WHITE PAPER

Going SOCless: The Next Leap in Enterprise Cybersecurity

STELLAR CYBER®

The enterprise SOC (Security Operations Center) concept is often glamorized – big monitors, flashy visualizations and tiers of analysts somehow consuming all this information. With the threat landscape increasing and attacks becoming more commonplace, there is no time to focus on anything except security results. That's why the future of enterprise cybersecurity is not the SOC, it's SOCless.

SOCless applies to enterprises of all sizes and security maturity. Whether you want to supercharge your mature security operations, or get the security ROI you know you're capable of, or get started on your security journey – SOCless is for you. If you run a security services provider, SOCless is still highly relevant, but in the sense that your organization is part of a SOCless solution for enterprises. Before unpacking what SOCless is, why it's important, and how to go SOCless – it's important to be clear on what SOCless is not. SOCless is not about trimming your already lean security team where many may work in the "SOC." Additionally, for enterprises, SOCless is not about abandoning SOC-as-a-Service offerings from trusted partners (in fact it is the opposite).

SOCless is a rejection of the status quo – alert fatigue, unhappy analysts – through rigorous security operations principles supported by scalable, automated systems. Or as Alex Maestretti (current CISO at Remitly, former Engineering Manager at Netflix) put it, the last thing you want "is a bunch of lame alerts creating busy work for a large standing SOC." SOCless solves that problem.

What is SOCless and why is it important?

Similar to Zero Trust, SOCless is an approach to security that embodies many concepts and principles. Aspirationally, SOCless means that every security alert requiring a human analyst wakes someone up. That means there is very little noise and every alert with a human in the loop goes to the right person, is of the highest fidelity, and has a clear response action menu. Otherwise, the security team would be burnt out after a week.

SOC-Based Approach	SOCless-Based Approach
Significant number of alerts to triage every day, requiring large teams	Very few alerts seen by analysts every day because of automation and noise reduction
Tiered analysts triage alerts and bring in infrastructure owners when needing escalation	Alerts are routed directly to security or infrastructure owner
Security operations team spends most of its time triggering alerts	Security operations team spends most of its time writing context into their detection and response platform and implementing fundamentals that improve fidelity

Does this all sound too good to be true? Or possibly even so simple that it doesn't sound revolutionary? The reality is, **SOCless isn't that complicated.** What's challenging is sticking to the commitment of proactive security and finding the right systems and partners that support the outcome of SOCless.

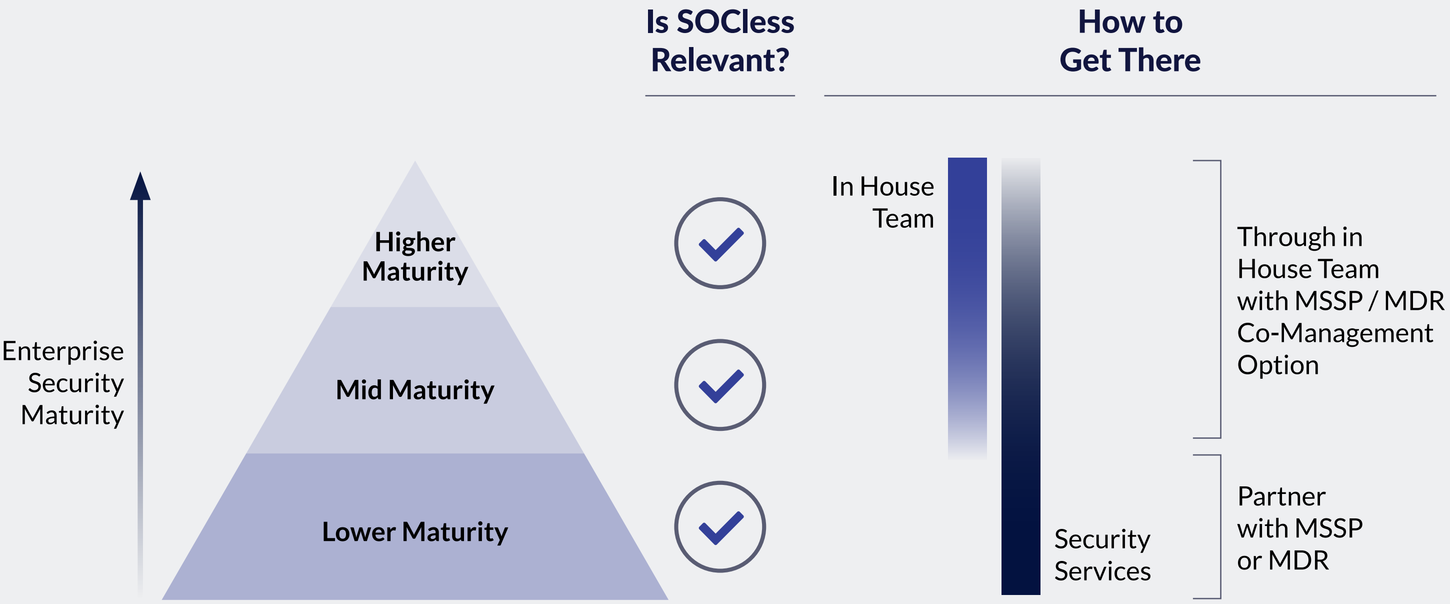
The results from being in this aspirational state are clear – better detection and response performance, happier security team. Importantly, there is no alert fatigue. It is impossible to keep up with the current threat landscape with a traditional enterprise SOC approach, that is why SOCless is so important – because it is necessary for survival.

