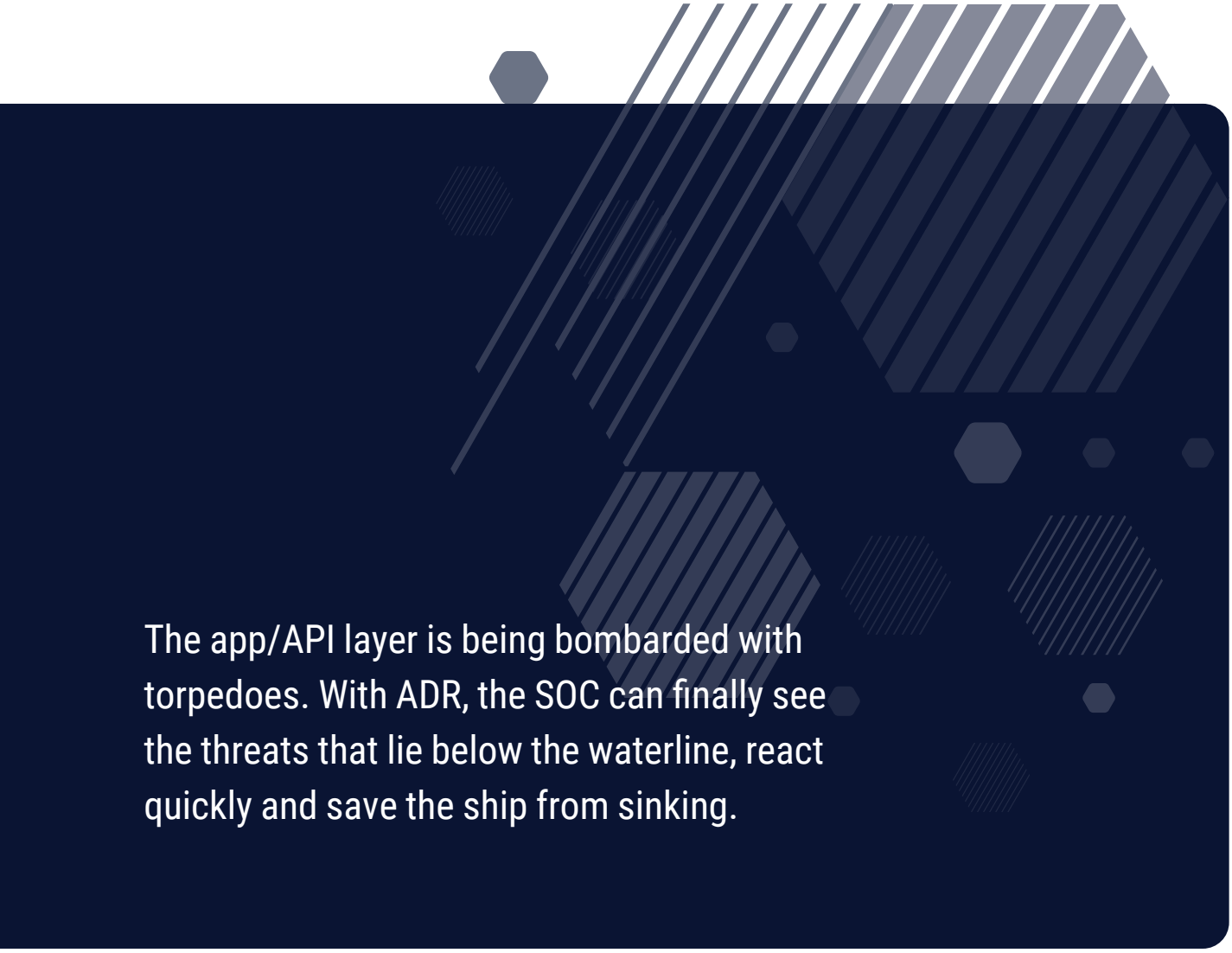
ADR and the SOC: 20K Leagues Under the SIEM

by Paul Senkel



The app/API layer is being bombarded with torpedoes. With ADR, the SOC can finally see the threats that lie below the waterline, react quickly and save the ship from sinking.

