately recover from.

In today's modern context, the future of IR is no longer confined only to the IR team. As we will outline in this whitepaper, the future of IR is all about collective understanding, visibility, buy-in, and collaboration throughout the team and the broader organization.

Whether it's the front-line SOC analyst investigating an alert or the incident responder handling an escalated incident, the team should be trained and ready BEFORE an event occurs. They critically also need the right solutions in place so that they're fully prepared.

Typical IR plans and strategies that rely on traditional technologies are no longer sufficient to stand up to the rapidly evolving needs of an organization, especially one that is under attack or has been breached.

Consider these important figures:

277 days
is the time required to contain a data breach and has remained the same for years.[1]

67% of businesses
suffer repeat cyber attacks within 12 months after the first data breach.[2]

It takes 26 days
to investigate a breach once detected and another 17.1 days for resolution.[3]

81% of SOC analysts
have experienced increasing workloads in the past year.[4]

1 Ponemon, Cost of a Breach 2023
2 CPO magazine, 2022
3 The State of Digital Forensics and Incident Response, IDC August 2023
4 Voice of the SOC Analyst 2023, Tines Report

This window of vulnerability, compromise, and time to respond has remained excessively long.

It is time for a new way of approaching IR. The future of IR requires a next-gen solution that features automation and collaboration at its core. Here's why each component is essential.

Automation

By implementing effective automated incident response solutions, you can drastically reduce the time to investigate and stay in control 24/7. There are two facets to automation - integrating with existing alerting systems to help trigger an investigation and reducing manual and error-prone tasks.

Automation can also streamline typical investigation processes, such as collection and analysis. By deploying a fast and powerful IR solution to your assets, you can expect:

- A solution that makes the incident response process faster and more efficient without compromising accuracy.
- Out-of-the-box, automated incident response solutions deliver essential benefits like:
- Fast response time to cyber incidents
- Reduced dwell times
- Reduces time spent on false positives and alerts
- Less manual work and processes
- Streamlined operations and workflows
- Security operations that are easier to manage at scale
- Fewer budget challenges

Collaboration

A collaborative response to incidents reduces investigation gaps and removes silos, so that teams can better work together. Unified insights within a shared workspace bring global and remote teams into the same space, using a consistent approach, to better understand the situation and conduct their investigations.

A Holistic Approach to Incident Response is a Modern Approach

A holistic, comprehensive incident response strategy includes people, processes, and technology and incorporates these elements.

Forensics and Digital Investigation Visibility:

Incorporate digital forensics capabilities and approaches for in-depth analysis of incidents. While traditional detection and monitoring solutions used in the Security Operations Center (SOC) - including EDR, SIEM, XDR - offer alert-level investigation capability, Incident Responders often require a deeper level of investigation capability and visibility.

In addition, response today needs to be more than a reactive, post-mortem collection of information after an incident. Integrating an investigation and response solution that offers a forensic approach can complement existing prevention and detection capabilities. While traditionally, DFIR tools had limitations for cybersecurity; the newer generation integrates automation, collaboration, and broad coverage to expedite evidence collection and analysis.

Incident Detection and Triage:

Detection and triage are critical aspects of a response workflow. Next-gen investigation and response solutions use automation to develop advanced forensic analysis techniques and methods that are faster, more comprehensive, and adaptable to evolving threats, bridging the gap between incident detection and response.

Automation can also be used to streamline and scale triage across digital assets to accelerate response times, as well as enable proactive, scheduled triage to reduce a lot of repetitive, manual work and make informed decisions faster.

Orchestration and Workflow:

Security orchestration, automation and response (SOAR) offers significant benefits by automating and coordinating response to cyber threats, improving efficiency, and reducing response times. When integrated with threat intelligence and digital forensic solutions, its effectiveness is further enhanced, providing deeper insights and comprehensive visibility into security incidents. This integration not only streamlines the incident response process but also enriches the analysis, aiding in more accurate and rapid decision-making in SOC and incident response investigations.

In addition, case management, investigation workflows and collaborative features found in comprehensive investigation platforms aid with streamlining the cross-team processes and empower teams to work together through an investigation.

Integration of Threat Intelligence:

Threat intelligence is essential to keep pace with the threat landscape. Intelligence informed automatic evidence analysis helps to spot anomalies and find indicators of compromise (IOCs). Intelligence should be integrated through feeds and ongoing detection development.

Decision-making and situational awareness are aided by insights provided by up-to-date detection and rule development. A platform that offers the ability to share and leverage community rules that the entire team can use, as well as verdicts and scoring provides context that can help investigators prioritize what to do next in their investigation, particularly when looking at hundreds or thousands of potential digital assets.

Incident Reporting and Documentation:

Incident documentation for post-incident analysis and regulatory compliance is a critical step in the incident response lifecycle. This is traditionally a very manual process that is not aided by the sprawl of tools used to investigate.

