SOLUTION BRIEF

SOC Prime & Corelight

Empowering Threat Detection & Hunting with Curated Sigma Rules Applied to Network Evidence

By applying SOC Prime's Detection as Code, Sigma language, and MITRE ATT&CK® coverage to network evidence generated by Corelight's Open Network Detection and Response (NDR) platform, security operations teams can enhance threat detection and hunting capabilities across industry-leading security analytic solutions.

Organizations are challenged with ever-increasing attack volumes and threat complexity, which requires ultra-responsiveness from security teams to keep up. Limited network visibility and endpoint protection gaps lead to blind spots and increased business risk, which pose a significant threat to reputational damage.

Due to a growing demand for endpoint protection against emerging cyber attacks, IT and security teams struggle to build custom threat hunting use cases based on endpoint telemetry alone, and continuously expand detection coverage as benchmarked against the MITRE ATT&CK framework.

Customer Pain Points

Limited Visibility
Lack of visibility across endpoint, network, and cloud

Increased Cybersecurity Risks
Gaps in EDR coverage lead to higher cybersecurity risks and potential data breaches

Threat Complexity
Security teams find it hard to stay on top of the emerging threat landscape

Insufficient Log Source Coverage
Lack of custom use cases tailored for organization-specific log sources

Moreover, security teams are overwhelmed with manual processes, disparate security tools, vast volumes of data coming from multiple security tools, and an industry talent shortage. All these challenges are exacerbated by high costs, the effort required to develop bespoke detections for organization-specific log sources, as well as the pressing need to improve overall corporate cybersecurity posture.

Accelerated Detection, Threat Investigation & Hunting Using Sigma and Corelight

SOC Prime has established the Detection as Code category, building a foundation for collective cyber defense. Being the first and largest commercial contributor to the Sigma language, SOC Prime fosters crowdsourced content development connecting over 600 threat researchers who share their collective cybersecurity expertise with industry peers to make sure security teams always have an algorithm against any TTP that was or will be used in a cyber attack.

SOC Prime's Detection as Code platform curates more than 200,000 pieces of context-enriched detection algorithms aligned with the MITRE ATT&CK framework and continuously updated. We enable security teams to address the challenges of building custom use cases based on Corelight network logs, organize and execute around strategic detection objectives, and manage the deployment of detection content at scale.

Collective Expertise: SOC Prime & Corelight

Corelight transforms network and cloud activity into evidence so that defenders can stay ahead of ever-changing attacks. Striving to foster community-backed engagement across industry peers, the company has created the Corelight Threat Hunting Guide, sharing insights into simple and relevant ways to discover attacks using Corelight network data. The guide is organized around the MITRE ATT&CK framework, detailing threat hunting scenarios, helping security teams develop a valid threat hunting theory and establish prioritization.

SOC Prime Highlights

200,000+

Context-enriched detection algorithms

9,000+

Unique Sigma rules mapped to MITRE ATT&CK

600+

Threat researchers

25+

SIEM, EDR & XDR platforms

Corelight Highlights

- Enterprise-class, Open Network Detection & Response Platform
- Founders and maintainers of open source Zeek®
- Augmented by continuous detection engineering from open source communities

SOC Prime is building collective cyber defense partnering with private businesses and cyber defense agencies, including NCSC and CERT teams, to test Sigma rules on the real battlefield. We enrich the collective cybersecurity expertise by contributing to open source projects. As part of this community-driven collaboration, SOC Prime has contributed to the community by providing 70 curated Sigma rules to accompany the Corelight Threat Hunting Guide. These on-demand detection algorithms enable teams to realize threat hunting hypotheses for exfiltration via DNS and search for threats based on Corelight network data matching the guide.

All Sigma rules built specifically for the Corelight Threat Hunting Guide are available in SOC Prime's threat detection content repository and can be seamlessly found by a custom tag "corelight thg".

