WE
SECURE
THE
FUTURE

Preventing Attacks with Intelligence and Analytics

A Collaborative Approach to Information Security

This paper provides an overview of the Check Point
and IBM Security alliance announced in February 2016

Executive Summary

In February of 2016, Check Point Software Technologies and IBM Security announced a deepening of their long-standing relationship, aimed at providing the customers of both companies with significant enhancements to their overall security infrastructure and management capabilities. The key elements of this alliance include:

- **Shared threat intelligence.** An open approach to collaborative defense under which IBM X-Force and Check Point's security research teams will directly collaborate through the bi-directional sharing of threat identification and analysis. This collective threat intelligence may be integrated into each company's threat intelligence products, to help deliver proactive threat protection to customers of both companies.

- **Integrated event management.** Check Point will be launching a new SmartEvent application in the IBM Security App Exchange for integration with the IBM Security QRadar Intelligence Platform. The app will deliver network data and security events from Check Point devices to QRadar to enable operators to view threat information in real-time directly from the QRadar console for faster incident response.

- **Advanced mobile protection.** Integration within IBM Maas360 enterprise mobility management (EMM) will allow customers to easily deploy and manage Check Point Mobile Threat Prevention to limit compromised devices from accessing enterprise networks and data, based on real-time insights. The combination of these capabilities provides automated protection against advanced threats across mobile devices, apps and networks, while significantly simplifying the implementation and ongoing monitoring of mobile security technology across the enterprise.

- **Managed security services.** IBM Managed Security Services (MSS) will continue to deepen its expertise in delivering and managing Check Point solutions for IBM customers. The deployment and management of a broader range of Check Point network security offerings will provide customers with cost-effective access to resources and expertise as their security requirements evolve.

This paper provides additional detail on the challenges organizations are facing that motivated our companies to form this new alliance, the expected benefits to our customers, and how our collaboration drives a proactive approach to securing the enterprise.

Three is not always a charm

Information Security is a practice defined by threes. The concepts of Confidentiality, Integrity and Availability serve as a foundational principle. And, the process of Detect → Protect → Respond serves as a framework for daily operational activities. For much of the past 20 years, these triads provided a comfortable operating environment that was imperfect, but at least appropriate to the threat environment in which most companies operated.

More recently, the scope and complexity of attacks and the impact of such threats suggest that the second of these concepts, the process of Detect → Protect → Respond, would benefit from greater collaboration across the security community. As attacks have evolved to a point where they cannot be detected through traditional, signature-oriented technologies, and they target applications and systems that are often outside the scope of an organization's security infrastructure, it is apparent that threat intelligence sharing and security technology integrations have become imperative.

What you don't know, can hurt you

Attacks increasingly employ tools that include new or modified variants of previous exploits, undetectable by solutions looking only for known vulnerabilities. Such methods present unique challenges to traditional IT security systems. Modified attacks can bypass signature-based systems and new zero-day exploits take advantage of system vulnerabilities that software companies have not yet had an opportunity to patch. The tools for creating unknown malware variants are available for purchase on marketplaces within the Dark Web. Nearly anyone with sufficient curiosity, gall or bitcoin can buy a zero-day and launch an attack that can bypass the vast majority of network security systems that rely solely on pattern-matching.