SOC defends organizations, the constant chasing and triaging, and especially the nitty-gritty task of trying to find out what really happened. If you have read my “Fear and Loathing in the SDLC” article, you will no longer consider the developers’ island as the happy island...but I must admit, despite everything, and for a long part of my 22+ year career as a developer and software architect, it was a happy place.



FIG. 1 Driving around in the figurative submarine Nautilus, fending of lurking threats



FIG. 2 The developers’ island is not an elysian island of the blessed

In this whitepaper, I leave the island and dare to set sail in order to explore the wild, dangerous sea. Based on real-life feedback from my colleagues who have worked in a SOC for multiple years, we will discover the tool landscapes (or seascapes?) and dive into those tools’ caveats, discovering why the collected information is more “muddy marshes” than “pristine waters.”

If you are new to life in the SOC, you’ll get a glimpse of why it takes a strong shell to stay in the SOC for a long time these days. If the SOC is already part of your life, then we’ll also sail to new horizons together and discover how Application Detection and Response (ADR) can help you to sail safely through the opaque, dangerous waters of Application Security (AppSec), clearing the blind spot that obscures the threats — be they torpedoes or injection attacks — that lurk below the surface of applications.

SOC duty vs. getting a life

You get paged for the third time in a week while spending well-deserved time with your significant other. You are at the movies. But something happened. You leave, it rains, so you sit in your cold car to log in and flip through what feels like a million tools, log files and reports to try to understand what just happened.

If you get lucky, you see what happened, and you can take the appropriate action fast and once again feel like the hero in the movie that you just missed. You saved your organization's or your customer's world from the apocalypse — again. It's not even exciting anymore. If being a superhero becomes your day job, everything can become a boring, yet draining, routine.



FIG. 3 With remote access always on duty

TRACK

DevOpsCon

DevSecOps & Cloud Security:
Shield the Production Cycle - Ship with Confidence.

Secure your SDLC with industry-leading solutions. Start threat modeling early and automate security testing throughout the lifecycle. Shift left with IaC scanning, software composition analysis, and other tests, while managing dependencies and securing cloud environments, open-source components, and Kubernetes deployments.

Learn from Industry Leaders about:

- **Shift Left Security Practices:** Integrate security into the early stages of development with IaC scanning, software composition analysis, and more.
- **Proactive Cloud Security:** Implement automated configuration management and security measures to protect cloud environments.
- **Open-Source Dependency Management:** Manage open-source dependencies and identify vulnerabilities using modern tools.
- **Generative AI for Enhanced Security:** Leverage AI for automating security tests and improving code quality during the development process.
- **Cloud Security Best Practices:** Safeguard your Kubernetes and cloud-native deployments with strategies for preventing vulnerabilities.
- **Security-Driven DevOps:** Learn how to integrate security tools and processes to maintain continuous security and compliance throughout your DevOps pipeline.

LONDON EDITION | MAY 12 – 16, 2025

The fact is, SOCs work with many tools. These tools cover a lot of facets in order to keep organizations safe. Having been born into IT as a webmaster and developer, I only really saw two facets of IT security. The network and … well, to be honest, for a long time, I didn't even think that AppSec was a real issue. These days, all too often, I discover that this "innocence" is still embedded in the creative minds of many developers.

So, what's on the SOC's menu?

- **Intrusion Detection Prevention:** Starting with network-based attacks, distributed denial-of-service (DDoS) and man-in-the-middle (MitM) attacks on the side.
- **Cloud-native application protection platform (CNAPP):** Starting with container and cloud security attacks, continuing with identity and access management (IAM), with serverless function-based attacks for dessert.
- **Internet and email:** Malware and viruses prepare your stomach for spam and phishing, while an assorted plate with impersonation, spoofing and ransomware will spice up your day.



FIG. 4 Traversing treacherous waters

- **Data loss prevention:** Email leakage, compromised accounts, unauthorized access, data exfiltration — four mains for the price of one, not for the faint-of-heart!
- **Endpoint detection and response (EDR):** An equilibrated choice of malware, privilege abuse and data exfiltration.

Sound yummy? Interesting? It sounds fascinating for sure, but if you have to "eat" all that every single day for breakfast, lunch and dinner, it's a lot to take in. Remember, we're sailing rough seas: You're bound to get queasy.