To realize a state of low noise, decentralized triage, high fidelity and actionable responses within security operations, there are several security principles an enterprise has to put into place:

- **Automate everything trivial** – Why? Keeps your analysts happier, shrinks the problem space humans have to deal with, improves MTTR.
- **Aggressive alert tuning** – Why? Lowers noise and improves fidelity.
- **Implement Zero Trust** – Why? Shrinks the data problem through verification, making many risky attack vectors impossible, thereby significantly reducing alert noise.
- **Contextualize all alerts** – Why? If someone is going to be woken up, it should be the right person, and they need to know exactly what to do.

How to go SOCless

Here is a quick summary on going SOCless. First, it's for all enterprises. Even the biggest, most technically competent ones – as noted earlier Netflix is SOCless, FOX Corporation is too. If you are a lower security maturity enterprise, partner with a leading MSSP (Managed Security Service Provider) or MDR (Managed Detection and Response) provider. If your security maturity is in the middle or on



the higher end, make the proactive commitment, implement the right systems, and consider a security partner for co-management.

Security maturity can be difficult to define, but ultimately is a measure of focus, investment, and core competency. So any enterprise in the "lower maturity" bucket likely has no dedicated security personnel and does not focus heavily on security itself even though it now knows it is increasingly important. Fortunately for SMBs and other lower security maturity enterprises, MSSPs and MDRs have been rapidly advancing their services in recent years and effectively are the solution to go SOCless for this security bucket. Many of these security partners will sell "SOC-as-a-Service." Don't be alarmed; this service is what is helping your enterprise go SOCless. The security partners have invested in the systems and processes to deliver that aspirational SOCless goal. What you receive from them is high fidelity, actionable information only. They have the expertise to set up automation, tune alerting through ML (Machine Learning), and contextualize alerts so you don't have to. As an analogy, purchasing "SOC-as-a-Service" or an equivalent offering so you can go SOCless is like a software company using IaaS (Infrastructure-as-a-Service) from a cloud provider so they can focus on software.

For more security-mature organizations, there should be some internal element to your approach to going SOCless, likely because of the complexity of your operations. That does not, however, rule out a security partner co-management arrangement, which can be very effective to reach SOCless. More on that later.

An internal security team's journey to SOCless is similar to a software development team's journey to modern DevOps. DevOps is a combination of principles just like SOCless – it takes the right systems (e.g., GitLab, CircleCI, Kubernetes) and the right processes (e.g., commitment to integration testing) to realize. Modern DevOps is what allows lean software teams to compete with the world's largest software teams – most time is spent on building the software, not on fixing bugs and figuring out infrastructure. SOCless is what allows a lean security team to protect the complex enterprises in today's threat environment.

In DevOps, developers put continuous testing upstream into the process in the form of unit tests, integration tests, and full system tests. These tests run automatically as new code checks in. No new feature goes out the door without the appropriate testing being written and deployed. Does this require extra effort up front? Yes, but the ROI is huge because there are so many bugs and issues that this prevents. In security, this equates to a shift from triage to writing, managing, and tuning detections and their associated responses. This shift may seem impossible if your team is underwater with alerts, but the pain is worth it if the foundations are set and your team can turn that corner.

This shift is impossible to do without the right systems in place. First, and most obvious, you need the right telemetry and tools that allow for automated response. Second, and still hopefully obvious, you need a SOAR (Security Orchestration, Automation, and Response) that can power significant levels of automation. Finally, you need a detection and response platform that allows your team to focus its time on managing high fidelity detections and not dealing with noise. The characteristics to look for in this platform is that it ships with detections out-of-the-box (so your team doesn't have to manage so many detections and can more easily leverage ML), enables robust custom detection management, contextualizes and correlates alerts automatically, responds directly to events, and is simple to use. If those conditions aren't met, your team won't make the shift from reactive to proactive.

As mentioned previously, for the more mature enterprise, co-management with an MSSP or MDR can make a lot of sense. This can help with making the transition to SOCless less painful and sustaining this proactive approach to security overall. Huge bonus points if this partner can provide real purple team testing so that your coverage can always be assessed and you know what telemetry and detection gaps there are so they can be fixed.

In summary, the future approach to enterprise security operations is not the SOC. It is not about triaging thousands of alerts every day or somehow being NASA for security. It's about going SOCless. SOCless is a rejection of the security operations status quo and a rigorous commitment to best practice security principles, automation, and a fully proactive detection and response mindset that results in high fidelity information and ultimately protection for the enterprise.