Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Earth Koshchei's Large-Scale Spear-Phishing Campaign Exposed

Date of Publication

December 20, 2024

Admiralty Code

A1

TA Number

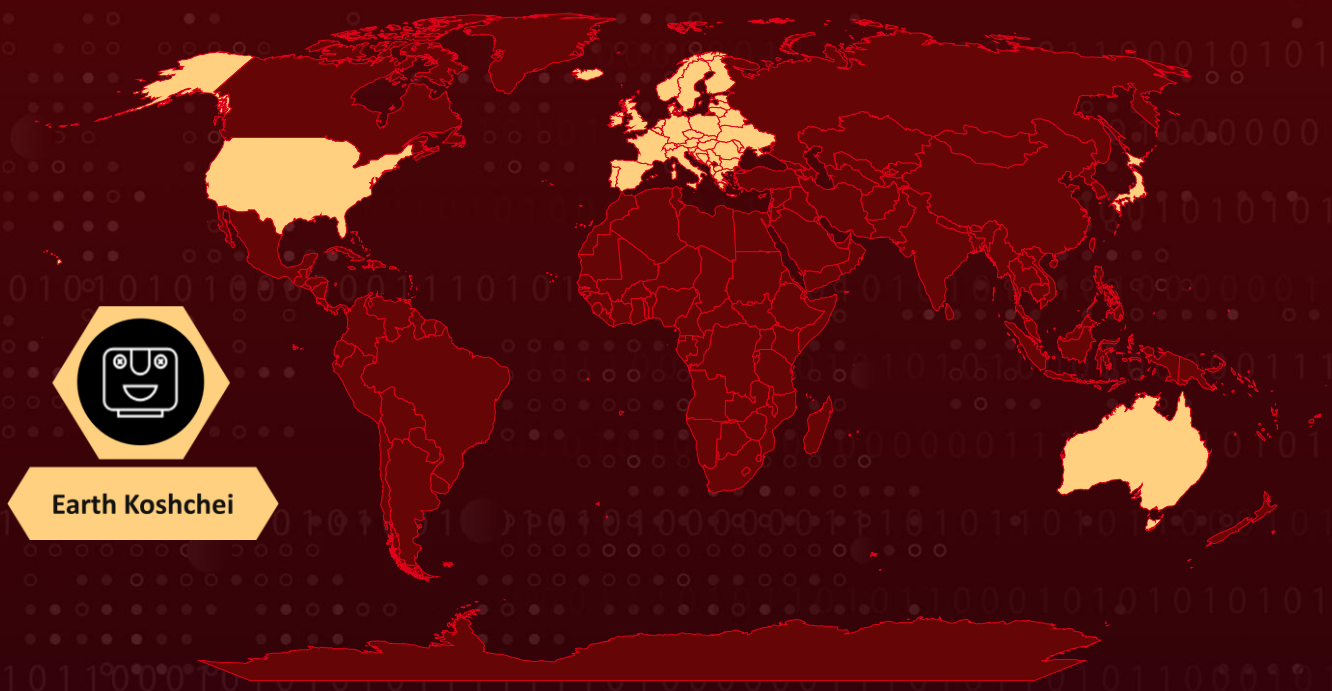
TA2024470

Summary

Attack Commenced: August - October 2024
Threat Actor: Earth Koshchei (aka APT29, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, Midnight Blizzard, UNC3524, Cranefly, TEMP.Monkeys, Cloaked Ursa, Blue Dev 5, NobleBaron, Solar Phoenix)
Targeted Regions: Europe, US, Japan, Ukraine, and Australia
Targeted Industries: Diplomats, Energy, Telecommunications, IT, Government, Think Tanks, NGOs, Politics, Aerospace, Defense, Banking

Attack: Earth Koshchei, also referred to as APT29, launched a highly advanced Remote Desktop Protocol (RDP) attack campaign, integrating spear-phishing tactics and malicious RDP configuration files to compromise high-value targets. By exploiting over 200 fraudulent domains designed to impersonate legitimate organizations, the group deceived victims into accessing rogue RDP relays, facilitating the deployment of malicious scripts and unauthorized system access.

