A Security Analyst's Guide to ChatOps

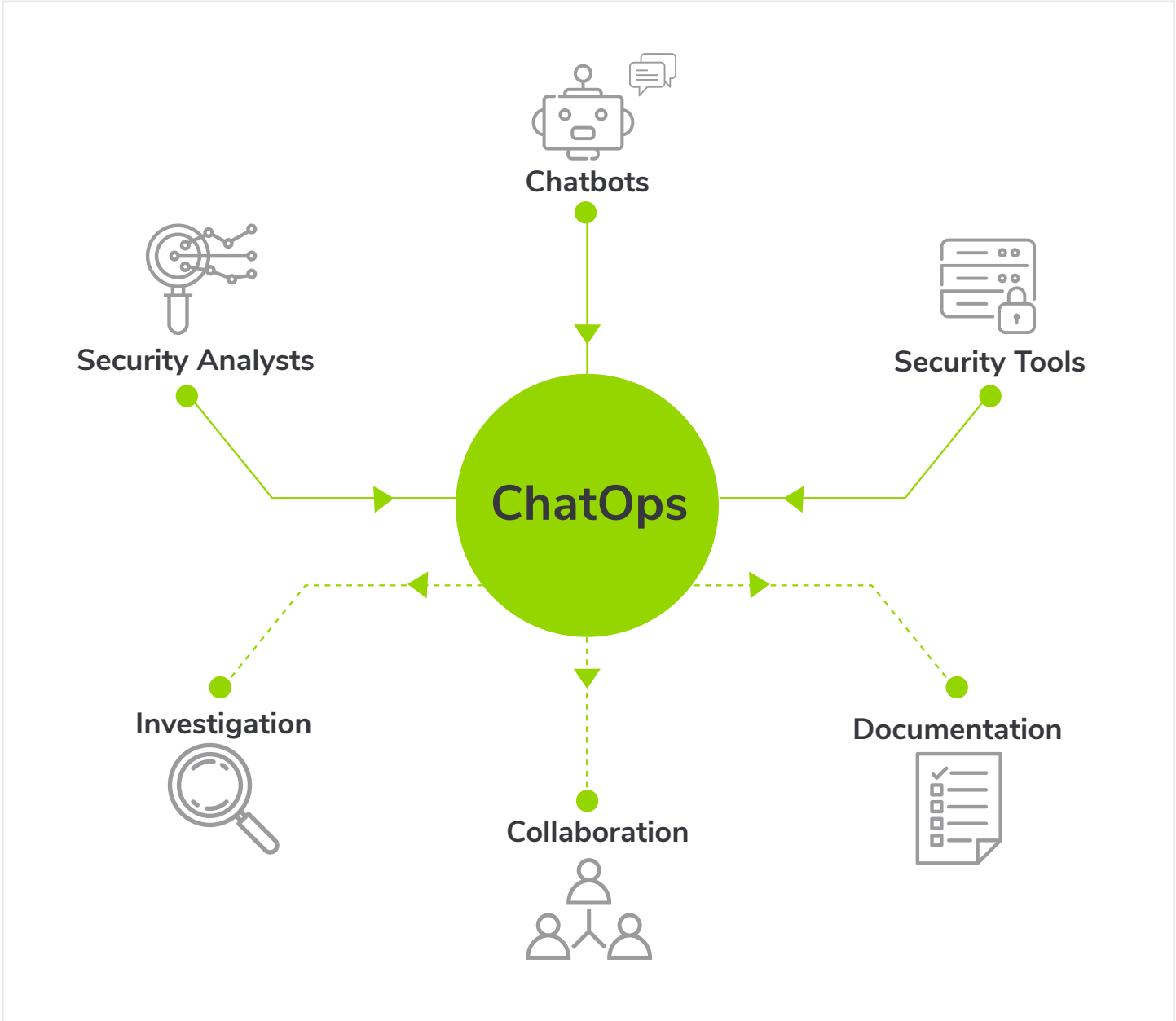
How To Future-Proof Your Security Teams With Collaborative Investigations

» TABLE OF CONTENTS «

WHAT IS SECURITY CHATOPS?

