# CHECK POINT + D3 SOAR

THE BEST NGFW MEETS THE BEST SOAR

## SOAR THAT'S COMPREHENSIVE AND EASY-TO-USE

### Solution Benefits

- Automated best-practice-based SecOps and IR playbooks
- Faster detection and response workflows—seconds, not minutes
- Accelerated investigations through integrations
- Increased visibility for team leaders through extensive trend reporting
- World-class support and collaboration from a vendor staffed by security experts

### Solution Features

- Out-of-the-box playbooks for common incident types
- Out-of-the-box integrations for 260+ security and IT solutions
- Automated MITRE ATT&CK or custom TTP correlation
- Enterprise-grade, multi-departmental case management system
- Industry's only fully codeless playbook editor—keep your analysts investigating instead of editing playbooks.

Security teams struggle to combat advanced attacks and protect their environments. That's because modern cyber threats are highly dynamic, with sophisticated adversaries constantly finding new ways to exploit outdated systems and lagging response times.

To meet the challenge, security and incident response leaders must form a unified defense — one that brings together intelligence, action, and best-of-breed technologies.

When detection and response workflows are automated and optimized, SOC (Security Operations Center) teams can do far more than prevent individual elements of an attack. It can identify threats, disrupt the kill chain, and help organizations strengthen their security posture.

## COMPREHENSIVE AND EASY-TO-USE SOAR

The combination of Check Point and D3 SOAR provides SOC teams with vastly improved visibility, intelligence and agility. Events in Check Point trigger automated playbooks in D3, which gather context from across the security ecosystem, including correlation against the MITRE ATT&CK framework. If the event is convicted, D3 will execute the remediation plan, which can be fully or partially automated. The whole process takes only seconds.

For example, a spear phishing use case might look like this:

D3 monitors the phishing inbox and creates an event in D3 SOAR by pulling the suspicious email content and attachment(s).

The file reputation is automatically checked in the Check Point Threat Prevention module. If the file is not found, an API call will be triggered to upload the original file for sandboxing.

D3 will also search SIEM logs for suspicious network flows on the involved endpoints. External IPs and URLs are enriched automatically.

If the reputation is malicious, a response playbook will be triggered to quarantine endpoints and block IPs and URLs.

D3 will also trigger searches for similar events based on MITRE ATT&CK TTP rules and observes affected endpoints and email recipients for signs of threats so that correlated events can be proactively detected, preventing advanced attacks and zero-day threats.

## THE CHECK POINT THREATCLOUD NETWORK, APPLIED THREAT INTELLIGENCE

The Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Real-time threat intelligence is enriched by AI engines to detect and block thousands of attacks daily. When customers send their own threat data to the ThreatCloud they receive protection updates with enriched threat intelligence.

Customers and technology partners who participate in the ThreatCloud network can use the collected malware data to benefit from increased security and protection. The ThreatCloud can then distribute attack information, and turn zero-day attacks into known signatures that Check Point network, cloud, endpoint, mobile and technology partners such as D3 Security can block.

## A NEXT-GENERATION APPROACH TO SECURITY OPERATIONS AND INCIDENT RESPONSE

Together Check Point and D3 Security enables:

**Improved Speed and Quality of Investigations –** In addition to integrating with Check Point, D3 Security also integrates with 260+ other solutions, enabling the seamless flow of intelligence and action across the SOC. Analysts can more easily identify threats, assess their criticality, and disrupt the kill chain—often with little to no manual intervention.

**Automated Incident Response Playbooks** – D3 Security comes packed with playbooks. Clients can access playbooks from a variety of frameworks or build their own using D3's codeless playbook editor, which abstracts all Python coding away. All D3 Security playbooks are agile and adaptable, providing maximum flexibility to SOCs facing dynamic threats.

**MITRE ATT&CK Framework Adoption** – Check Point and D3 Security customers can bring to the surface ultra-rich context by mapping and correlating events against the ATT&CK framework, enabling a rich and varied array of TTP-oriented dashboards, reports, and workflows.

**Dramatic MTTR Reductions** – SOC and IR teams using the Check Point and D3 Security joint solution benefit from incredible gains in operating efficiency and correlation capabilities, leading to dramatic response time reductions across incident types. D3 Security clients have experienced MTTR (mean time to recovery) reductions of up to 99% by adopting SOAR and throwing out their manual incident-handling procedures.

## ABOUT D3 SECURITY

D3 Security's Next-Generation SOAR Platform combines full-lifecycle security orchestration, automation and response (SOAR) with proactive MITRE ATT&CK and TTP correlation. SOC operators around the world use D3 to automate manual processes, improve the speed and quality of investigations, and dramatically reduce MTTR and false positives. Plus, unlike SOAR tools which require Python skills to operate, D3's Codeless Playbooks abstract coding away, making it easy for anyone to build, modify and scale playbooks and integration. Go to D3Security.com to get started.

## ABOUT CHECK POINT SOFTWARE

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.