Attack Regions



Attack Details

#1 Earth Koshchei, also known as APT29 or Midnight Blizzard, conducted a rogue Remote Desktop Protocol (RDP) campaign marked by meticulous preparation and advanced attack techniques. Between August and October 2024, the campaign used spear-phishing emails to deliver malicious RDP configuration files, resulting in potential data breaches, malware installation, and system compromise.

#2 The attack chain started with spear-phishing emails crafted to trick recipients into executing a rogue RDP configuration file. This action redirected victims to one of the group's 193 RDP relays. These rogue servers imitated legitimate RDP server behavior, allowing attackers to exploit the sessions to deploy malicious scripts, modify system settings, or inject payloads.

#3 The PyRDP proxy enabled access to victims' file systems, facilitating directory browsing, file modification, and the extraction of sensitive information, including credentials and proprietary data. Earth Koshchei exhibited extensive planning by registering over 200 domain names mimicking legitimate entities, such as Australian, Ukrainian, and Dutch governmental organizations.

#4 These domains formed the backbone of their campaign infrastructure. On October 22, 2024, Earth Koshchei launched a massive spear-phishing attack targeting high-profile entities, including governments, military organizations, think tanks, and academic researchers, with a specific emphasis on Ukrainian targets.

Recommendations

Email Security and Spear-Phishing Protection: Implement advanced email filtering solutions to detect and block spear-phishing attempts with malicious RDP configuration files. Use multi-factor authentication (MFA) for email accounts to minimize risks associated with credential theft.

Endpoint and Network Protection: Disable unused Remote Desktop Protocol (RDP) services to reduce the attack surface. Configure RDP access through secure gateways or VPNs with strict authentication mechanisms. Monitor and log RDP connections for suspicious activities, such as abnormal access attempts or connections to unknown relays.

Anonymization and Proxy Abuse Detection: Detect and block the use of anonymization layers such as TOR, residential proxies, or commercial VPNs when accessing critical systems. Correlate logs to identify patterns suggesting the use of such tools in ongoing campaigns.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**T1566** Phishing	**T1204** User Execution
T1552.001 Credentials In Files	**T1566.001** Spearphishing Attachment	**T1078.003** Local Accounts	**T1078** Valid Accounts
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1090** Proxy	**T1552** Unsecured Credentials
T1083 File and Directory Discovery	**T1018** Remote System Discovery	**T1560** Archive Collected Data	**T1560.003** Archive via Custom Method
T1005 Data from Local System	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1204.002** Malicious File
T1574 Hijack Execution Flow	**T1046** Network Service Discovery	**T1570** Lateral Tool Transfer	**T1563.002** RDP Hijacking
T1563 Remote Service Session Hijacking	**T1021.001** Remote Desktop Protocol	**T1021** Remote Services	**T1036** Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	103[.]144[.]139[.]253, 103[.]144[.]139[.]254, 103[.]144[.]139[.]73, 103[.]144[.]139[.]74, 104[.]161[.]58[.]10, 141[.]195[.]117[.]126, 141[.]195[.]117[.]127, 141[.]195[.]117[.]128, 141[.]195[.]117[.]129, 155[.]138[.]238[.]169, 162[.]216[.]243[.]210, 172[.]86[.]73[.]187, 175[.]110[.]112[.]221, 175[.]110[.]114[.]9, 178[.]255[.]43[.]30, 185[.]100[.]234[.]105, 185[.]172[.]39[.]220, 185[.]172[.]39[.]230, 185[.]177[.]126[.]225, 185[.]187[.]155[.]69, 185[.]243[.]112[.]24, 185[.]243[.]114[.]9, 185[.]243[.]115[.]124, 193[.]29[.]56[.]221, 195[.]3[.]220[.]48, 37[.]28[.]153[.]214, 37[.]28[.]157[.]246, 45[.]137[.]21[.]10, 45[.]137[.]21[.]11, 45[.]82[.]66[.]39, 45[.]86[.]162[.]170, 46[.]30[.]188[.]187, 46[.]30[.]189[.]62, 46[.]30[.]189[.]91, 5[.]183[.]95[.]158, 5[.]183[.]95[.]240, 5[.]187[.]49[.]186, 66[.]206[.]13[.]130, 92[.]204[.]164[.]50, 179[.]43[.]148[.]82, 104[.]225[.]129[.]128, 104[.]238[.]57[.]40, 104[.]238[.]60[.]216,