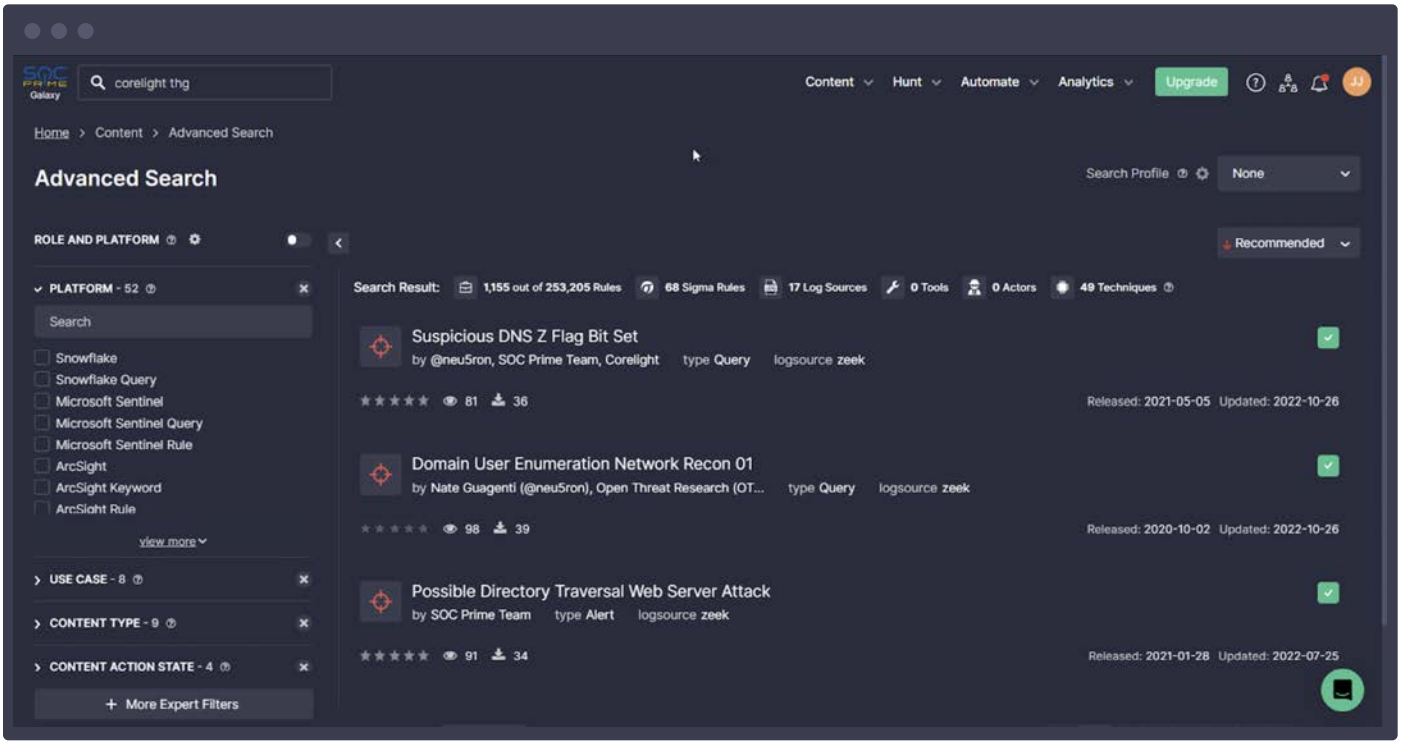
SOC Prime & Corelight Collective Expertise in Numbers