The simplest way to define ChatOps for security is as a **platform for conversation-driven investigations.** When security analysts, security tools, chatbots, and IR workflows exist in the same chat window and reinforce each other in a virtuous cycle: that's ChatOps in action.

Let's take an example. While responding to incidents, security analysts today may use one window for running investigation commands, another window (like Skype or WhatsApp) for conversing with fellow analysts, and a third window (email, text documents, or ticket management) for documenting their IR processes and logs. With ChatOps, analysts can perform all three actions – investigation, collaboration, and documentation – using the same solution, without having to change windows, and while leveraging the power of chatbots and other security tools.



WHY IS CHATOPS NEEDED IN SECURITY?

Despite a diverse and mature set of solutions to choose from, security analysts face a host of challenges that lead to sub-optimal incident response.

- **Lack of skilled analysts:** With a shortage of millions of analysts expected over the coming years, many Security Operations Centers (SOCs) are understaffed, leading to increased workload, stress, and rate of error among staffed analysts.
- **Rising alert numbers:** With an increased threat surface, a greater number of entry vectors
- for attackers, and an increase in specialized cyber security tools, the number of alerts are constantly on the rise. Analysts need help in identifying false positives and duplicate incidents, and keeping the alert numbers in check without burning out.
- **Product proliferation:** Analysts use numerous tools –both within and outside the purview of security – to coordinate and action their response to incidents. A recent NASDAQ report stated that the average organization uses up to 15 products! This involves lots of screen switching, fragmented information, and disjointed record keeping.
- **Siloed work environments:** An implicit but dangerous problem that mid to large sized SOCs face is security analyst tunnel vision and extreme narrowing of skill-sets. There is rarely, if ever, any cross-pollination of skills across analysts that result in effective joint investigations and reduced resolution times.
- **The Bus Factor:** Since security analysts are at such a premium, a sudden personnel loss can leave SOCs in a state of disarray. Senior analysts take most of their expertise with them when they leave and little knowledge remains stored within the organization.

ChatOps for security has the potential to alleviate all the above-mentioned problems in one fell swoop. It has caused sea changes in speed and efficiency in other industries like software development, customer service, and even online gaming! Let's take a deeper look.

THE RISE OF CHATOPS

Although ChatOps in security and allied fields is still fledgling, it has already gained considerable traction in wide-ranging industries and applications.

The most frequent and in-depth use of ChatOps today is in software development. By interweaving software engineers, deployment servers, code scripts, and chatbots into one platform – christened as DevOps – this industry has witnessed sharp increase in application deployment speed, business continuity, transparency, and even self-diagnosis and healing of production failures.

Customer service for online businesses is another area where ChatOps is on the rise. You can now use Slack to call a Lyft ride.

Facebook has integrated chatbots and other AI services into its Messenger app, allowing 900 million users to avail more efficient customer service from businesses with Facebook presence. As ChatOps doesn't require powerful coding expertise to automate complex actions, it is receiving encouraging traction in industries that depend on online communication.

One surprising industry where ChatOps has long resided is online gaming. Players can bring up command line interfaces during a game to customize everything from the crosshair type to the background brightness for easier enemy spotting. There are numerous chatbots available on Discord that provide players with real-time stats, inventory information, and in-game lore. Since online gaming is often team-based and depends heavily on collaboration, it is an ideal testing bed for ChatOps capabilities.

With all these industries already benefiting from ChatOps, it is only a matter of time before security teams look at its merits more discerningly.

THE BENEFITS OF SECURITY CHATOPS

Security ChatOps can result in both individual benefits for security analysts and end-to-end benefits for SOCs, striking a balance between qualitative improvement in an analyst's work life and quantitative reduction in operational risk for a SOC. Let's take a look at some benefits:

Increased Transparency

Currently, security analysts balk at collaborating on incident response because of the tiresome housekeeping that comes with it. Information sharing across analysts is done through email or ticketing solutions, creating unproductive back-and-forth exchanges and tab congestion. Tracking IR flows and processes for future incidents is taxing and often done on paper. Retrospectively searching for task ownership and accountability is a futile exercise amidst all the clutter.