TYPE	VALUE
IPv4	104[.]36[.]229[.]110, 109[.]205[.]214[.]45, 109[.]205[.]214[.]50, 109[.]205[.]214[.]52, 13[.]49[.]21[.]253, 135[.]181[.]130[.]232, 141[.]195[.]117[.]125, 142[.]91[.]38[.]80, 146[.]71[.]81[.]13, 149[.]154[.]158[.]133, 149[.]154[.]158[.]205, 149[.]154[.]158[.]250, 149[.]154[.]158[.]63, 149[.]154[.]158[.]85, 149[.]28[.]9[.]18, 151[.]236[.]14[.]116, 151[.]236[.]15[.]134, 151[.]236[.]16[.]101, 151[.]236[.]16[.]102, 151[.]236[.]16[.]128, 151[.]236[.]16[.]138, 151[.]236[.]16[.]149, 151[.]236[.]16[.]193, 151[.]236[.]16[.]213, 151[.]236[.]16[.]22, 151[.]236[.]16[.]220, 151[.]236[.]16[.]226, 151[.]236[.]16[.]236, 151[.]236[.]16[.]24, 151[.]236[.]16[.]245, 151[.]236[.]16[.]38, 151[.]236[.]16[.]98, 151[.]236[.]22[.]149, 151[.]236[.]22[.]36, 158[.]255[.]213[.]154, 158[.]255[.]213[.]168, 158[.]255[.]213[.]185, 158[.]255[.]213[.]192, 158[.]255[.]213[.]227, 158[.]255[.]213[.]49, 162[.]252[.]172[.]109, 162[.]252[.]172[.]155, 162[.]252[.]172[.]158, 162[.]252[.]172[.]167, 162[.]252[.]172[.]223,

TYPE	VALUE
IPv4	162[.]252[.]172[.]59, 162[.]252[.]175[.]233, 166[.]0[.]187[.]183, 166[.]0[.]187[.]199, 166[.]0[.]187[.]231, 166[.]0[.]187[.]233, 166[.]0[.]187[.]235, 166[.]0[.]187[.]236, 166[.]0[.]187[.]237, 166[.]0[.]187[.]240, 166[.]0[.]187[.]241, 166[.]0[.]187[.]242, 166[.]0[.]187[.]243, 166[.]0[.]187[.]245, 166[.]0[.]187[.]252, 172[.]86[.]70[.]64, 172[.]96[.]137[.]125, 176[.]97[.]70[.]55, 178[.]162[.]203[.]91, 178[.]239[.]171[.]41, 179[.]43[.]163[.]18, 179[.]43[.]180[.]74, 185[.]172[.]39[.]50, 185[.]172[.]39[.]51, 185[.]172[.]39[.]52, 185[.]187[.]155[.]33, 185[.]187[.]155[.]71, 185[.]187[.]155[.]72, 185[.]187[.]155[.]73, 185[.]187[.]155[.]74, 185[.]187[.]155[.]78, 185[.]187[.]155[.]79, 185[.]187[.]155[.]81, 185[.]216[.]72[.]182, 185[.]216[.]72[.]185, 185[.]216[.]72[.]192, 185[.]216[.]72[.]196, 185[.]76[.]79[.]118, 185[.]76[.]79[.]130, 185[.]76[.]79[.]140, 185[.]76[.]79[.]16, 185[.]76[.]79[.]167, 185[.]76[.]79[.]178, 185[.]76[.]79[.]190, 185[.]76[.]79[.]229, 185[.]76[.]79[.]233,

