Break Glass if Needed: The Work-From-Home SOC

Maintain Resiliency with Your WFH SOC

A work from home SOC is not optimal, it's for emergency use only.

As organizations establish work-from-home initiatives, maintaining business continuity and productivity is critical. Security is key to the success of this transition. In fact, it's more than important than ever, given the current global pandemic. Cybercriminals will take advantage of any (perceived) weakness, as they have done recently by creating phishing campaigns pretending to come from the Centers for Disease Control or the World Health Organization.

There are many things organizations can do to ensure employees stay healthy and safe while also maintaining resiliency. Central to this is making sure the organization keeps running securely, particularly when it comes to the security operations center (SOC). How do companies remain resilient during these times? It's time to look at the work-from-home SOC.

Apply Automation to Reduce Reliance on Personnel

Automation and reducing reliance on personnel is a crucial aspect of maintaining an effective security operation in a time of crisis. If manpower must be limited, investment in automation should be accelerated. Automating your SOC can reduce staffing needs and give you comfort in knowing that your business is being monitored at all times. This is invaluable when members of your SOC team are unable to work, be it for health, family or other reasons. Migration to the cloud, whether SaaS or IaaS solutions, has also reduced the need for people to be in a data center and physically manage systems.

In security operations, the main bottleneck has always been the limitations of human nature; that is, no matter how intelligent human security analysts are, they will never get better or faster at monitoring vast quantities of security log data and alerts that an organization's sensors are producing today. Automation is a valuable tool that addresses this disconnect.

A SOC's operational processes are intentionally formally structured, regular and repeatable. The vast majority of today's SOCs, then, are built according to patterns that are highly responsive to automation. You can automate tasks that are difficult or impossible for human brains to manage, such as correlating an IP address associated with an alert with a sequence of events that took place on another part of the network two weeks ago.

Not only is implementing automation practical from a staffing perspective, it also means you can ensure that your team members are able to focus on more interesting and fulfilling activities or projects, such as threat hunting versus staring and monitoring a console for hours at a time. If automation can analyze and triage security data better than humans can, SOC analysts are less likely to get burned out. Automation, then, decreases the chance of errors and employee turnover. This ultimately helps your company stay resilient, even during difficult times.

Originally published in Security Boulevard. March 25, 2020https://securityboulevard.com/2020/03/moving-to-a-new-reality-the-work-from-home-soc/

We built the Respond Analyst for just this purpose - to operate like human experts 24x7 with the ability to investigate high volumes of alerts and determine if something is a false positive or critical incident that needs immediate attention and response. Our product is easy to get started - no content creation, playbooks or coding required - and can be a great part of a business continuity strategy to provide augmented security triage when people are scarce. And, we can give you an army of experienced "virtual" analysts at a fraction of the cost, whether you outsource to an MSSP or hire in-house.

Implement the Right Staffing and Communications Plans for Your SOC Employees

While the right communications plan is always important, organizations are quickly adapting to the current immediacy of work-from-home scenarios.

A good plan includes:

- Making sure the appropriate notifications are set up and going to the appropriate team members.
- Ensuring team contact information is up to date, including both work and personal phone numbers and email addresses.
- Creating an FAQ document that provides information on who to contact on different subjects/topics that may arise.

It's also important to look at scheduling, including planning shifts with both primary and backup staff. Everyone within the SOC team needs to know not only their own role but also the availability of the entire staff. Key to this is publishing staff schedules in a way that everyone can access and making sure that shifts and turnover policies are transparently communicated.

Using Today's Collaboration Tools for Success

There is a plethora of sophisticated collaboration technologies available today that enable remote work as similarly as possible to in-office work for many industries. And these tools can help ensure the success of the work-from-home SOC on top of the implementation of automation.

While automation will go a long way toward ensuring business continuity, the SOC team will need video and voice conferencing tools. Tools that provide remote access to the network, such as VPNs and other communications services such as email are also essential.

Another key tool is ticketing or case management technology. When an incident is identified, these enable collaboration among members of the security team as well as outside functional teams. Investigative efforts and analysis can be logged in the ticket or case and then shared among stakeholders.