ChatOps changes all this. When a team of analysts collaborates on a single window, **every chat, action, and command is tracked and visible to all parties.** This provides full transparency to both analysts and any external stakeholders with access who want to view progress. It's also easier to track accountability and link ownership of tasks with specific analysts, aiding measurement and making successful tasks repeatable

Knowledge Management

The skills gap in cybersecurity is well-known, with a global shortage of 1.5 million qualified analysts expected by 2019. In such a scenario, the Bus Factor looms large over every SOC. Sudden personnel losses result in an exodus of expertise and knowledge, with junior analysts required to start from scratch and pave their own way in the big, bad world of IR.

Working in ChatOps provides **robust one-stop archival of all actions, comments, and investigation commands.** Since everything is indexed, the security database becomes a vault where all analyst knowledge is stored for posterity. Personnel changes will no longer engulf IR in darkness, and greenhorn analysts will have a wealth of historical precedent to fall back on when dealing with unfamiliar incidents.

Comply or Die

Apart from documenting IR flows for archival, organizations also need comprehensive incident records for compliance purposes. With digital assets continuing their heady ascent in value, companies are required to comply with strict industry-specific regulations and auditing checks. With multiple security products, analyst accounts, and communication channels, trying to record all that information in one place is like herding sheep in the snow.

ChatOps can be **integrated with tools that securely transfer all information to a company's compliance database,** map to any specific recording formats that a company might use, and have summaries ready for easy retrievals. Even in the distributed and many-sourced digital world, ChatOps will provide the thoroughness of a physical ledger for reporting and compliance purposes.

Hit That Nitrous Boost

One of the most common gripes from security analysts is the time it takes to successfully respond to and close an incident. This slow speed stems from many reasons: the sheer number of alerts swamp analysts into submission, flitting between multiple security products leaves them in a daze, and working in silos deprives them of each other's expertise. When each issue adds up, it's like running a marathon with cemented boots.

ChatOps solves all three problems mentioned above. **A single window eliminates the need to jump between screens**, the chat-based interface encourages analysts to share knowledge and work together, and these joint investigations directly lead to a reduction in alert volumes. Each second of downtime after a cyberattack can spell financial doom for organizations; in this race against time, ChatOps provides a much-needed nitrous boost.

Always Be Learning

Meeting current challenges is the need of the hour; however, getting ahead of challenges and having the upper hand is the utopian state that security analysts pine for. With all this indexed information that ChatOps makes available, what's the best way to put the information to use rather than letting it gather digital dust? The answer – and it's the answer to most things nowadays – is machine learning.

ChatOps coupled with machine learning can act as a powerful force multiplier and enable analysts to drastically reduce response times, increase efficiency, and anticipate attacks. Machines can analyze stored data and suggest which analyst would be best placed to deal with a particular attack, how the workload should be divided among analysts to best cater to specific skill-sets, and which commands/actions would be most appropriate to deal with specific attacks.

ChatOps Benefits

Increased Transparency

- Full visibility for analysts and external stakeholders
- Easier tracking of accountability and assigning ownership of tasks

Knowledge Management

- One-stop archival for all commands and actions
- Analyst knowledge is stored for posterity

Regulatory Compliance

- ChatOps integration with tools that transfer documentation to compliance database
- Summaries ready for easy retrieval

Increased Speed

- Single window eliminates the need to switch between screens
- Easy coordination of security tools, chatbots, and analysts

Future Learning

- Suggest analyst-task matching and common investigation actions
- Easier training for junior analysts

EVALUATING CHATOPS READINESS FOR YOUR SECURITY TEAM

There is a right and wrong time to bring in ChatOps for your security operations and incident response. If you roll out ChatOps when the timing, resources, or need fitment aren't right, you will not only fail to get benefits out of ChatOps, but also potentially close the door for future ChatOps implementation when the need is more explicit.