TYPE	VALUE
IPv4	185[.]76[.]79[.]244, 185[.]76[.]79[.]53, 185[.]76[.]79[.]59, 185[.]76[.]79[.]60, 185[.]76[.]79[.]62, 185[.]76[.]79[.]86, 188[.]214[.]33[.]222, 190[.]211[.]254[.]32, 192[.]121[.]23[.]126, 192[.]36[.]27[.]226, 192[.]36[.]57[.]107, 193[.]200[.]17[.]162, 193[.]29[.]59[.]9, 194[.]37[.]97[.]189, 198[.]50[.]106[.]140, 198[.]50[.]106[.]141, 2[.]58[.]14[.]80, 2[.]58[.]200[.]78, 2[.]58[.]200[.]79, 2[.]58[.]200[.]80, 2[.]58[.]201[.]112, 2[.]58[.]201[.]27, 2[.]58[.]203[.]61, 209[.]182[.]225[.]10, 212[.]1[.]213[.]198, 212[.]1[.]213[.]200, 23[.]108[.]190[.]249, 23[.]160[.]56[.]100, 23[.]160[.]56[.]105, 23[.]160[.]56[.]110, 23[.]160[.]56[.]115, 23[.]160[.]56[.]122, 23[.]160[.]56[.]123, 23[.]160[.]56[.]90, 23[.]160[.]56[.]95, 23[.]227[.]194[.]189, 37[.]1[.]196[.]172, 38[.]180[.]110[.]238, 38[.]180[.]136[.]93, 38[.]180[.]137[.]213, 38[.]180[.]146[.]178, 38[.]180[.]146[.]193, 38[.]180[.]146[.]210, 38[.]180[.]146[.]216, 38[.]180[.]146[.]230,

TYPE	VALUE
IPv4	38[.]180[.]146[.]28, 38[.]180[.]146[.]29, 38[.]180[.]146[.]30, 38[.]180[.]146[.]32, 38[.]180[.]199[.]28, 38[.]180[.]230[.]79, 38[.]180[.]5[.]60, 38[.]180[.]81[.]168, 38[.]180[.]83[.]103, 38[.]180[.]83[.]120, 38[.]180[.]88[.]106, 38[.]180[.]90[.]36, 38[.]180[.]91[.]2, 45[.]11[.]230[.]105, 45[.]11[.]230[.]111, 45[.]11[.]230[.]144, 45[.]11[.]230[.]155, 45[.]11[.]230[.]60, 45[.]11[.]231[.]8, 45[.]11[.]231[.]9, 45[.]134[.]110[.]55, 45[.]134[.]110[.]78, 45[.]134[.]110[.]82, 45[.]134[.]110[.]83, 45[.]134[.]111[.]123, 45[.]134[.]111[.]126, 45[.]137[.]213[.]17, 45[.]141[.]58[.]59, 45[.]141[.]58[.]60, 45[.]41[.]187[.]233, 45[.]67[.]84[.]14, 45[.]67[.]85[.]40, 45[.]80[.]193[.]9, 46[.]19[.]141[.]186, 46[.]249[.]38[.]131, 5[.]133[.]9[.]252, 62[.]72[.]7[.]213, 80[.]87[.]206[.]241, 81[.]17[.]31[.]106, 82[.]180[.]139[.]47, 84[.]32[.]188[.]148, 84[.]32[.]188[.]153, 84[.]32[.]188[.]193, 84[.]32[.]188[.]197,

TYPE	VALUE
IPv4	84[.]32[.]188[.]200, 89[.]35[.]131[.]153, 89[.]46[.]234[.]115, 89[.]46[.]234[.]152, 89[.]46[.]234[.]93, 93[.]188[.]163[.]16, 93[.]188[.]164[.]74, 95[.]156[.]207[.]121, 95[.]217[.]113[.]133
Domains	admin-ch[.]cloud, aeinc[.]solutions, albrightstonebridge[.]cloud, amazonmeeting[.]cloud, amazonsolutions[.]cloud, americanprogress[.]cloud, aspeninstitute[.]cloud, asucloud[.]us, aws-data[.]cloud, aws-il[.]cloud, aws-join[.]cloud, awsmeet[.]cloud, aws-meet[.]cloud, aws-meetings[.]cloud, s3-stig[.]cloud, s3-ua[.]cloud, s3-ucia[.]cloud, s3-us[.]navy, s3-zoho[.]cloud, saiccloud[.]us, servicenowinc[.]us, shicloud[.]online, sipacolumbia[.]us, skykick[.]solutions, softcat[.]cloud, ssi-gouv-fr[.]cloud, statecloud[.]us, stratfor[.]cloud, swcloud[.]us, symbolsecurity[.]cloud, trustifi[.]cloud, ua-aws[.]army, ua-energy[.]cloud, ua-gov[.]cloud, ua-mil[.]cloud, ua-sec[.]cloud, ukrainesec[.]cloud,

