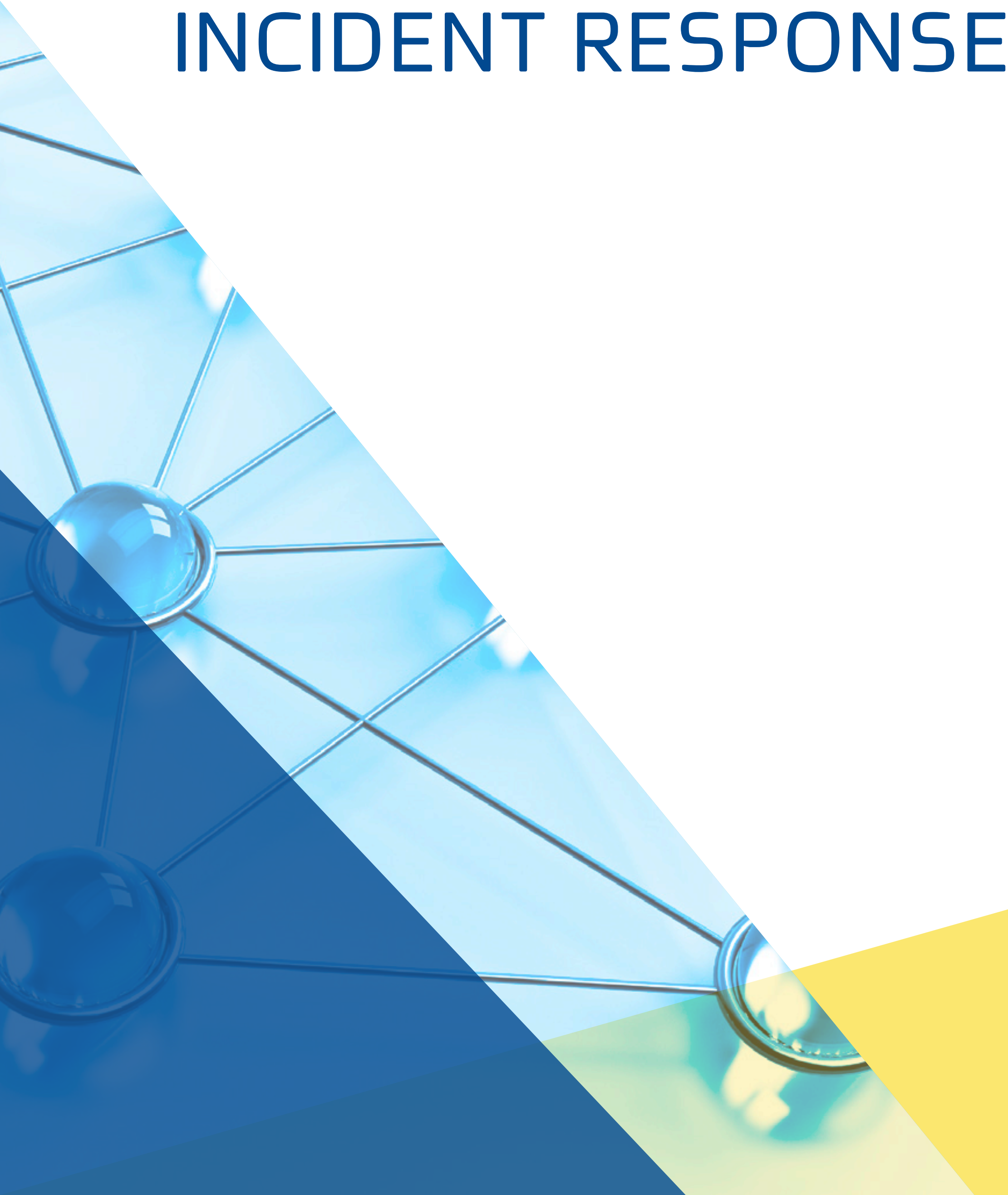
CYBERBIT
PROTECTING A NEW DIMENSION

5 WAYS
OF EMPOWERING YOUR INCIDENT RESPONSE TEAM



WHITE PAPER

Empower Your People

Incident response has never been so complicated. The amount of information, people, processes, procedures, policies, regulations, systems and teams involved assure that not only the complexity of threats is on the rise, but that the amount of actions and measures for containment are growing.