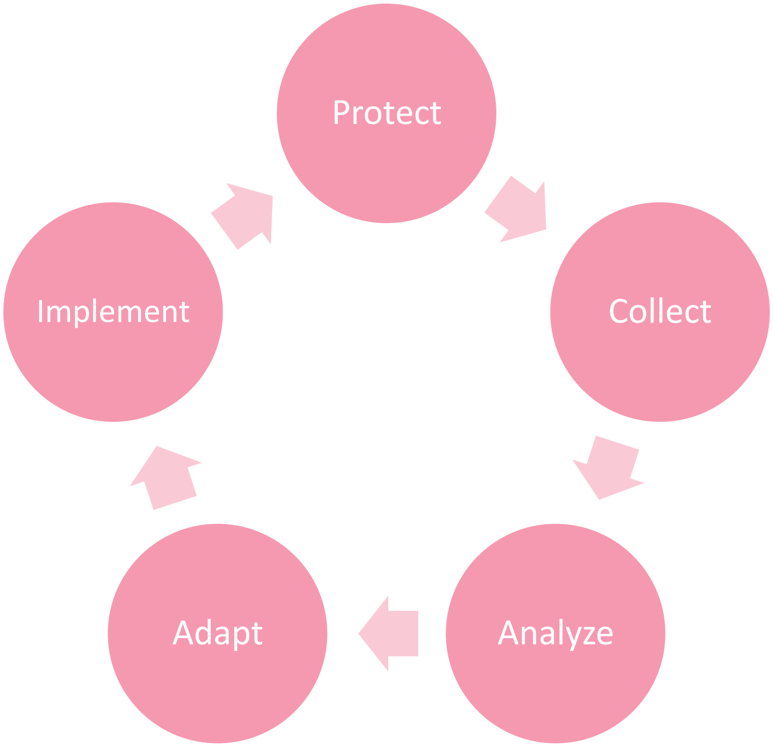
Methods of attack vary. Often, attacks are distributed via email or instant messaging "phishing" schemes. They may also be placed within infected websites or in malicious files on legitimate web properties. Attacks may target personal, web-based email accounts or popular chat tools that exist outside the protected systems of companies or organizations.

This combination of varied attack vectors and unknown vulnerabilities / exploits expands the scope of an individual company's threat environment. The result is a situation in which the pool of potential attackers, who are frequently working together in an organized fashion, has greatly expanded and targets can now include nearly any employee. Not surprisingly, the increase in potential attackers and targets leads to organizations of all sizes facing a volume of continuously changing threats and alerts that can exceed tens of thousands every day.

What to do

To cope with this complex attack environment, companies must consider a revised security approach that emphasizes prevention over detection and is built on intelligence and analytics.

The following diagram shows the lifecycle of this new approach.



- **Protect**: organizations must attempt to block all phases of an attack by leveraging most advanced malware and exploit protection technologies in addition to advanced network segmentation.
- **Collect**: log all relevant data in order to build a comprehensive database of events covering all aspects of the network, systems and applications – and integrate this information to enable comprehensive analysis.
- **Analyze**: operate a continuous analytics lifecycle that includes historical data and real-time events, and that incorporates intelligence feeds from internal and external sources.
- **Adapt**: modify security policies and rule-bases leveraging the learnings derived from the analytical process, and, as much as feasible, lay the groundwork for automated policy-making and protection configuration.
- **Implement**: push updated protections throughout the network and extend all protections to all enforcement points on the network and to all platforms on which users interact with company information.

How to do it

To help organizations transition to this new security approach, IBM Security and Check Point have developed an alliance that combines threat intelligence sharing, technology integrations and managed security services. This relationship is intended to help organizations implement the above principles efficiently and effectively.

The following sections describe the integration points and solutions that will be available through the IBM Security – Check Point alliance.

Prevent first with the most advanced protection technologies

In spite of the near continuous rise in attack volume and complexity, many companies implement advanced security solutions in monitor-only mode, and some have not implemented them at all. This tendency may be out of a fear of false positives requiring attention of already overworked incident response team, or concerns about investment in new (and thus unproven) technology.

And yet, practical experience shows that the cost of a security breach increases the longer an attack is able to operate on a network. A monitor-only approach will provide potential awareness of a successful attack, but it will also give the attack the opportunity to spread across the network and obtain valuable information until action can be taken to remediate the breach.