Even the best data aggregation cannot help you digest all that. As all analogies stop working at some point, I will refrain from suggesting adding spices or your preferred digestive drink. I learned that SOC guys and gals are tough old salts and can stand the rough weather as long as the ship's ropes and winches are in good shape and enable them to keep the ship in the clear.

However, even with all these tools, our sailors still cannot see below the waterline. That's too bad, given that there's a lot going on down there. If you cannot see what is happening in your applications, then not even analysis of all traffic can supply a targeted, proactive approach.

It is challenging to aggregate the information you need to figure out if something bad happened inside an application. You need to pull it out of the web application firewall (WAF), database logs and eventually server logs. Sometimes, it's not even possible to get that information: If the attack happened purely inside the application, using the existing access rights of the application — a bit like what SQL injections do — then the SOC will be totally blind to it.

Doing that forensic work is hard if you are already busy with patch management; keeping 5-6 different operating systems secure; and staying on top of zero days on all the levels that you can manage: network, server, container, operating system, etc. However, on the application level, you have the impression that you are always two steps behind: very frustrating. There is so little time for root cause analysis, especially if you have scanty context.

So that's the big problem ...

How can you analyze and protect yourself against something that you cannot see?

Imagine you are being asked to sail around the world. Alone. You can never properly sleep. You will face all kinds of weather and many other challenges. But that is fine. You know that you are a good sailor, you have a great ship, you run it tight and you know you can do it.



FIG. 5 Chief officer getting some rest

Now you are being asked to sail around the continent. You must stay close to the shores at all times. You cannot see the reefs, and you know that in some bay there's a submarine army of a hostile nation state, waiting to sink you with torpedoes. Now, you are being told to do it wearing a blindfold. The reasonable reply would be: "Are you out of your bloody mind?" And yet, this is the reality of life in the SOC.

While the intrusion detection and prevention system (IDPS), data loss prevention (DLP), EDR, CNAPP, etc. systems cover a great deal of the IT landscape, they are blind to what happens below the surface, inside the application.

Life in the SOC is hard. It's hard because of this confluence of not seeing, not knowing and yet still being responsible for IT security overall that generates fatigue and weariness. There is already a lot of alert fatigue with all these tools: alerts that need to be aggregated, combined and triaged. It's the need to write meaningful reports that respect agreed service-level agreements (SLAs), with all the forensic work needed for finding out if, below some small, icy tip, a large iceberg is lurking.

It's especially hard if you are blind to a whole category of attacks that are ever-increasing.

How can it be that we sail blindly in dangerous waters?

For a long time, many organizations thought that the WAF was enough. And most are still not aware that newer technology like ADR, which can be embedded directly into applications, can make a huge difference. ADR revolutionizes AppSec in production, like sonar has made sailing a lot safer. Being able to see what happens in the application layer enables the SOC to make better and faster decisions like sonar enables the sailing crew to avoid underwater dangers.

WAFs, which are mostly signature-based, cannot defend efficiently against elaborate or new attacks. They just cannot recognize them. And if they block everything that just looks a bit weird, then they might block a delivery address from being created because it is the "Rue de la Toison d'Or" in Quebec … which looks a bit like a SQL injection.

SESSION

DevOpsCon

Developers vs. Security: Tech's Smoldering Cold War (Why ADR Is the Negotiated Peace Treaty We've Been Waiting For)

with John D Wood (Contrast Security)

Tech's smoldering Cold War: developers race to ship features while security stalls progress with noise, false positives, and endless backlogs. Legacy ‚Shift Left' approaches have failed, frustrating teams and crushing productivity. This talk flips the script with Application Detection and Response (ADR), focusing on real runtime risks, slashing false positives, and enabling swift fixes. With humor and sharp insights, we'll arm developers with witty comebacks to outdated security demands and show why ADR is the peace treaty the industry needs.

LONDON EDITION | MAY 12 – 16, 2025

Using a WAF is like using sonar that only alerts you to reefs and torpedos, but which lets you run into a floating underwater mine — because it does not recognize the threat. Or sonar which constantly alerts you to what it interprets as dreadful dangers ahead, although in reality it's just a swarm of harmless little fish. Only complete visibility enables fast and accurate decision making.