This means that it's not easy for your incident response team to be on top of things. You need them to be focused, and accurate, so that they don't miss out anything, and have the means to respond to the threats they encounter.

Incident response teams should be focused on one thing - mitigating and responding to your network's cyber threats and incidents. They should not be bothered with irrelevant information and distractions, and they should not be kept busy with details of procedures that are required as part of a policy and not as a means to accelerate the response. They need to be able to provide you with the best network protection possible.

In order to assure your cyber incident response team yields the maximum and produces the best results, here are five things you can do, which will empower your team and allow it to skyrocket:

Have them separate the wheat from the chaff

so many things to be done and so little time... this is why you want to assure your team only deals with what is important - the essence of how to secure your network and respond to cyber threats and incidents. You don't want them bothered about important yet mechanical tasks of reporting to management, sending event summaries and documenting every action done by writing it down. You want them to be free of worrying and checking whether the procedures were fully followed, and highlight them with what is most important and urgent. And of-course you want any one of these tasks to be automated. Wherever possible, whenever possible. Clear their path wherever you can.

Clear the path of your incident response team wherever you can, whenever you can

Keep an updated and knowledgeable team

your team needs to be updated. Updated as to what's going on in the SOC when they're around, what went around the SOC when they were away, and what intelligence information exists that might affect your organization. Being fully updated allows your team to analyze faster, understand better, and respond more accurately to cyber incidents and threats. Keeping your team updated is not an easy task - apart from providing them with the tools and mechanisms to receive the information, you need to assure updating is part of your everyday processes and shift tasks, so that your team members know this is not merely an optional task, but rather an integral part of your SOC operations. You will shortly discover your SOC leaped forward and is now better and sharper.

SOC situational awareness

provide you and your team with an overview of the organizational cyber domain. This will allow you and them to have a full picture of your SOC operations and missions. They can investigate this data to discover trends and directions that will provide them with a better understanding of the challenges, threats and incidents they're dealing with. Not only that, but you will also receive a better understanding of your current cyber domain and of how to better allocate your resources to deal with your missions and challenges. The ability to overview the organizational cyber domain is critical to gain a profound understanding of what threats and challenges you face, and is part of being updated as to what is going on in your SOC. This understanding allows your team to grow and develop.

Don't rest on your laurels

keep improving - your processes, procedures and policies. Investigate. Conduct post-incident analysis. This is the best way to learn and improve - understand where your weaknesses are, and where are your strengths. See what needs to be changed and what you could improve - based on measurements, audits, and KPIs. Only by post-incident investigation can you make the most of each handled incident. You can understand how your organizational procedures are carried out, review the SLAs and time-to-response, and verify that the process was carried out efficiently. Be sure to conduct post-event analysis and investigation not only on major cyber incidents, but also on minor ones on a weekly basis - so that you maintain an improvement cycle and implement lessons learned for constant refinement.

Be sure to conduct post-event analysis and investigation not only on major cyber incidents, but also on minor ones

Impose order on the chaos

assure your team's desktops are neat and clean - without too many screens and systems open all at once. This way you avoid unnecessary distractions that will bring noise into your operators' and analysts' surroundings and attract their attention. The less screens and systems your team has to deal with, the more attention they can give to every single incident and case. The more you aggregate and collaborate all the necessary information into one central system - you free your team's attention and allocate it to where you need it the most without any disturbances and unwanted attractions.

Stay on top of your cyber operations - implement an incident response platform

What it all means is that you need your team to be focused, updated, have easy access to all incident and threat information, and you want to automate as much of the processes as possible to assist in decision making and assure your organizational procedures and best practices are being followed.

The best way of doing this is by implementing one central system to consolidate everything you know and do in one place - an incident response platform.