To help companies address this need, IBM Security and Check Point each offer a range of advanced attack prevention solutions. Included among these are IBM Security Network Protection (XGS), a next-generation intrusion prevention system (IPS), and Check Point's Next Generation Threat Prevention products. The IBM XGS uses the Protocol Analysis Module (PAM), developed by IBM X-Force®, for deep packet inspection. Utilizing heuristics and behavioral-analysis from PAM, IBM XGS is able to protect against entire classes of vulnerabilities in ways that simple pattern-matching signatures cannot. Check Point's Sandblast offerings, which incorporate CPU-level exploit detection, as well as Threat Extraction functionality that provides users with a safe, reconstructed version of content while sandbox analysis is being performed, further enhance protection from advanced threats.

Continuous logging, analytics and intelligence

The first phase of a security attack often involves some form of reconnaissance. Basic forms of exploration can include port scanning to identify available egress options or OS fingerprinting for selecting relevant exploits.

A more aggressive effort will use multiple exploratory methods in parallel or in sequence. And, even though attackers often hide themselves through address spoofing or through the use of anonymizers such as TOR, there will remain identifiers that security administrators can use to find source and method information about the parties trying to break through network defenses.

In order to find these identifiers, security analysts need to use multiple tools simultaneously, such as:

1. Aggregators that pull and correlate logs from security, network, server, desktop systems and applications to provide a comprehensive view of attack activity.
2. Full-packet captures that give visibility into the deepest parts of an attack.
3. Real-time protection tuning functions that can filter out network noise or track modifications to attack tools in real-time.

Check Point is developing a SmartEvent app that will be deployed on the IBM Security App Exchange.[1] This app will enable integration of the Check Point SmartEvent data with IBM Security QRadar bringing leading analytical tools into a combined intelligence platform. Analysts can access the full set of QRadar and SmartEvent functions within the QRadar console. This integration significantly speeds the analytical process; all analysis functions can be carried out within the QRadar console. Analysts also benefit from SmartEvent's internal aggregation functions, which help summarize the Check Point logs into more easily understandable event information with the option to fine-tune Check Point protections directly from the SmartEvent toolset operating as an integrated application within QRadar.

The integration provides additional benefit when coupled with a prevent-first approach. Administrators can use the analytics provided by the integration of QRadar and SmartEvent to write custom signatures for the IBM XGS next-generation IPS appliances and capture the output of the analytical process as indicators that can be imported into the Check Point Threat Prevention feature set. Doing so will help security administrators close the loop that begins with the logs that represent the first signs of an attack and ends with the updating of protection technologies to block the continued attack attempt.

The importance of intelligence

Internal event data provides a wealth of information for analysts to identify and block attacks. But, it will always be limited to what is seen or occurs on an individual company's network. This significantly limits attribution, which is crucial to future prevention efforts. It also restricts prediction. A company's security practitioner cannot benefit from the wisdom of other organizations that have already seen attack methods that remain unknown to that security administrator.

The IBM Security – Check Point alliance enables shared insights from two leading security intelligence platforms: IBM X-Force Exchange and ThreatCloud. Backed by global teams of researchers and analysts, X-Force Exchange and ThreatCloud individually incorporate feeds from

[1] The Check Point SmartEvent App is expected to be available on IBM Security App Exchange in late 1Q-2016.

thousands of sensors and gateways distributed around the globe. Both companies use their intelligence networks to generate and distribute that information in their security technologies for threat protection. They also provide unique research on advanced campaigns, such as those carried out by organized crime and actors within countries rated high for malicious activities, and publish details on vulnerabilities and other threat indicators that potentially can be exploited by individual or coordinated threat actors.

As a part of the newly strengthened relationship, the IBM X-Force and Check Point research teams will share information on new and evolving attacks. The combined investigative effort can provide a range of benefits to customers and the broader security community, including:

1. Continuous dialog between the IBM X-Force and Check Point research teams, both during live incident response efforts and through joint research efforts.
2. Validation of potential findings across each company's research tools and active sensor networks to improve accuracy and reduce false positives.
3. Shared indicators that can be translated into the protection language of the two companies, including STIX and TAXII open protocols, so that customers who leverage both companies' products can block attacks simultaneously on multiple platforms for true defense-in-depth.
4. A global understanding of attack trends and methods, with research centers throughout the world.