TYPE	VALUE
Domains	awsmeetings[.]online, aws-online[.]cloud, awsplatform[.]online, aws-ukraine[.]cloud, backupify[.]cloud, barracuda[.]solutions, brookings[.]cloud, bund-de[.]cloud, caci[.]solutions, capgemini[.]services, ceip[.]cloud, cepa[.]solutions, cer[.]zone, cfr-aws[.]cloud, citoc[.]cloud, clari[.]cloud, clearancejobs[.]cloud, cnas[.]zone, c-r[.]services, crisisgroup[.]services, csbaonline[.]cloud, cwinc[.]cloud, defence-au[.]cloud, defense-gouv[.]cloud, democracyendowment[.]cloud, dep-no[.]cloud, difesa-it[.]cloud, druva[.]cloud, ecfr[.]cloud, eopgov[.]cloud, europa-eu[.]cloud, europeanvalues[.]cloud, exclaimer[.]solutions, forces-gc[.]cloud, foreignpolicy[.]cloud, freedomhouse[.]cloud, gc-cloud[.]ca, gmfus[.]cloud, go-conference[.]cloud, go-jp[.]cloud, go-meet[.]pro, go-meeting[.]cloud, go-meeting[.]online, go-meet-up[.]com, google-meet[.]cloud, googlemeet[.]zone,

TYPE	VALUE
Domains	gouv-fr[.]cloud, gov-au[.]cloud, gov-aws[.]cloud, gov-fi[.]cloud, gov-gr[.]cloud, gov-lt[.]cloud, gov-lv[.]cloud, gov-pl[.]cloud, gov-sk[.]cloud, govtr[.]cloud, gov-trust[.]cloud, govua[.]cloud, gov-ua[.]cloud, gv-at[.]cloud, heritagecloud[.]org, justice[.]technology, kam-lt[.]cloud, macfound[.]services, mae-ro[.]cloud, mapn-ro[.]cloud, mde-es[.]cloud, mfa-gov[.]cloud, mfa-gov-il[.]cloud, mfa-gov-tr[.]cloud, microsoftmeeting[.]cloud, microsoft-meeting[.]cloud, mil-be[.]cloud, mil-ee[.]cloud, mil-pl[.]cloud, mil-pt[.]cloud, mimecast[.]cloud, minbuza[.]cloud, mindef-nl[.]cloud, mod-cloud[.]uk, mod-gov-il[.]cloud, morh-hr[.]cloud, ms-conference[.]cloud, msconferences[.]cloud, ms-meeting[.]com, ms-meeting[.]online, ms-meetings[.]online, msz-pl[.]cloud, mvep-hr[.]cloud, mzv-cz[.]cloud, mzv-sk[.]cloud, ncfta[.]cloud,

TYPE	VALUE
Domains	ncsc[.]solutions, ndu[.]solutions, nrcc[.]cloud, oktacloud[.]us, opensocietyfoundations[.]cloud, parseccomputer[.]cloud, polycom[.]solutions, presidencia-pt[.]cloud, prio[.]zone, pulsesecure[.]cloud, quirinale[.]cloud, regeringskansliet-se[.]cloud, rrt[.]solutions, rubrik[.]zone, s3[.]army, s3-acronis[.]cloud, s3-army[.]cloud, s3-atlassian[.]cloud, s3-aws[.]cloud, s3-aws[.]global, s3-bah[.]cloud, s3-be[.]cloud, s3-blackberry[.]cloud, s3-cloud[.]us, s3-csis[.]cloud, s3-de[.]cloud, s3-dgap[.]cloud, s3-dk[.]cloud, s3-dnc[.]cloud, s3-esa[.]cloud, s3-fbi[.]cloud, s3-hudson[.]cloud, s3-ida[.]cloud, s3-iri[.]cloud, s3-knowbe4[.]cloud, s3-marcus[.]cloud, s3-monitoring[.]cloud, s3-nato[.]cloud, s3-ned[.]cloud, s3-nsa[.]cloud, s3-proofpoint[.]cloud, s3-pt[.]cloud, s3-rackspace[.]cloud, s3-rand[.]cloud, s3-spacex[.]cloud, s3-state[.]cloud,