An incident response platform saves you and your team's time, focus and energy. It allows you to focus on what really is important, and not on the margins and accompanying bureaucracy of incident response procedures. A good incident response platform facilitates:

1. **Automation of processes and procedures -** to save time wherever possible and allow your team to focus on the essence and not waste time on bureaucratic and mechanical tasks.
2. **Support for the decision making process -** with decision support modules that provide recommendations to the operators and analysts on what to do next while dealing with a cyber incident - allowing you to map your procedures and best practices into the system.
3. **Intelligence driven security -** combining intelligence information with network information to deliver best SOC results
4. **Post-incident investigation and analysis -** that allows you to follow up on your SLAs, KPIs and actual actions done in the mitigation and response process by reviewing the documentation, audit trail, reports and measurements - allowing you to learn and conclude from every single incident handled.
5. **Constant improvement-** of your processes, tasks, and procedures - by allowing you to overview any information in the form of retrieving specific events or by reports and investigative BI data that allows you to draw conclusions and learn lessons of your procedures and tasks.
6. **Work with one main console -** operating as the hub of the SOC - collaborating and aggregating all information from all systems to one central console, from which response measures can also be conducted.

1 Automation of processes and procedures

2 Support for the decision making process

3 Intelligence driven security

4 Post-incident investigation and analysis

5 Constant improvement

6 Work with one main console

By implementing an incident response platform your team is free to focus on what really matters - mitigating and responding to cyber threats quickly, accurately and effectively.

CYBERBIT
PROTECTING A NEW DIMENSION

CyberShield MnR - Mitigation and Response

CyberShield MnR is CYBERBIT's incident response platform - designed to facilitate organizations with quick and effective mitigation and response to cyber threats, based on informative decisions and actions. CyberShield MnR has automated capabilities that provide you with as much relevant information as possible for carrying out response actions so that you can minimize the required timeframes to provide the most accurate and knowledgeable response and mitigation measures. CyberShiled MnR main benefits include:

- Decision support (automatic)
- Linking to similar past events (automatic)
- Situational awareness and reports (automatic)
- Threat intelligence collaboration
- One centralized console for SOC operations
- Post incident investigation capabilities
- Tools for improving SOC procedures and processes
- Shift management
- Export of events and incidents to mail, word or pdf by one click

CYBERBIT Ltd.
Hamachshev 2, Netanya 4250712, Israel
Tel: 972-9-8864525, Fax: 972-9-8864556
www.cyberbitc.com | sales@cyberbitc.com

CYBERBIT
PROTECTING A NEW DIMENSION

About CYBERBIT

CYBERBIT is a fully owned subsidiary of Elbit Systems Ltd. - Israel's largest defense company. Marking the cyber and intelligence domains as strategic growth engines - Elbit founded CYBERBIT to lead its activities in these domains and be the spearhead of intelligence and cyber solutions worldwide.

CYBERBIT's solutions span the full range of intelligence and cyber technologies and capabilities, allowing its customers to receive either local or end-to-end solutions to the challenges and needs of their organizations, leveraging the technology, knowledge and methodologies gained by years of experience with high-end customers around the world.

CYBERBIT's leading cyber security solutions, constituting CyberShield suite, provide advanced malware detection and mitigation across multiple types of IT and SCADA networks - aimed to DETECT, ANALYSE and RESPOND to cyber threats:

- **CyberShield MnR (Mitigation and Response) -** cyber incident response platform for shortening event handling time and improving efficiency and accuracy of the response process while applying best practices and informed decision making
- **CyberShield AnD (Analysis and Detection) for IT -** for identifying anomalies across the networks and detecting advanced threats by using behavioral analysis and context-rich detection algorithms
- **CyberShield AnD (Analysis and Detection) for SCADA -** for visibility, discovery and security of critical infrastructure networks
- **CyberShield TnS (Training and Simulation) -** for simulating attack scenarios and security breaches in a stand-alone environment in order to train cyber security professionals and decision makers on responding to cyber breaches and threats

Get in touch with us to see how we can help you empower your cyber incident response team and improve your SOC efficiency.

Visit www.cyberbitc.com
or contact us at sales@cyberbitc.com

CYBERBIT Ltd.
Hamachshev 2, Netanya 4250712, Israel
Tel: 972-9-8864525, Fax: 972-9-8864556
www.cyberbitc.com | sales@cyberbitc.com