Regular security policy revision with automation

Ultimately, the outcome of any security analytics and intelligence effort should be proposed modifications to security policy and device rule-bases. Considering the continuous flow of attacks and the needs of the business to innovate and grow, companies need to find ways to speed the deployment of policy updates.

The IBM Security – Check Point alliance gives customers a broad set of tools to streamline the policy revision effort:

1. IBM Managed Security Services provides a global team of security experts who can create, augment and modify policies at the organizational and device level.
2. The Check Point management suite enables the consistent application of security management policies across the network. Additionally, the new R80 security management platform incorporates a fully automated rule-base infrastructure to which security engineers can interface through the system's GUI, command line and web services.
3. IBM Security and Check Point professional services experts can assist companies in the design and integration of automation tools that can enable lines of business to engineer rule-base changes independently while empowering security teams to review proposed changes and modify/approve as required.

Building upon an 18 year relationship between the companies, IBM Managed Security Services will continue to deliver high-value services for Check Point products around the globe. Additionally, IBM Security offers both technology solutions and professional services focused on identifying vulnerabilities and helping organizations optimize their security programs around the findings from the assessment process.

Implement protections on all platforms

New policies or changes to rule-bases are meaningless if they are not implemented quickly and uniformly across the organization. And yet, many organizations struggle to push changes efficiently across all systems and devices. The IBM Security – Check Point alliance was specifically designed to ease the security implementation challenge.

IBM and Check Point have partnered since 1998 to offer managed security services to companies of all industries and sizes. The IBM Managed Security Services team can assist customers to monitor their Check Point technologies and can implement changes to policies 24x7x365 across the globe. The IBM Security Operations Centers are staffed with engineering and analysis teams who are certified on Check Point products at the highest levels, and Check Point works with IBM to ensure that the IBM team members remain up-to-date on new products, technologies and methods.

The two companies have also taken this partnership to a new level through advanced technology integration focused on protecting organizations mobile strategies.

Advanced Mobile Protection

All companies seek to leverage mobile platforms to expand their reach to employees, partners and customers. And yet, attackers have begun to add mobile devices to their target list. To help address this challenge, Checkpoint Mobile Threat Prevention (MTP) has integrated with IBM MaaS360 Enterprise Mobility Management solution. The integrated solution will allow customers to prevent compromised devices from accessing enterprise networks and data, based on real-time insights from Checkpoint MTP and automated policy enforcement plus threat remediation from IBM MaaS360. Customers can now:

1. Simplify deployment of MTP by leveraging IBM MaaS360 to remotely configure and distribute MTP mobile app on managed mobile devices,
2. Gain visibility into high risk devices based on real-time risk scoring from MTP, and
3. Enforce policies and take remedial action against threats using IBM MaaS360.[2]

[2] Availability of the integration enabling Check Point Mobile Threat Prevention (MTP) to trigger IBM MaaS360 actions/policies to remediate threats based on risk evaluation is expected in late 1Q-2016.

Conclusion

The threat landscape is constantly changing, and security-minded organizations are looking to optimize their defenses in order to limit business risk. By leveraging the combined strengths of IBM Security and Check Point in areas of threat research, security incident and event management (SIEM), mobile threat protection integration, and managed services, organizations will be better positioned to effectively, *and efficiently*, stay one step ahead of the latest threats.

Many of the components of this new alliance will be transparent to customers of both vendors, as IBM Security and Check Point simply take advantage of a greater level of collaboration in threat intelligence sharing. Others will be more visible, as Check Point launches its SmartEvent app in the IBM Security App Exchange and product integration to allow deployment and management of advanced threat prevention for mobile devices are made available. In all, this will make securing your environments with the latest in threat protection even easier to achieve.