In addition to the effort required for consolidating relevant information, not all reporting needs are the same, so teams have to build different versions of reports and account for different audience needs. Using automated reporting tools helps to generate comprehensive incident reports that conveys information needed to different technical and non-technical audiences.

The power of working remotely

Remote capabilities remove the need to be reliant on resource-heavy/costly physical manual work and travel. This is important in today's ever expanding digital environment.

This is particularly important in hostile environments, where travel or resources are prohibitively challenging, or when assets are geographically dispersed with the teams responsible being thousands of miles away.

Remote working with the right solution can also bring collaboration benefits since everyone can access the investigations and share their input

Consolidation of tools

If everyone involved in an investigation is relying on different tools, processes, and methodologies, it creates friction, gaps and siloes. It also hinders the ability to perform comprehensive response. It's impossible to realize efficiencies if you can't aggregate data and tools onto a single pane of glass. It's about working in a way that's unified, not disparate.

By enabling cross-platform, you can also move beyond the need for specialist capabilities for specific platforms and instead work with a common feature-set across the team.

This directly enables more investigation capabilities down the chain.

DFIR professionals are using **11-15 paid or open sources** tools for investigation [1]

A third of SOC analysts use over 30! [2]

Why Investigation and Response Automation is Essential

Automation and collaboration are critical to solving many of the challenges organizations face when it comes to security. Particularly among a growing skills shortage in the field. Research from (ISC)2 finds that the number of security professionals needs to increase by 65% to protect the critical assets of organizations worldwide effectively.

1 The State of Digital Forensics and Incident Response, IDC August 2023
2 Voice of the SOC Analyst 2023, Tines Report

To meet this demand, 2.7 million professionals are needed. However, the skills gap the industry faces makes that difficult, as 44% of cyber professionals say the skills gap has only increased in recent years, according to joint research by the Information Systems Security Association (ISSA) and Enterprise Strategy Group (ESG).

Through automated IR, most of the repetitive manual work of forensic investigations is eliminated and made more accessible, so humans can be given more mission-critical tasks and can focus on other things. Consider these key benefits of automated response investigations.

Speed and Efficiency

Automated incident response capabilities enhance speed and efficiency in handling security incidents. Security leaders know the number one priority is understanding and containing a threat quickly, and the challenge is balancing these needs with a holistic approach to visibility and investigation.

Automated IR helps teams enhance the operational tempo, remove time spent on manual and repetitive tasks, and focus on finding "unknown" unknowns, uncovering hidden threat, and speeding up incident response.

Consistency

Consistency is a cornerstone of effective incident response procedures and teamwork. Automating investigation and response ensures a uniform execution of predefined actions, eliminating oversights and providing a standardized approach to incident handling.

This consistency is essential to enhance the reliability of the results and build a robust defense against cyber threats.

Standardization

Automation can enforce standard procedures, ensuring that all steps are followed correctly and in the proper order. This can be particularly important for legal proceedings, where the collection and handling of evidence may be scrutinized.

Scalability

As networks and digital ecosystems grow and become more complex, the amount of data to be analyzed for forensic purposes increases exponentially. Automation can help handle these larger data volumes without the need for proportionate increases in human resources.

As threats become more sophisticated, the need for scalable solutions is essential.

Reduced human error

People are not perfect and do make mistakes, especially when tired, working with large amounts of data, or when under strict time pressure. Automated processes can help minimize the chance of human error in critical forensic-level tasks.

Working through an investigation end-to-end, from the start point all the way through to reporting and stakeholder communications, using traditional DFIR and security tools takes several days, weeks or months. Next-gen solutions allow you to condense the process of collecting forensic evidence into mere minutes, analyzingthe collected evidence rapidly with clear signposting as to where to focus attention, and cutting down manual work, empowering investigators to move swiftly to close investigations.

Automated Incident Response (AIR) is the Future of IR

A modern IR strategy requires an agile, scalable, remote, automated solution that easily integrates into other security platforms. Binalyze AIR is an investigation and incident response automation platform powered by DFIR. It drives investigation at speed whilst optimizing your existing team's efforts - leveling up your capabilities.

AIR provides:

- Full forensic-level visibility across platforms, including cloud
- Consolidated insights in a unified easy to use interface
- Remote and scalable data acquisition, triage & analysis
- End-to-end investigation capabilities
- Integration with existing security investments
- Intelligence-led automated analysis

Learn how Binalyze can bring your IR strategy into the future with advanced digital forensics and incident response solutions tailored to meet the demands of today's threat landscape.

binalyze!

To find out more about our next-gen solution, visit us at Binalyze.com or start your free 14-day trial today.

Visit us at www.binalyze.com

Binalyze OÜ
Harju maakond, Tallinn,
Kesklinna linnaosa, Hobujaama
tn 4, 10151, Estonia