The time to implement ChatOps is right when:

- Your incident response involves a mixture of automatable, well-defined tasks and cerebral, analyst-driven tasks.
- You have trouble tracking investigation tasks to specific analysts and attaching accountability.
- Coordinating between all the security tools at your disposal is time-consuming and potentially increases rate of error.
- You need to collate information from multiple sources for auditing and documentation.
- The incident resolution times are too long when analysts work separately (in silos) to resolve them.

A few other factors highlighting your security team's readiness for ChatOps are:

- Your team is experiencing alert fatigue from certain incidents even after implementing automation.
- You can't afford to train new analysts or have them make costly mistakes on the job in lieu of training.

In short, if your team is spending too much time in silos and foresees a benefit in combining investigation, collaboration, and documentation actions in one window, it's time to give ChatOps a try.

Let's use the above framework to tackle a common example: phishing incidents. The filled in table is given below.

Criteria	Answers
Does phishing incident response involve a mixture of automatable and manual tasks?	**Yes.** Mail parsing, enrichment, and initial triage are all automated. Deeper investigative actions are manual and performed by analysts.
Do you have trouble tracking investigation tasks to specific analysts and attaching accountability?	**Yes.** It's tough to know which actions were performed, their order, their effectiveness, and who performed them.
Do you have trouble coordinating between security tools at your disposal?	**Yes.** We use different tools for active directory queries, indicator enrichment, mail linkup, ticket management, and endpoint protection.
Do you need to collate information from multiple sources for auditing and documentation?	**Yes** and **No.** Ticket management provides a good, broad audit trail, but we don't have task-specific visibility and lack a single documentation source for sophisticated investigations.
Are the incident resolution times too long when analysts work separately (in silos) to resolve them?	**Yes.** There is often a back-and-forth where analysts perform an action, get feedback when analysts down the queue perform their actions, and have to change their initial work as a result.
Is your team experiencing alert fatigue even after implementing automation?	**Yes.** The base phishing triage and containment have been automated, but deeper investigations are too varied to be automated. Phishing alert numbers are rising and attack vectors are getting varied.
Are you facing challenges in training new analysts?	**Yes.** Senior analysts are too busy with day-to-day work to train them and there is no dynamic information source that junior analysts can access and experiment with to accelerate their training.
CONCLUSION	**Pilot ChatOps for your phishing incident response**

In the Appendix, there is a blank worksheet of the framework above that you can use to evaluate your security team's readiness for ChatOps by applying the framework to certain incidents/sub-teams.

CHATOPS IMPLEMENTATION BEST PRACTICES

Even after you've done your research on ChatOps, bought into its benefits, and evaluated your security team's readiness to implementation, there are by-lanes that can be tricky to navigate while carrying out the implementation. It's helpful to keep these best practices in mind:

- **Decide the method of implementation.** Based on your organizational resources, strengths, and areas of improvements, you can choose to either build your own ChatOps platform using publicly available bots and plugins or invest in ChatOps solutions specifically made for SOCs.

- **Start small.** It makes sense to choose a subset of your IR team or a specific set of incidents to pilot implementation of ChatOps. Based on the readiness framework provided in the previous section, check which incidents/teams have the strongest readiness with the least resource load, and use those as testing grounds for ChatOps.

- **Iterate.** Hardly any solution is implemented perfectly on the first attempt. If your ChatOps pilot ran into some snags but you saw potential for future success: study where the pilot fell short, change your subsequent plan of action accordingly, and implement another pilot to validate improvements the second time round.

ABOUT DEMISTO

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.

Appendix

SECURITY CHATOPS CHECKLIST

Security Team/Process: .....

Criteria	Answers
Does phishing incident response involve a mixture of automatable and manual tasks?	
Do you have trouble tracking investigation tasks to specific analysts and attaching accountability?	
Do you have trouble coordinating between security tools at your disposal?	
Do you need to collate information from multiple sources for auditing and documentation?	
Are the incident resolution times too long when analysts work separately (in silos) to resolve them?	
Is your team experiencing alert fatigue even after implementing automation?	
Are you facing challenges in training new analysts?	
CONCLUSION	