TYPE	VALUE
Domains	usaid[.]cloud, ukrtelecom[.]cloud, us-army[.]cloud, usip[.]us, us-mil[.]cloud, veeam[.]solutions, wilsoncenter[.]cloud, wrapsnet[.]cloud, zero-trust[.]solutions, zixcorp[.]cloud, zoom-meeting[.]cloud, zoom-meeting[.]live, zoom-meeting[.]pro, zoommeeting[.]today, zoom-meeting[.]today, zoommeeting[.]zone, zoom-meetings[.]cloud, 4freerussia[.]cloud
SHA256	50bed47064e4ecd01c4a9271e63af7cfdf52ea4096f205470e41eef7eb01c1e1, 648afcc709ac18c4fe235d24bf51a8230e9700b97c3dcc0a739816966f2b58b6, 280fbf353fdffefc5a0af40c706377142fff718c7b87bc8b0daab10849f388d0, f357d26265a59e9c356be5a8ddb8d6533d1de222aae969c2ad4dc9c40863bfe8, ba4d58f2c5903776fe47c92a0ec3297cc7b9c8fa16b3bf5f40b46242e7092b46, 8b45f5a173e8e18b0d5c544f9221d7a1759847c28e62a25210ad8265f07e96d5, 36e45fdeba3fdb3708fb1c2602c30cb5b66fbc5ea790f0716390d9f69c363542, 2fb1d01f9859c676ef37b060c5e8db0a12472c96260114a6edee45d8546184c9, a246253fab152deac89b895a7c1bca76498b4aa044c907559c15109c1187a448, 1c1941b40718bf31ce190588beef9d941e217e6f64bd871f7aee921099a9d881, f32fa0e3902a1f287280e2e6ddcbfe4fc0a47f1fa5ddb5e04a7651c51343621e

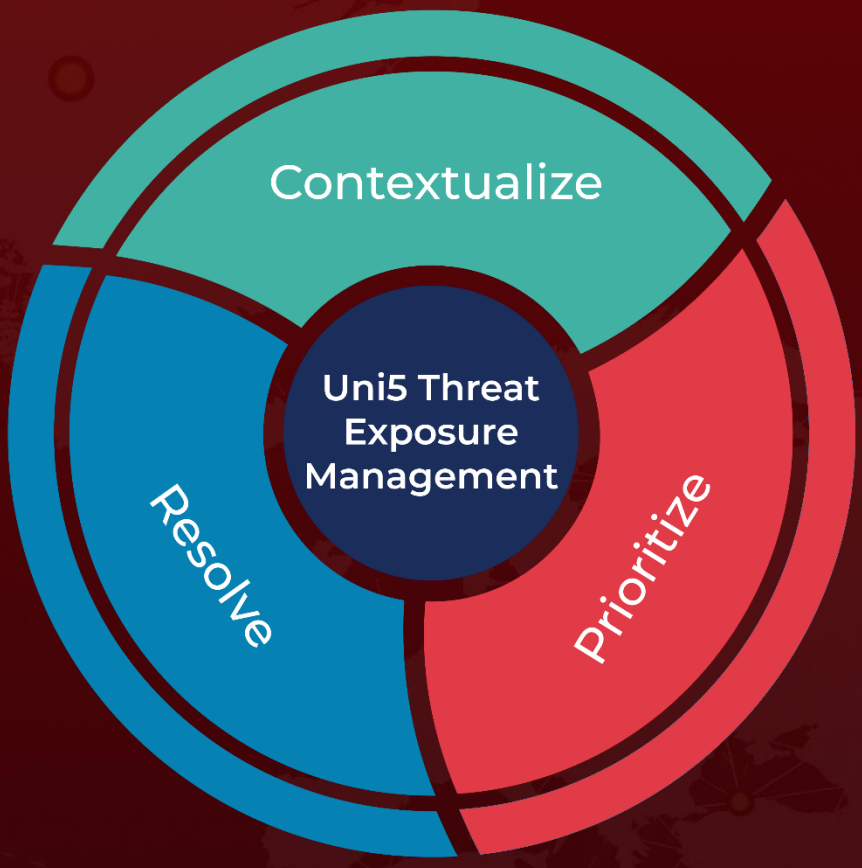
References

https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 20, 2024 . 6:30 AM

More at www.hivepro.com