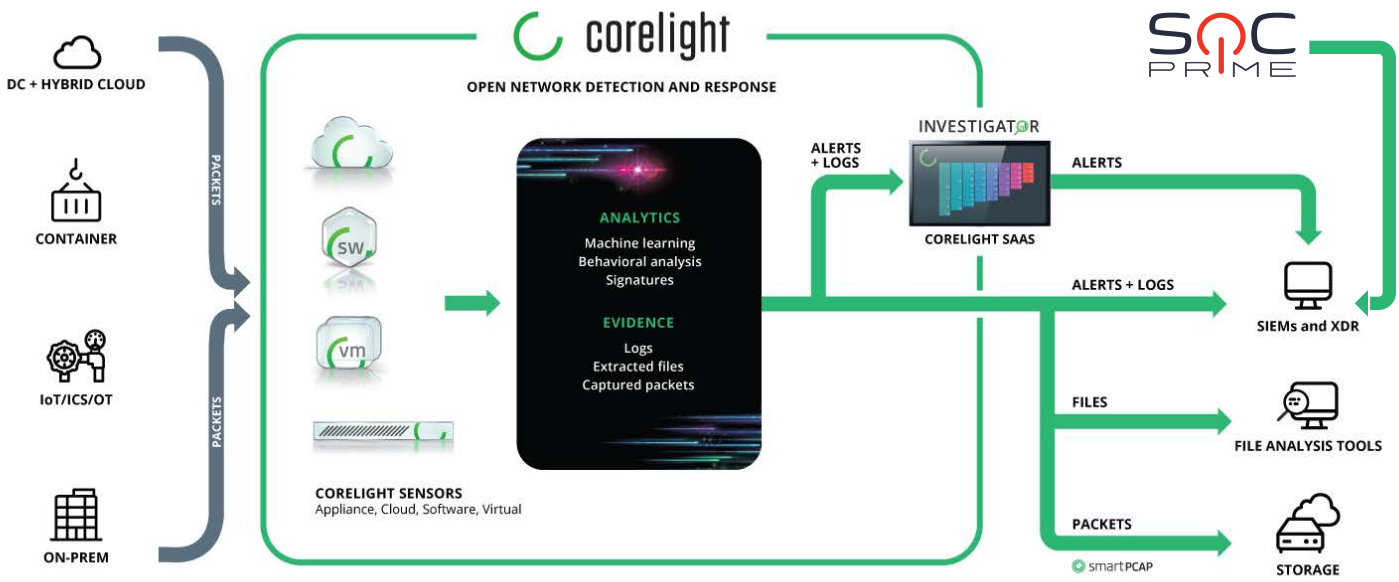
2,000+

Detections based on Zeek network data from Corelight

70

Curated Sigma rules for the Corelight Threat Hunting Guide





WE INTEGRATE WITH YOUR FAVORITE TOOLS, INCLUDING THESE:

aws · CROWDSTRIKE · Cribl · DEVO · elastic · Google Cloud · MANDIANT · Microsoft · splunk> · + OTHERS

Integration Details

Corelight Sensors provide cyber defenders with the best-in-class network evidence and insights to reduce alert fatigue and streamline investigation enabling accelerated hunting and detection capabilities. Leveraging Sigma rules based on Corelight and other applicable network data available in SOC Prime's Detection as Code platform, these sensors correlate threat intelligence with the identified network behavior. The resulting evidence, alerts, packets, and extracted files can be pushed to SIEM, EDR, XDR solutions, and data lakes, such as Elastic and Splunk.

SOLUTION BRIEF

Drive Immediate Value with SOC Prime & Corelight

SOC Prime's Detection as Code platform enables IT and security teams to stay on top of emerging threats by obtaining curated detection content to proactively defend before attacks hit. SOC Prime's integration with Corelight Open NDR allows addressing the challenges of custom detection content shortage and limited visibility into threats that matter most by delivering and supporting out-of-the-box use cases mapped to ATT&CK and covering Corelight network logs. Leveraging custom threat hunting use cases based on endpoint telemetry enables teams to significantly reduce gaps in EDR coverage and minimize security risks. Fusing Sigma language and Corelight network evidence, organizations can obtain ready-to-use detection algorithms tailored for multiple SIEM, EDR, and XDR solutions while significantly saving security team hours on detection content research and development along with maximizing the value of SOC investments.

Key Benefits

Proactive Cyber Defense
Prioritize in minutes and deploy detection content against the latest threats before adversaries have a chance to attack

Improved Visibility into Threats
Minimize endpoint visibility gaps with advanced NDR evidence and curated threat hunting on endpoint use cases aligned with MITRE ATT&CK

Cross-Platform Detection Content Development
Save R&D effort on SOC content development covering Corelight network data and tailored for 25+ SIEM, EDR, & XDR solutions

Cost Efficiency
Maximize your team engineering capacity and extract more value of SOC investments with the world's largest threat detection marketplace of ready-to-deploy use cases

About SOC Prime

SOC Prime operates the world's largest and most advanced platform for collective cyber defense that cultivates collaboration from a global cybersecurity community and curates the most up-to-date Sigma rules compatible with over 25 SIEM, EDR, and XDR platforms. SOC Prime's innovation, a community-driven approach based on Detection-as-Code principles, and cutting-edge technology leveraging Sigma language and MITRE ATT&CK® as core pillars are recognized by the independent research companies, credited by the leading SIEM, XDR & MDR vendors, and trusted by 8,000+ organizations, including 42% of Fortune 100 and 21% of Forbes Global 2000.

About Corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our Open Network Detection and Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology. For more information: corelight.com

For more information about SOC Prime, visit https://socprime.com or follow us on LinkedIn or Twitter.