Security and Resilience Even in Uncertain Times

The current health crisis serves as a reminder that the next business-disrupting event could happen at any time. To stay resilient and maintain business continuity and productivity, keeping a strong and uninterrupted cybersecurity posture is a necessity. Accomplishing this requires an action plan. Automation is a business-critical partner for enabling the work-from-home SOC, reducing the burden for SOC staff and possibly even reducing staffing needs. In conjunction with cloud apps and services, automation reduces or eliminates the need for in-office analysts when the team needs to work remotely or is offline. Use the steps above to formulate a plan if you don't have one already. If you do, check that plan against these steps to make sure you've covered all the bases for a high-functioning SOC that works no matter the circumstances or the location of your staff.

Remote SOC Q&A with Kyriba CISO, Eric Adams

Kyriba is a global treasury management solution provider with an international footprint of offices to support its global customer base. Kyriba built its own private, dedicated cyber defense facility in San Diego. Together with a lean but agile security team, Eric Adams, CISO at Kyriba, was tasked with building a cybersecurity program that would span the globe and meet the financial industry's strictest standards. To achieve enterprise grade security monitoring and free up his team to work on an ever-growing list of projects, Kyriba uses Respond Software to offload monitoring and triaging duties. This automation provides 24x7 coverage and support for teams operating remotely.

What is the biggest challenge small security teams face when running remote/WFH security operations?

The biggest challenge of a SOC security team is taking that traditional model of being in a closed secure room in an office and transforming that into a secure model that allows that SOC analyst or SOC engineer to do this same function remotely and securely. In addition, we need to keep the same level of collaboration and awareness that a team working together in the same room would have when they are in-person.

How is Kyriba's security team dealing with the shelter-in-place orders?

First, we had to ask ourselves, if there was a crisis, how ready is our team to work remotely? How much have we worked remotely before any crisis or BCP situation occurred? Were personnel allowed to work from home even partially if sick or due to other circumstances?

What turned out to be a good move is that we planned for an overhaul of our business continuity plan 18 months ago with scenarios including a natural disaster, a social uprising, and a pandemic. We understood even at that time, a pandemic was probably one of the most likely scenarios even back then. Since Disaster Recovery is for Systems and Business Continuity Planning (BCP) is for people, we had to define how to activate plans for different scenarios. What is different in the BCP planning for different types of disaster scenarios is that regional or geographic planning for backup personnel is different for those than during a global pandemic. For regional planning, we needed to plan for redundancy of personnel in roles in different geographic locations. Primary and backup people needed to have the training, knowledge, and access to take on roles as needed from different locations. For a global pandemic, where everyone is working remotely from home, we needed to make sure to have that same primary and backup (and multiple levels of backup in many cases), but also to make sure everyone had the capability to work from home. This included everyone having laptops, VPN access, and the infrastructure geared for those employees to work from home.

What are some best practices for organizations in implementing remote/WFH security operations?

All employees WFH:

- Multifactor authentication (MFA) on EVERYTHING. Including internal resources, but also 3rd party cloud services
- Remote Access through VPN with MFA enabled.
- Increased usage of remote collaboration with video including Zoom and similar systems, and also messaging such as Teams, Slack, and similar.
- Increased training to employees of increased vigilance to watch for opportunistic attackers via fake emails, fake COVID-19 maps with Malware payloads, etc.

For SOC personnel WFH:

- [In addition to all of the above]
- Increase the online meeting frequency since SOC personnel are typically in a security hardened room onsite at the office in order to remove the isolation barrier and keep the communications at the previous level of operation.
- Ensuring automation and key tooling are operational at all times, keeping in close contact with vendors to check on status and updates when needed.
- Increased vigilance looking for opportunistic attacks based on the changing threat landscape.

How is automation helping Kyriba keep their environment and business safe during this crisis?

The risk would be much higher if we did not have automation in place. If our SOC analysts were to become sick, we could have key alerts unseen and therefore not acted upon. Knowing how to engineer and use from your vendors' Robotic Process Automation, AI, and Threat Intelligence feeds from your industry and customize these for your business has been very key.