Why WAFs struggle to stop these slippery fish

WAFs just aren't enough [1]. They either overblock or underblock, as they cannot possibly know what an application can or should handle. **Take a closer look [2] at the differences between Contrast and WAFs.** But now that you know that the WAF cannot protect you in a comprehensive and precise manner, let's have a look at how ADR can make a real difference in an organization's security posture and how it can improve the daily life of the SOC.

How can ADR make a difference?

ADR can track traffic from the request to the sink — i.e., a database, a file system, any specific node to which the data should be delivered. If something malicious is being observed, it can provide the full execution stack trace on what functions were called inside the application. This gives a great deal of context on what is being tried, what may be happening and what has already happened. ADR could even block malicious action if you let it. It is part of the app, having been added to the app while it was being loaded into memory. Being part of the app, it can cleanly stop the execution of the program for the concerned user and alert the SOC with full context.

I am not sure that my C-levels understand the blind spot...

It is tough to understand and see the blind spot when you are yourself blind to it. However, one analogy that works very well is the supermarket. Alternatively, use a bank if that's more spot-on.

Just ask the question:

SOC: "Can you imagine a bank or a supermarket without CCTV or security guards?"

The likely answer is:

C: "No, but why …"

SOC: “Because that is what our IT infrastructure looks like today from a security perspective. We have perimeter defenses, we monitor all kinds of data flows, but we have no idea what is going on inside our shops — as in, inside our applications.”

C: “OK, got it. But I thought we had firewalls and WAFs?”

SOC: “Yes, but they are like monitoring what kind of types of cars you allow to enter your parking lot. It still does not allow you to understand who is a thief and who is a regular customer. A WAF cannot understand intention.”

C: “What can we do about it?”

SOC: “There is a new thing called ADR: Application Detection and Response.”

C: “We already got that, right?”

SOC: “No. You’re probably thinking of EDR. That’s for endpoint detection and response. EDR could spot malicious action — if the application triggers it and if we know that it’s not supposed to do that.”

C: “OK …”

SOC: “ADR works from within the application. And the long-time Runtime Security champion Contrast Security does that in a way that can even block malicious action inside the app. It’s a game changer, as we cannot just get more clarity on what happens, but we can even reduce post-breach events.”

C: “Sounds amazing. Care to join me for lunch?”

WORKSHOP

DevOpsCon

Rethinking DevOps and DevSecOps with Generative AI: Insights and Innovations

with John Willis (Botchagalupe Technologies)

This workshop talk is designed to provide insights into the revolutionary impact of generative AI tools on DevOps and DevSecOps. The presentation will explore how advanced AI technologies like Large Language Models (LLMs), LangChain, LangSmith, and vector databases (RAGs) transform the software delivery and security landscape.

LONDON EDITION | MAY 12 – 16, 2025

Conclusion

In a world where nations employ hackers in order to hack other countries' companies, it's hard to stay on top of a game that includes a submarine army waiting for you in the next bay.

SOC teams are hard to scale, because the job is hard. Lots of alert fatigue, high workloads, being on call, having to take into account so many different attack vectors. Fortunately, specific tools help target specific attack vectors and protect the different layers.

Finally, the long neglected application layer can also be protected appropriately, with ADR. As the evolution of Runtime Application Self-Protection (RASP), ADR will reduce the overall number of incidents that require action and will fill the gap of the current missing defense. ADR instantaneously provides new visibility and can also block attacks. Finally, the SOC will no longer feel as if they're always two steps behind when it comes to AppSec and can actually reduce the number of incidents.



With over 20 years of experience in software development and architecture across Europe, Paul Senkel has made the leap from building applications to revolutionising how companies approach AppSec. He's passionate about bridging the divide between security and development teams, making AppSec fixes not just painless but genuinely enjoyable. His unique blend of technical expertise and understanding of team dynamics helps organisations foster a culture of security that's both effective and engaging.

Links

[1] https://www.contrastsecurity.com/glossary/waf-vs-rasp?hsLang=en

[2] https://www.contrastsecurity.com/security-influencers/how-contrast-protect-differs-from-web-applications-firewalls-wafs

DevOpsCon

THE GLOBAL CONFERENCE SERIES FOR **DEVOPS & BUSINESS TRANSFORMATION**

